AVG 9.0 Email Server Edice

Uživatelský manuál

Verze dokumentace 90.2 (8. 12. 2009)

Obsah

1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu ***AVG 9.0 Email Server***.

AVG 9.0 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 9.0 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 9.0 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.

Poznámka: *Tato dokumentace obsahuje pouze popis specifických vlastností edice AVG 9.0 Email Server. Ostatní nastavení a vlastnosti aplikace AVG naleznete popsány v dokumentaci k Internet Security Edici, která je dostupná skrze http://www.avg.cz.*

2. Podmínky instalace

2.1. Podporované operační systémy

AVG 9.0 Email Server je určen k ochraně e-mail serverů s těmito operačními systémy:

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

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. Hardwarové požadavky

Minimální hardwarové požadavky pro ***AVG 9.0 Email Server*** jsou tyto:

- Intel Pentium CPU 1,5 GHz
- 500 MB volného místa na pevném disku (z instalačních důvodů)
- 512 MB RAM paměti

Doporučené hardwarové požadavky pro ***AVG 9.0 Email Server*** jsou tyto:

- Intel Pentium CPU 1,8 GHz

- 600 MB volného místa na pevném disku (z instalačních důvodů)
- 512 MB RAM paměti

2.4. Odinstalujte předchozí verze

Máte-li nainstalovanou starší verzi ***AVG Email Serveru***, je nutné ji před zahájením instalace ***AVG 9.0 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.***

- Pokud jste dříve používali verzi AVG 8.x či starší, nezapomeňte odinstalovat také jednotlivé serverové doplňky.

2.5. Servisní balíčky pro MS Exchange

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 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.

Servisní balík pro MS Exchange 2007 Server (instalace je volitelná)

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

3. Instalační proces AVG

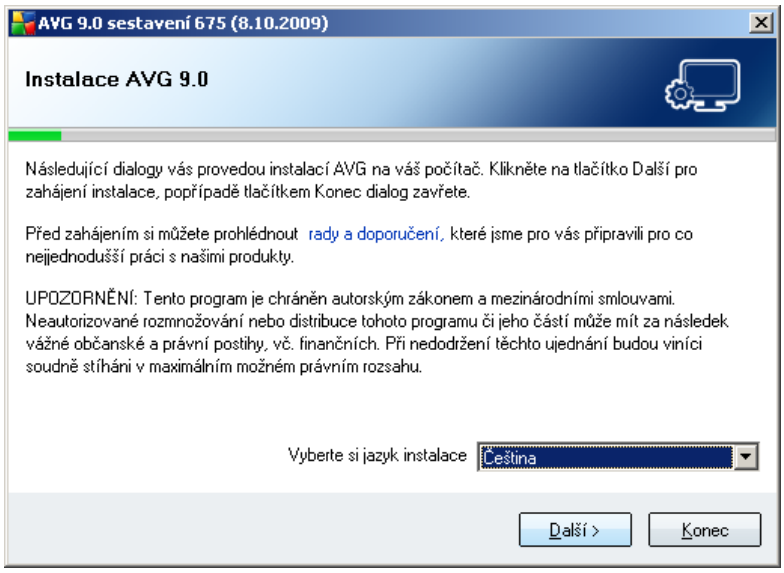
Pro instalaci AVG na váš počítač potřebujete aktuální instalační soubor. Instalační soubor najdete na CD, které bylo součástí zakoupeného balení AVG, ale tento soubor může již být zastaralý.

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:

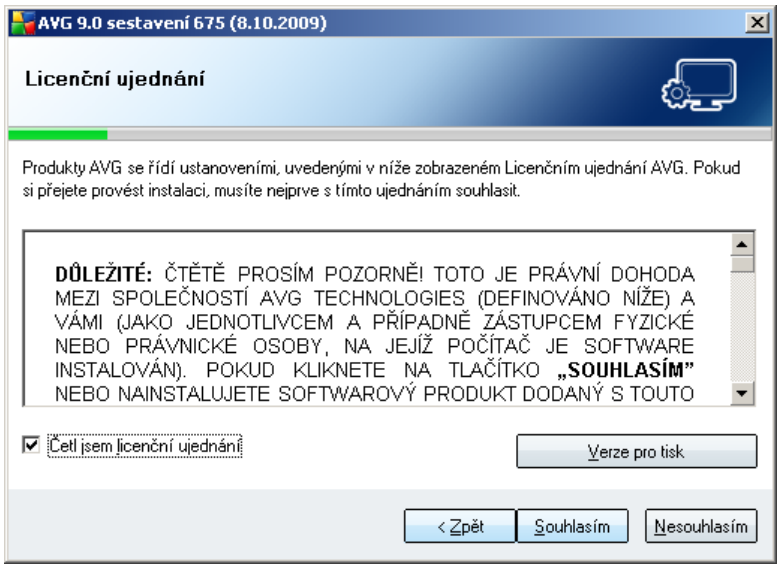
3.1. Spuštění instalace



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 zaškrtnutím políčka Četl jsem licenční ujednání. Stiskem tlačítka ***Souhlasím*** pokračujte dále v instalaci.

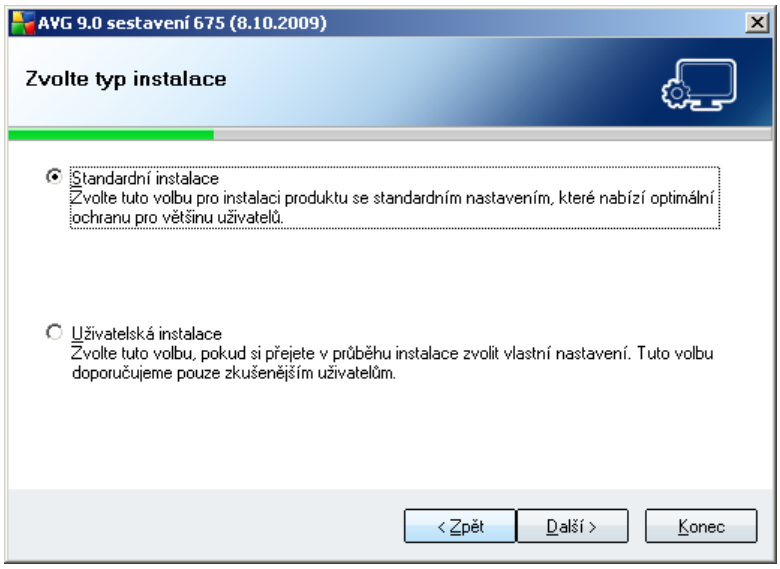
Pokud s licenční smlouvou nesouhlasíte a stisknete tlačítko ***Nesouhlasím***, instalace bude okamžitě ukončena.

Tlačítkem ***Verze pro tisk*** můžete v novém okně zobrazit verzi určenou pro tisk.

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 typ instalace



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

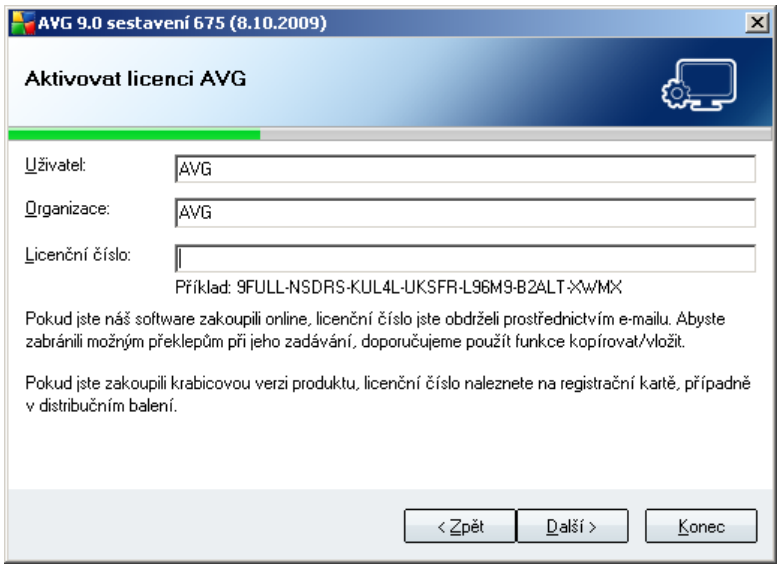
Většině uživatelů doporučujeme použít ***standardní instalaci***, kdy bude AVG nainstalován zcela automaticky s nastavením definovaným výrobcem. Toho nastavení zaručuje maximální úroveň bezpečnosti a optimální využití zdrojů. Pokud se v budoucnu vyskytne potřeba některé konkrétní nastavení změnit, budete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

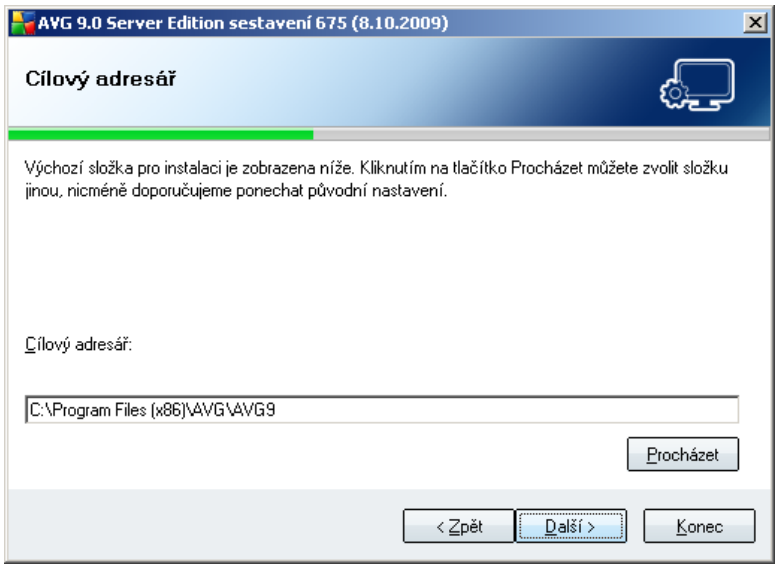
Vepište své jméno (pole ***Uživatel***) a název vaší organizace (pole ***Organizace***). Do položky ***Licenční/Prodejní číslo*** pak zadejte své licenční číslo. Toto číslo najdete buďto na registrační kartě v krabicovém balení AVG, anebo v potvrzovacím emailu, který jste obdrželi při zakoupení AVG on-line. 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***.

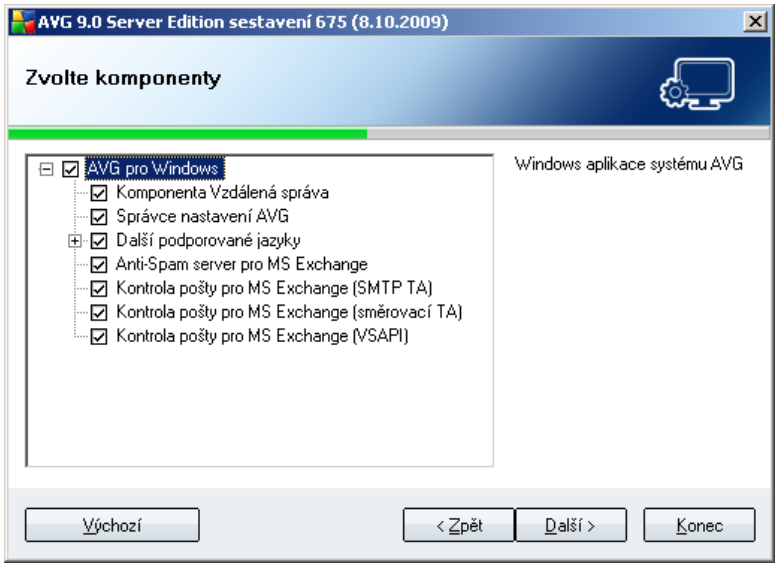
Pokud jste v předchozím kroku zvolili standardní instalaci, přejdete rovnou do dialogu ***Probíhá instalace***. Při volbě uživatelské instalace budete pokračovat dialogem ***Cílový adresář***.

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!

- ***Komponenta Vzdálená správa*** - pokud budete chtít tuto instalaci spravovat vzdáleně, zaškrtněte tuto volbu.

  Poznámka: *Pouze serverové komponenty z tohoto seznamu lze spravovat prostřednictvím Vzdálené správy!*

- ***Správce nastavení AVG*** - nástroj určený zejména správcům sítí sloužící ke kopírování, úpravě a distribuci konfigurace AVG, kterou lze následně uložit např. na přenosné médium a aplikovat ručně či jiným způsobem na vybrané stanice.

- ***Další podporované jazyky*** - zvolte si jazyky uživatelského rozhraní, které

chcete nainstalovat.

Základní přehled jednotlivých serverových komponent:

- ***Anti-Spam server pro MS Exchange***

  Kontroluje všechny příchozí e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nechtěným zprávám.

- ***Kontrola pošty pro MS Exchange (směrovací TA)***

  Kontroluje všechny přicházející, odcházející a interní e-mailové zprávy procházející skrze HUB roli MS Exchange.

  Dostupné pouze pro MS Exchange 2007 a lze nainstalovat pouze na HUB roli.

- ***Kontrola pošty pro MS Exchange (SMTP TA)***

  Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange.

  Dostupné pouze pro MS Exchange 2007 a lze nainstalovat na EDGE i HUB roli.

- ***Kontrola pošty pro MS Exchange (VSAPI)***

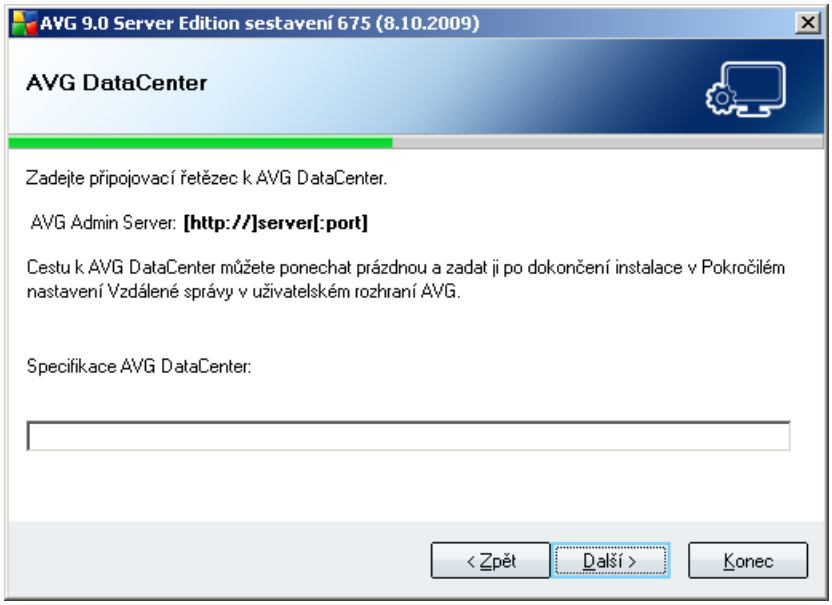
  Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Poznámka: *Nabídka komponent se liší podle verze MS Exchange, který používáte.*

Pokračujte stiskem tlačítka ***Další***.

3.8. Uživatelská instalace - DataCenter

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



3.9. 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***.

3.10. 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.

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

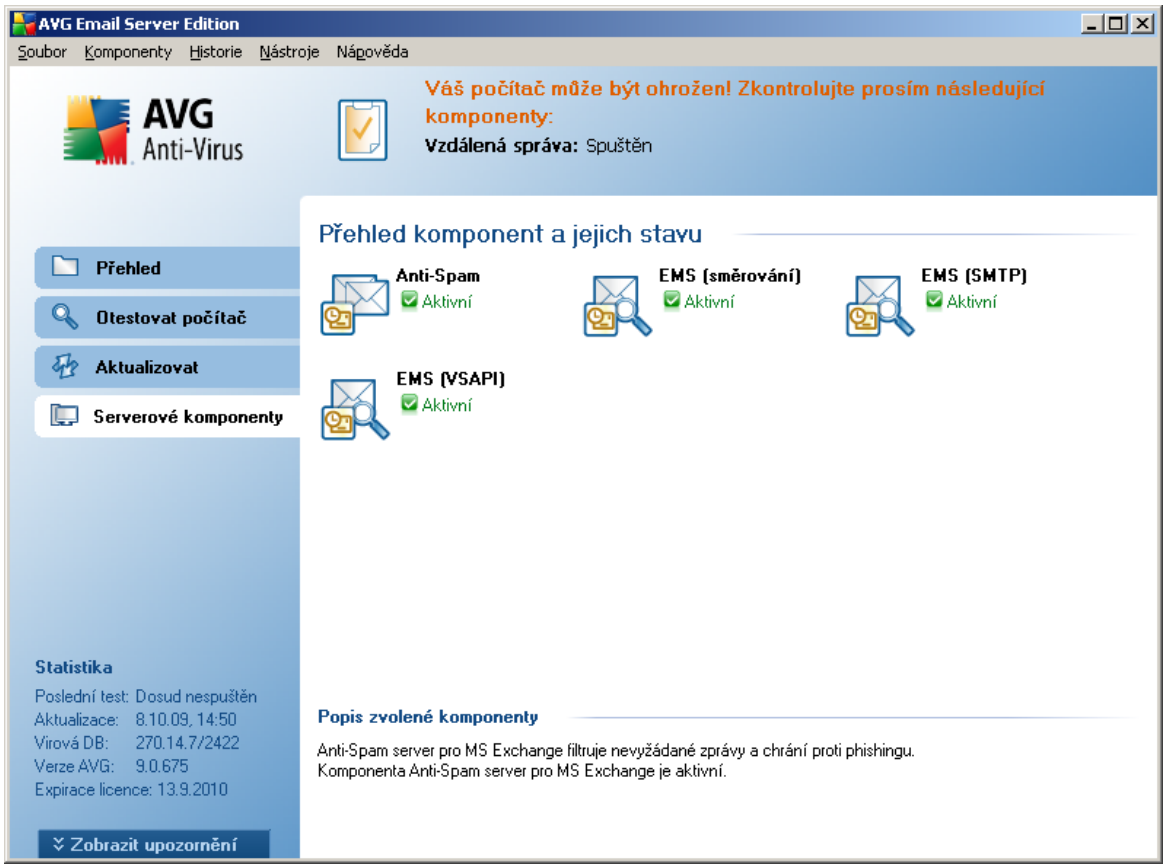
- ***Kontrola pošty pro MS Exchange Server 2007***
- ***Kontrola pošty pro MS Exchange Server 2000/2003***

- ***AVG pro Kerio MailServer***

4. Kontrola pošty pro MS Exchange Server 2007

4.1. Přehled

Konfigurace Kontroly pošty pro MS Exchange Server 2007 je plně integrována v rámci aplikace AVG 9.0 Email Server jako serverová komponenta.



Základní přehled jednotlivých serverových komponent:

- ***Anti-Spam - Anti-Spam server pro MS Exchange***

  Kontroluje všechny příchozí e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nechtěným zprávám.

- ***EMS (směrování) - Kontrola pošty pro MS Exchange (směrovací transportní Agent)***

  Kontroluje všechny přicházející, odcházející a interní e-mailové zprávy procházející skrze HUB roli MS Exchange.

  Dostupné pouze pro MS Exchange 2007 a lze nainstalovat pouze na HUB roli.

- ***EMS (SMTP) - Kontrola pošty pro MS Exchange (SMTP transportní agent)***

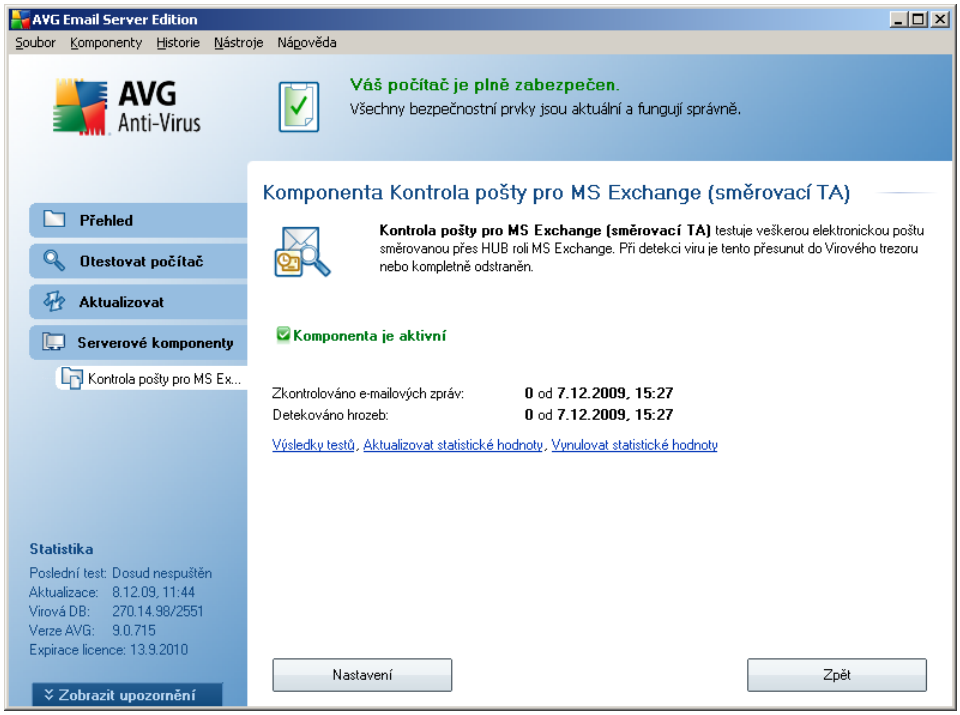
  Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange.

  Dostupné pouze pro MS Exchange 2007 a lze nainstalovat na EDGE i HUB roli.

- ***EMS (VSAPI) - Kontrola pošty pro MS Exchange (VSAPI)***

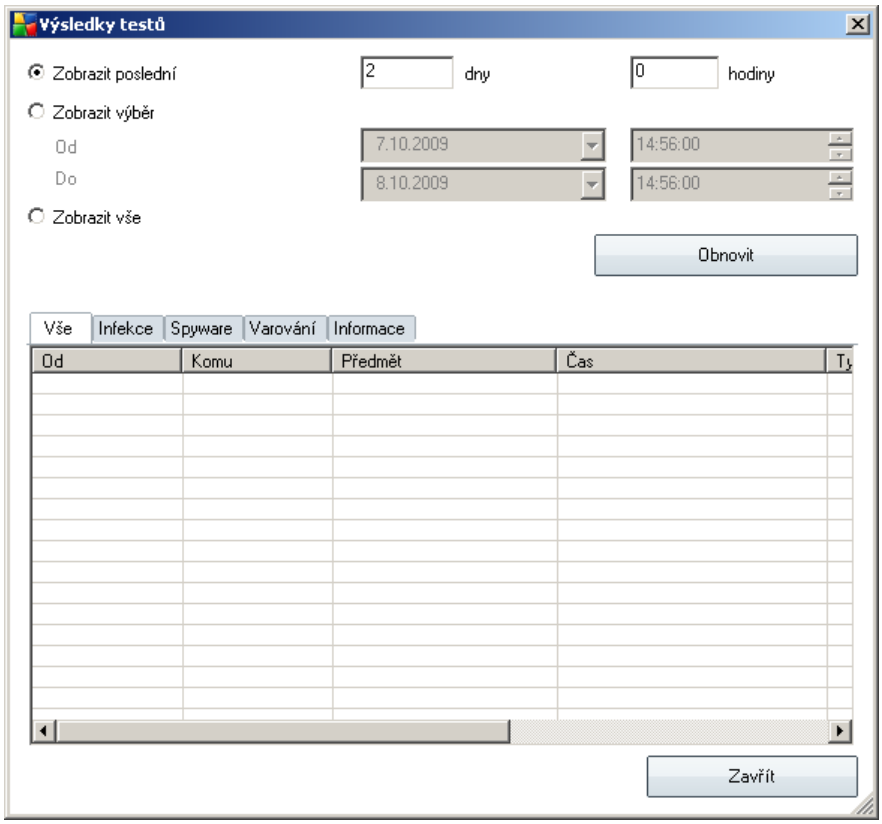
  Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Klikněte dvakrát na požadovanou komponentu pro zobrazení jejího rozhraní. S výjimkou komponenty Anti-Spam sdílejí všechny komponenty společné ovládací prvky:



- ***Výsledky testů***

  Otevře nový dialog s přehledem výsledků testů:



Zde můžete zkontrolovat zprávy rozdělené do několika záložek podle jejich závažnosti. Více informací o konkrétní závažnosti a jejím nastavení naleznete v popisu nastavení jednotlivých serverových komponent.

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit těmito volbami:

- ***Zobrazit poslední*** - vložte preferovaný počet dní a hodin.
- ***Zobrazit výběr*** - zvolte libovolný časový a datumový rozsah.
- ***Zobrazit vše*** - zobrazí výsledky za celé období.

Tlačítkem ***Obnovit*** znovu načtete výsledky testů.

- ***Aktualizovat statistické hodnoty*** - aktualizuje statistiky uvedené v dialogu.
- ***Vynulovat statistické hodnoty*** - vynuluje všechny statistiky.

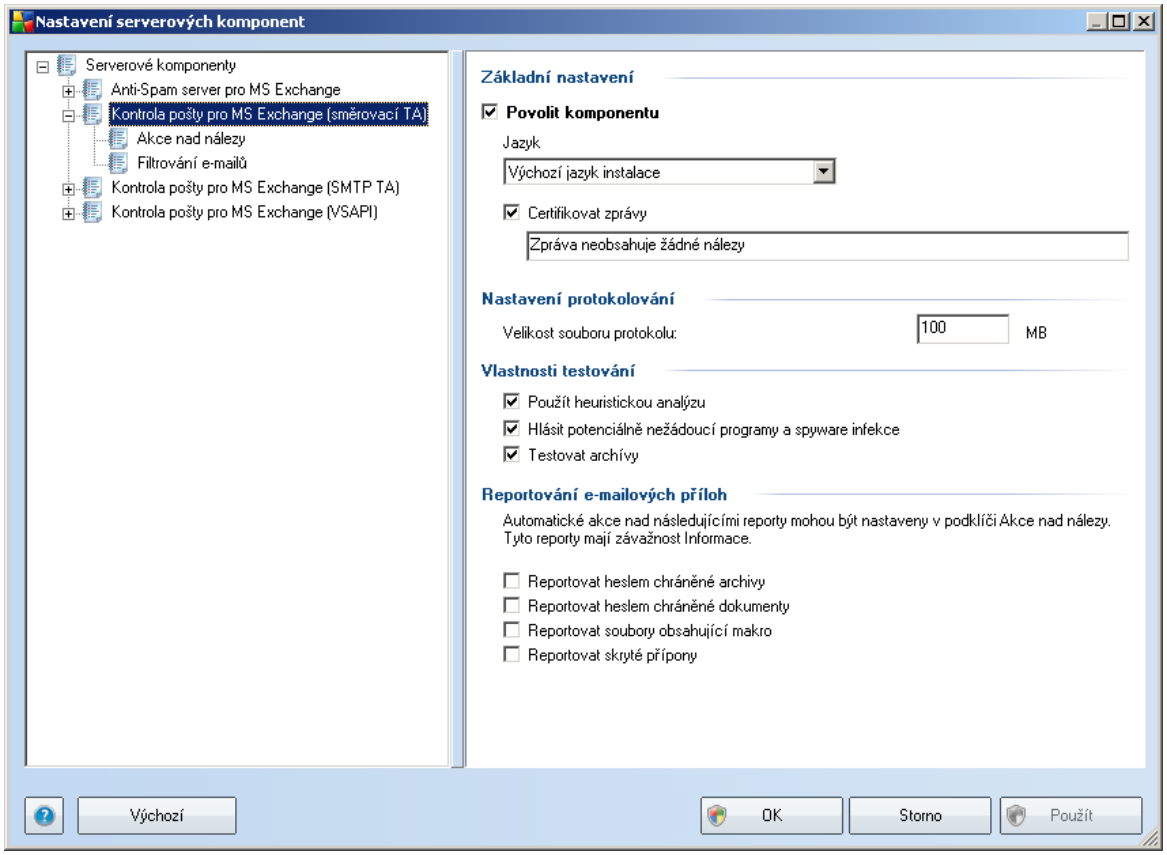
Funkční tlačítka v dialogu jsou tato:

- ***Nastavení*** - tímto tlačítkem otevřete nastavení dané komponenty.
- ***Zpět*** - tímto tlačítkem se vrátíte zpět na seznam komponent.

Bližší nastavení jednotlivých komponent naleznete v kapitolách níže.

4.2. Kontrola pošty pro MS Exchange (směrovací TA)

Tato položka obsahuje možnosti nastavení ***Kontroly pošty pro MS Exchange (směrovací transportní agent)***.



V sekci ***Základní nastavení*** naleznete následující možnosti:

- ***Povolit komponentu*** - odškrtněte pro vypnutí celé komponenty.
- ***Jazyk*** - zvolte preferovaný jazyk komponenty.
- ***Certifikovat zprávy*** - zaškrtněte, pokud si přejete přidat certifikační poznámku ke všem testovaným zprávám. Zprávu můžete upravit v následujícím políčku.

Sekce ***Nastavení protokolování*** obsahuje tyto volby:

- ***Velikost souboru protokolu*** - zvolte preferovanou velikost protokolovacího souboru. Výchozí hodnota je 100 MB.

Sekce ***Vlastnosti testování*** obsahuje tato nastavení:

- ***Použít heuristickou analýzu*** - zaškrtněte pro povolení použití heuristické analýzy v průběhu testování.
- ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - zaškrtněte pro hlášení potenciálně nežádoucích programů a spyware.
- ***Testovat archívy*** - zaškrtněte pro zahrnutí také testování archivních souborů (zip, rar, atp.)

Sekce ***Reportování e-mailových příloh*** umožňuje vybrat položky, které si přejete hlásit v průběhu testování. Pokud je položka zaškrtnutá, bude každá zpráva s takovou přílohou obsahovat v předmětu text [INFORMACE] (ve výchozím nastavení). Toto výchozí nastavení lze změnit ve větvi ***Akce nad nálezy***, část ***Informace*** (viz níže).

K dispozici jsou následující možnosti:

- ***Reportovat heslem chráněné archivy***
- ***Reportovat heslem chráněné dokumenty***
- ***Reportovat dokumenty obsahující makro***
- ***Reportovat skryté přípony***

Součástí nastavení jsou tyto podpoložky ve stromové struktuře:

- ***Akce nad nálezy***
- ***Filtrování e-mailů***

4.3. Kontrola pošty pro MS Exchange (SMTP TA)

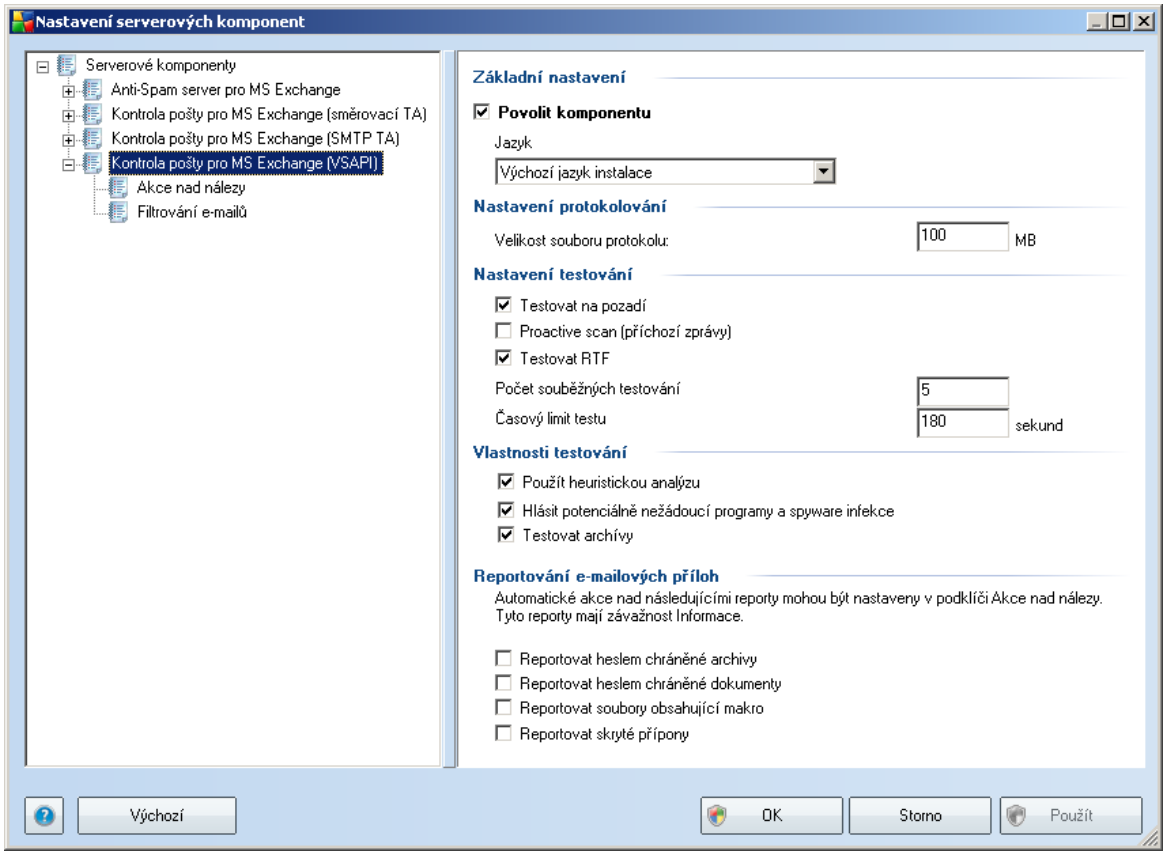
Konfigurace Kontroly pošty pro MS Exchange (SMTP Transportní Agent) je stejná jako pro směrovací transportní agent. Více informací naleznete v kapitole ***Kontrola pošty pro MS Exchange (směrovací TA)*** výše.

Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

- ***Akce nad nálezy***
- ***Filtrování e-mailů***

4.4. Kontrola pošty pro MS Exchange (VSAPI)

Tato položka obsahuje možnosti nastavení ***Kontroly pošty pro MS Exchange*** (VSAPI).



V sekci ***Základní nastavení*** naleznete následující možnosti:

- ***Povolit komponentu*** - odškrtněte pro vypnutí celé komponenty.
- ***Jazyk*** - zvolte preferovaný jazyk komponenty.

Sekce ***Nastavení protokolování*** obsahuje tyto volby:

- ***Velikost souboru protokolu*** - zvolte preferovanou velikost protokolovacího souboru. Výchozí hodnota je 100 MB.

Sekce ***Nastavení testování*** obsahuje tato nastavení:

- ***Testovat na pozadí*** - 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, dostanou 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 scan*).

- ***Proactive scan (příchozí zprávy)*** - 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. Jakmile jsou zprávy umístěny do úložiště serveru Exchange, jsou zařazeny také do obecné fronty k testování s nízkou prioritou (maximum 30 položek). Následně jsou testovány podle metody FIFO (First in, first out). Pokud je k některé položce zaznamenán přístup zatímco je stále ve frontě, její priorita se změní na vysokou.

  Poznámka: *Nadbytečné zprávy jsou přesunuty do úložiště bez otestování.*

Upozornění: *I v případě, vypnutí obou voleb (**Testování na pozadí** a **Proactive Scan**), zůstává i nadále aktivní rezidentní test, který se spustí v momentě stahování zprávy klientem MS Outlook.*

- ***Testovat RTF*** - zvolte, zdali si přejete testovat také RTF soubory.
- ***Počet souběžných testování*** - ve výchozím nastavení běží testovací proces paralelně ve více vláknech, zejména pro zvýšení obecného výkonu. Počet souběžných vláken lze změnit v tomto nastavení.

Výchozí počet vláken je vypočítán jako dvojnásobek "počtu procesorů" + 1.

Minimální počet vláken je vypočítán jako ("počet procesorů" + 1) vyděleno dvěma.

Maximální počet vláken je vypočítán jako "počet procesorů" krát 5 + 1.

Pokud je nastavena hodnota nižší nebo minimální, případně maximální či vyšší, je použita hodnota výchozí.

- ***Časový limit testu*** - maximální souvislý interval (*v sekundách*), po který může jedno vlákno přistupovat k právě testovanému objektu (výchozí hodnota je 180 sekund).

Sekce ***Vlastnosti testování*** obsahuje tato nastavení:

- ***Použít heuristickou analýzu*** - zaškrtněte pro povolení použití heuristické analýzy v průběhu testování.
- ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - zaškrtněte pro hlášení potenciálně nežádoucích programů a spyware.
- ***Testovat archívy*** - zaškrtněte pro zahrnutí také testování archivních souborů (zip, rar, atp.)

Sekce ***Reportování e-mailových příloh*** umožňuje vybrat položky, které si přejete hlásit v průběhu testování. Pokud je položka zaškrtnutá, bude každá zpráva s takovou přílohou obsahovat v předmětu text [INFORMACE] (ve výchozím nastavení). Toto výchozí nastavení lze změnit ve větvi ***Akce nad nálezy***, část ***Informace*** (viz níže).

K dispozici jsou následující možnosti:

- ***Reportovat heslem chráněné archivy***
- ***Reportovat heslem chráněné dokumenty***
- ***Reportovat dokumenty obsahující makro***
- ***Reportovat skryté přípony***

Některé prvky v tomto nastavení 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-

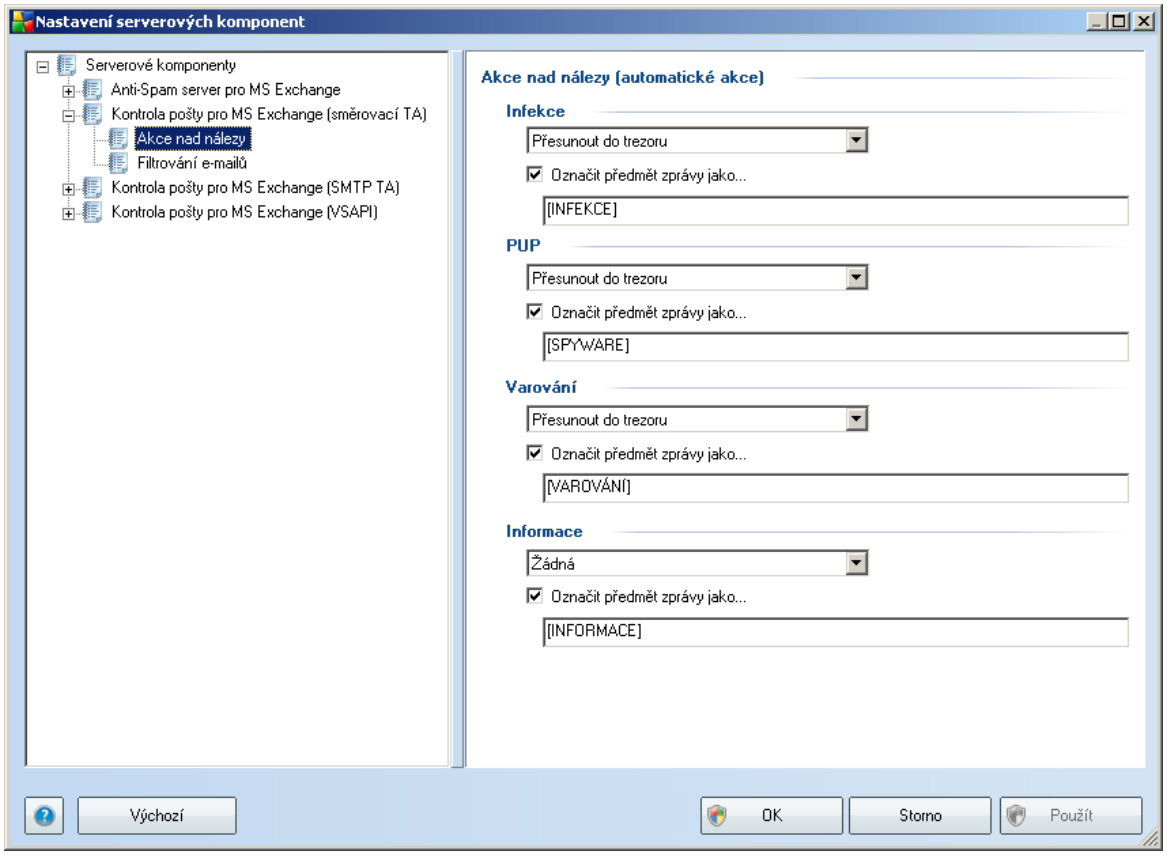
us;328841&Product=exch2k – popis principů spolupráce Exchange s antivirovými programy

- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 – informace o doplňcích ve VSAPI 2.5 v aplikaci Exchange 2003 Server

Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

- ***Akce nad nálezy***
- ***Filtrování e-mailů***

4.5. Akce nad nálezy



V části ***Akce nad nálezy*** lze zaškrtnout a vybrat automatické akce, které mají být provedeny v průběhu testování. Akce jsou k dispozici pro následující položky:

- ***Infekce***
- ***PUP (Potenciálně nežádoucí programy)***
- ***Varování***
- ***Informace***

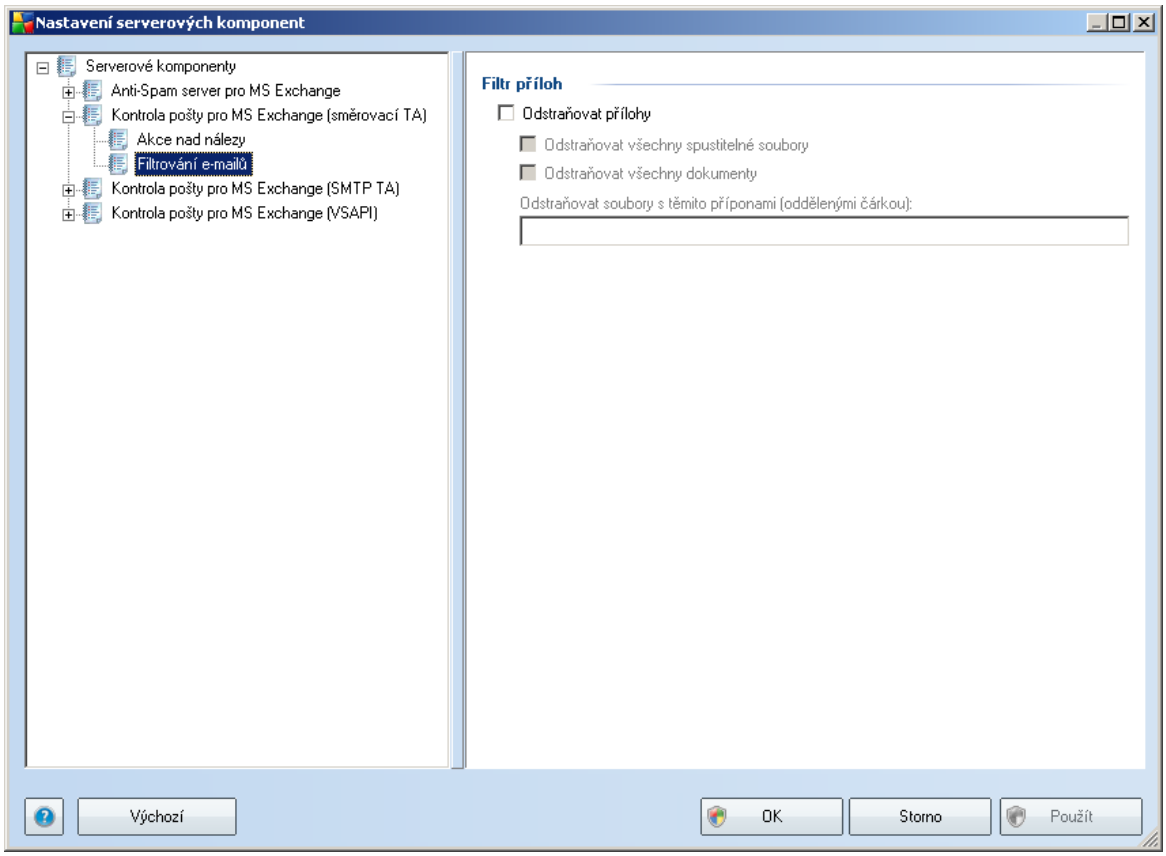
Z rolovací nabídky zvolte pro každou položku vždy jednu akci:

- ***Žádná*** - nebude provedena žádná akce.
- ***Přesunout do trezoru*** - dané nebezpečí bude přesunuto do Virového trezoru.
- ***Odstranit*** - dané nebezpečí bude odstraněno.

Pokud si přejete přidat do předmětu zprávy zpracované určitou akcí textovou informaci pro lepší třídění a přehled, zaškrtněte příslušné políčko ***Označit předmět zprávy jako*** a vložte požadovanou hodnotu.

Poznámka: *Poslední zmíněnou vlastnost nelze aplikovat v případě nastavení Kontroly pošty pro MS Exchange (VSAPI).*

4.6. Filtrování e-mailů



V části ***Filtr příloh*** můžete zvolit přílohy, které mají být automaticky odstraněny. K dispozici jsou následující možnosti:

- ***Odstraňovat přílohy*** - zaškrtněte pro povolení této funkce.
- ***Odstraňovat všechny spustitelné soubory*** - odstraní všechny spustitelné přílohy.
- ***Odstraňovat všechny dokumenty*** - odstraní všechny dokumenty v příloze.
- ***Odstraňovat soubory s těmito příponami (oddělenými čárkou)*** - vložte přípony, které si přejete automaticky odstranit. Hodnoty oddělte čárkou.

5. Kontrola pošty pro MS Exchange Server 2000/2003

5.1. Přehled

Konfigurace Kontroly pošty pro MS Exchange Server 2000/2003 je plně integrována v rámci aplikace AVG 9.0 Email Server jako serverová komponenta.

Základní přehled jednotlivých serverových komponent:

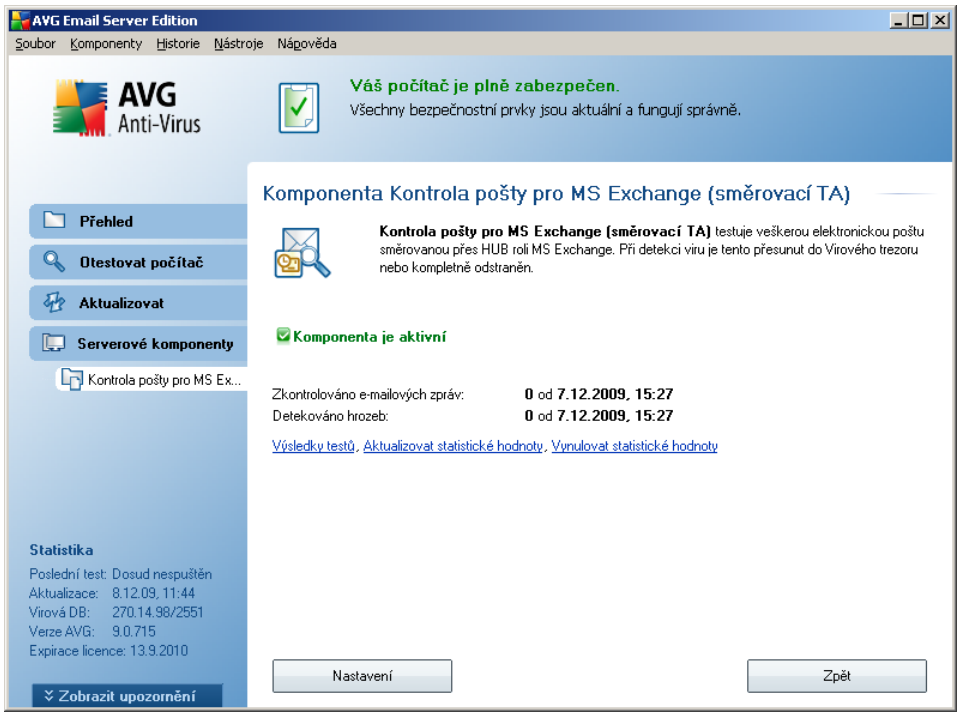
- ***Anti-Spam - Anti-Spam server pro MS Exchange***

  Kontroluje všechny příchozí e-mailové zprávy a označuje nevyžádanou poštu jako SPAM. K analýze každé zprávy využívá několik metod, což zajišťuje maximální možnou ochranu proti nechtěným zprávám.

- ***EMS (VSAPI) - Kontrola pošty pro MS Exchange (VSAPI)***

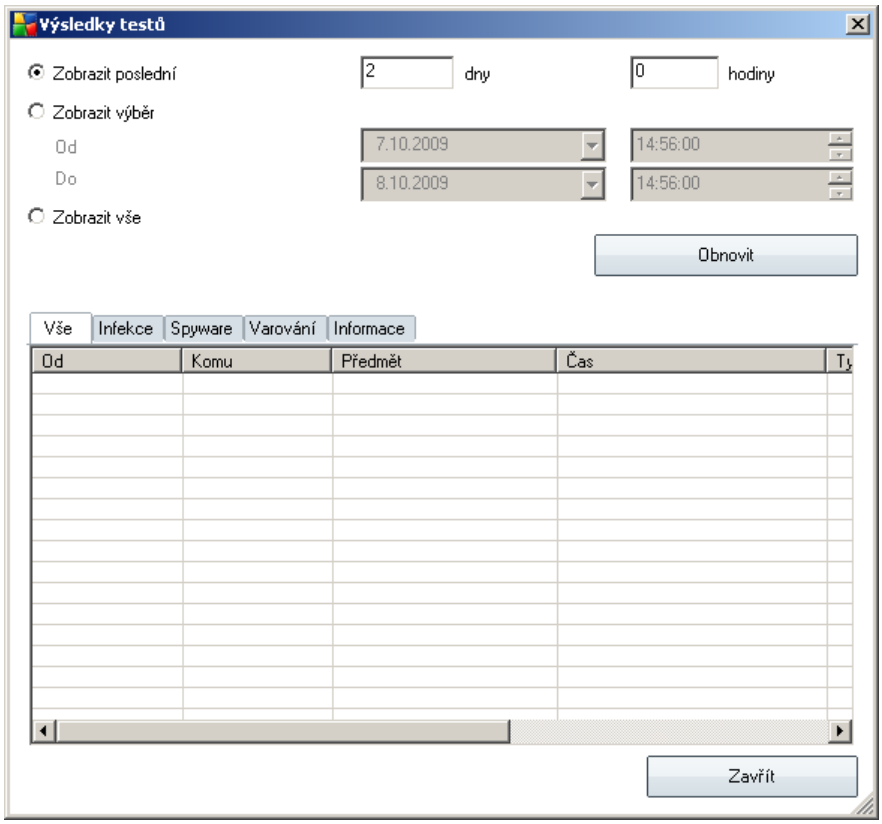
  Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Klikněte dvakrát na požadovanou komponentu pro zobrazení jejího rozhraní. S výjimkou komponenty Anti-Spam sdílejí všechny komponenty společné ovládací prvky:



- ***Výsledky testů***

  Otevře nový dialog s přehledem výsledků testů:



Zde můžete zkontrolovat zprávy rozdělené do několika záložek podle jejich závažnosti. Více informací o konkrétní závažnosti a jejím nastavení naleznete v popisu nastavení jednotlivých serverových komponent.

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit těmito volbami:

- ***Zobrazit poslední*** - vložte preferovaný počet dní a hodin.
- ***Zobrazit výběr*** - zvolte libovolný časový a datumový rozsah.
- ***Zobrazit vše*** - zobrazí výsledky za celé období.

Tlačítkem ***Obnovit*** znovu načtete výsledky testů.

- ***Aktualizovat statistické hodnoty*** - aktualizuje statistiky uvedené v dialogu.
- ***Vynulovat statistické hodnoty*** - vynuluje všechny statistiky.

Funkční tlačítka v dialogu jsou tato:

- ***Nastavení*** - tímto tlačítkem otevřete nastavení dané komponenty.
- ***Zpět*** - tímto tlačítkem se vrátíte zpět na seznam komponent.

Bližší nastavení jednotlivých komponent naleznete v kapitolách níže.

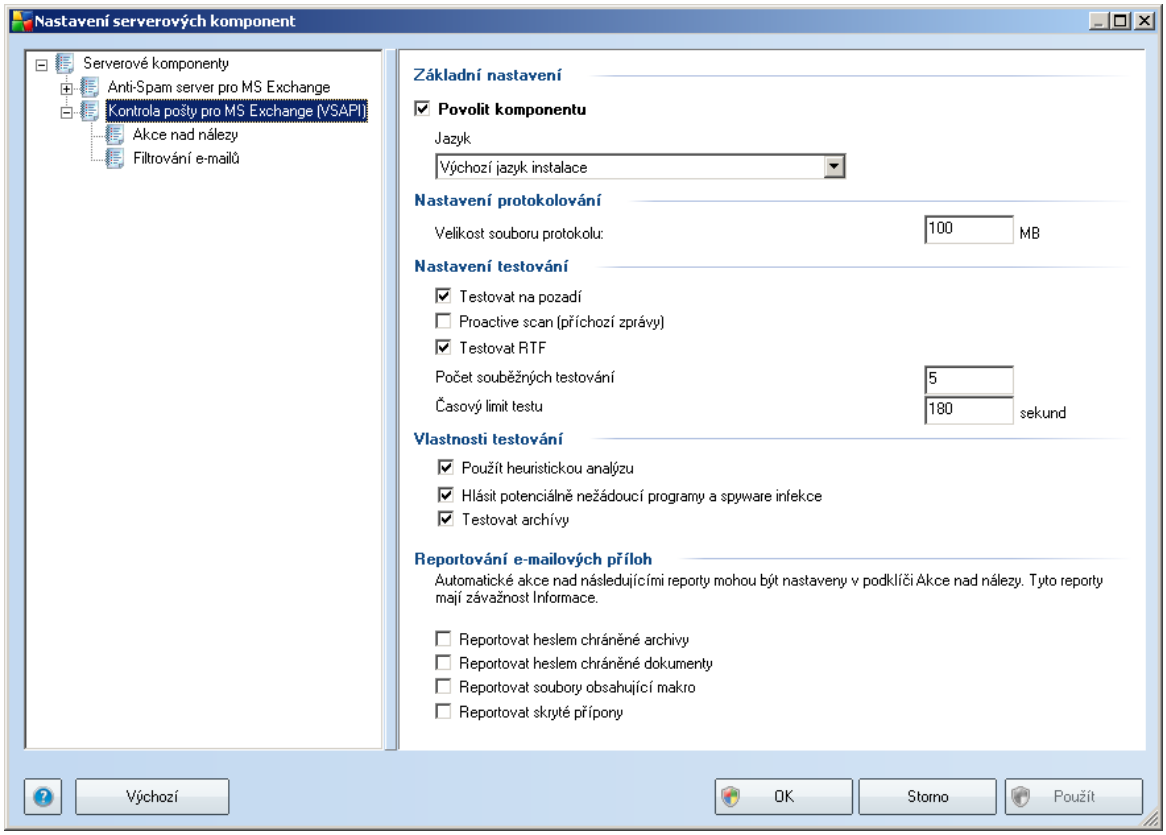
5.2. VSAPI 2.0

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***.

5.3. Kontrola pošty pro MS Exchange (VSAPI)

Tato položka obsahuje možnosti nastavení ***Kontroly pošty pro MS Exchange*** (VSAPI).



V sekci ***Základní nastavení*** naleznete následující možnosti:

- ***Povolit komponentu*** - odškrtněte pro vypnutí celé komponenty.
- ***Jazyk*** - zvolte preferovaný jazyk komponenty.

Sekce ***Nastavení protokolování*** obsahuje tyto volby:

- ***Velikost souboru protokolu*** - zvolte preferovanou velikost protokolovacího souboru. Výchozí hodnota je 100 MB.

Sekce ***Nastavení testování*** obsahuje tato nastavení:

- ***Testovat na pozadí*** - 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 scan*).

- ***Proactive scan (příchozí zprávy)*** - 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. Jakmile jsou zprávy umístěny do úložiště serveru Exchange, jsou zařazeny také do obecné fronty k testování s nízkou prioritou (maximum 30 položek). Následně jsou testovány podle metody FIFO (First in, first out). Pokud je k některé položce zaznamenán přístup zatímco je stále ve frontě, její priorita se změní na vysokou.

  Poznámka: *Nadbytečné zprávy jsou přesunuty do úložiště bez otestování.*

Upozornění: *I v případě, vypnutí obou voleb (**Testování na pozadí** a **Proactive Scan**), zůstává i nadále aktivní rezidentní test, který se spustí v momentě stahování zprávy klientem MS Outlook.*

- ***Testovat RTF*** - zvolte, zdali si přejete testovat také RTF soubory.
- ***Počet souběžných testování*** - ve výchozím nastavení běží testovací proces paralelně ve více vláknech, zejména pro zvýšení obecného výkonu. Počet souběžných vláken lze změnit v tomto nastavení.

  Výchozí počet vláken je vypočítán jako dvojnásobek "počtu procesorů" + 1.

  Minimální počet vláken je vypočítán jako ("počet procesorů" + 1) vyděleno dvěma.

  Maximální počet vláken je vypočítán jako "počet procesorů" krát 5 + 1.

  Pokud je nastavena hodnota nižší nebo minimální, případně maximální či vyšší, je použita hodnota výchozí.

- ***Časový limit testu*** - maximální souvislý interval (*v sekundách*), po který může jedno vlákno přistupovat k právě testovanému objektu (výchozí hodnota je 180 sekund).

Sekce ***Vlastnosti testování*** obsahuje tato nastavení:

- ***Použít heuristickou analýzu*** - zaškrtněte pro povolení použití heuristické analýzy v průběhu testování.
- ***Hlásit potenciálně nežádoucí programy a spyware infekce*** - zaškrtněte pro hlášení potenciálně nežádoucích programů a spyware.
- ***Testovat archívy*** - zaškrtněte pro zahrnutí také testování archivních souborů (zip, rar, atp.)

Sekce ***Reportování e-mailových příloh*** umožňuje vybrat položky, které si přejete hlásit v průběhu testování. Pokud je položka zaškrtnutá, bude každá zpráva s takovou přílohou obsahovat v předmětu text [INFORMACE] (ve výchozím nastavení). Toto výchozí nastavení lze změnit ve větvi ***Akce nad nálezy***, část ***Informace*** (viz níže).

K dispozici jsou následující možnosti:

- ***Reportovat heslem chráněné archivy***
- ***Reportovat heslem chráněné dokumenty***
- ***Reportovat dokumenty obsahující makro***
- ***Reportovat skryté přípony***

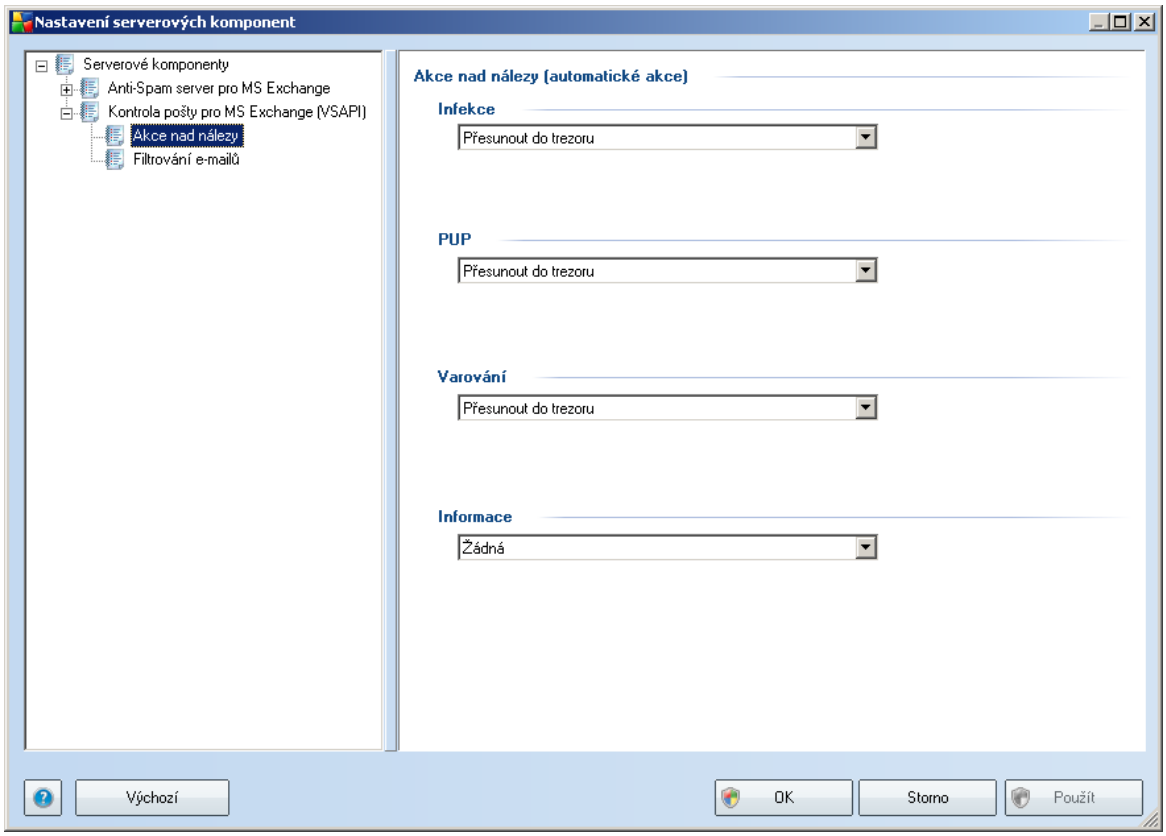
Některé prvky v tomto nastavení tvoří uživatelské rozšíření aplikačního rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- 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
- 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

Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

- ***Akce nad nálezy***
- ***Filtrování e-mailů***

5.4. Akce nad nálezy



V části ***Akce nad nálezy*** lze zaškrtnout a vybrat automatické akce, které mají být provedeny v průběhu testování. Akce jsou k dispozici pro následující položky:

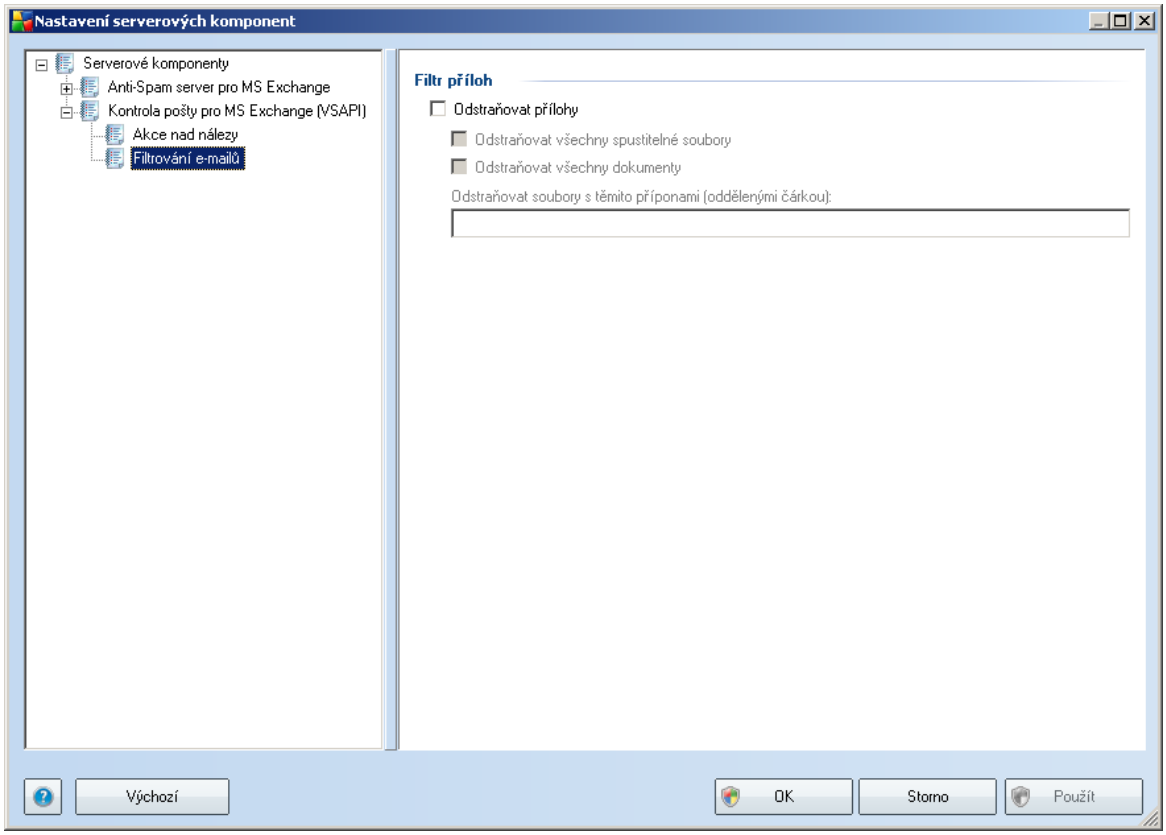
- ***Infekce***
- ***PUP (Potenciálně nežádoucí programy)***
- ***Varování***
- ***Informace***

Z rolovací nabídky zvolte pro každou položku vždy jednu akci:

- ***Žádná*** - nebude provedena žádná akce.
- ***Přesunout do trezoru*** - dané nebezpečí bude přesunuto do Virového trezoru.

- ***Odstranit*** - dané nebezpečí bude odstraněno.

5.5. Filtrování e-mailů



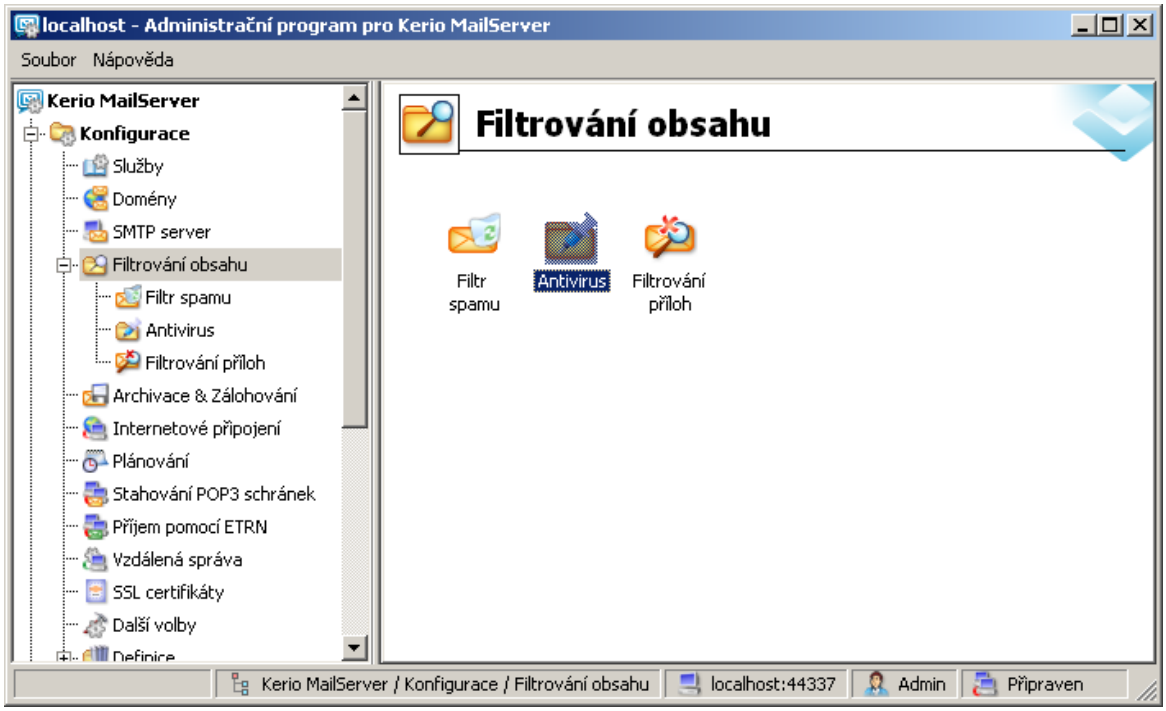
V části ***Filtr příloh*** můžete zvolit přílohy, které mají být automaticky odstraněny. K dispozici jsou následující možnosti:

- ***Odstraňovat přílohy*** - zaškrtněte pro povolení této funkce.
- ***Odstraňovat všechny spustitelné soubory*** - odstraní všechny spustitelné přílohy.
- ***Odstraňovat všechny dokumenty*** - odstraní všechny dokumenty v příloze.
- ***Odstraňovat soubory s těmito příponami (oddělenými čárkou)*** - vložte přípony, které si přejete automaticky odstranit. Hodnoty oddělte čárkou.

6. AVG pro Kerio MailServer

6.1. 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***.

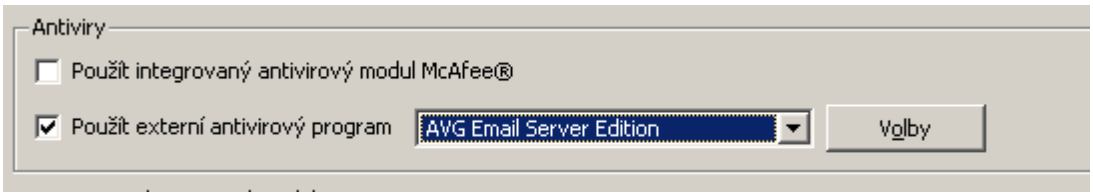


Na hlavním panelu aplikace se zobrazí dialogové okno ***Filtrování obsahu***. V rámci tohoto okna je možné volit ze tří nabídek:

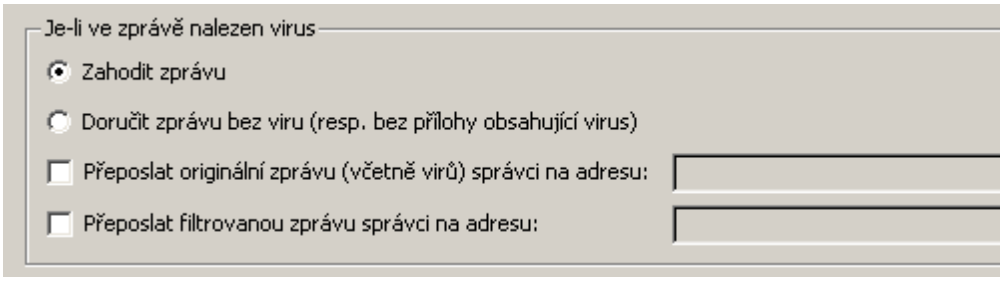
- ***Filtr spamu***
- ***Antivirus***
- ***Filtrování příloh***

6.1.1. 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:

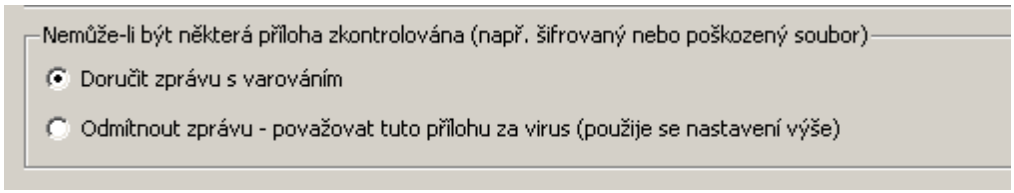


V následující části můžete specifikovat pravidla pro akce provedené v rámci detekce infikované zprávy nebo filtrování příloh:



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.

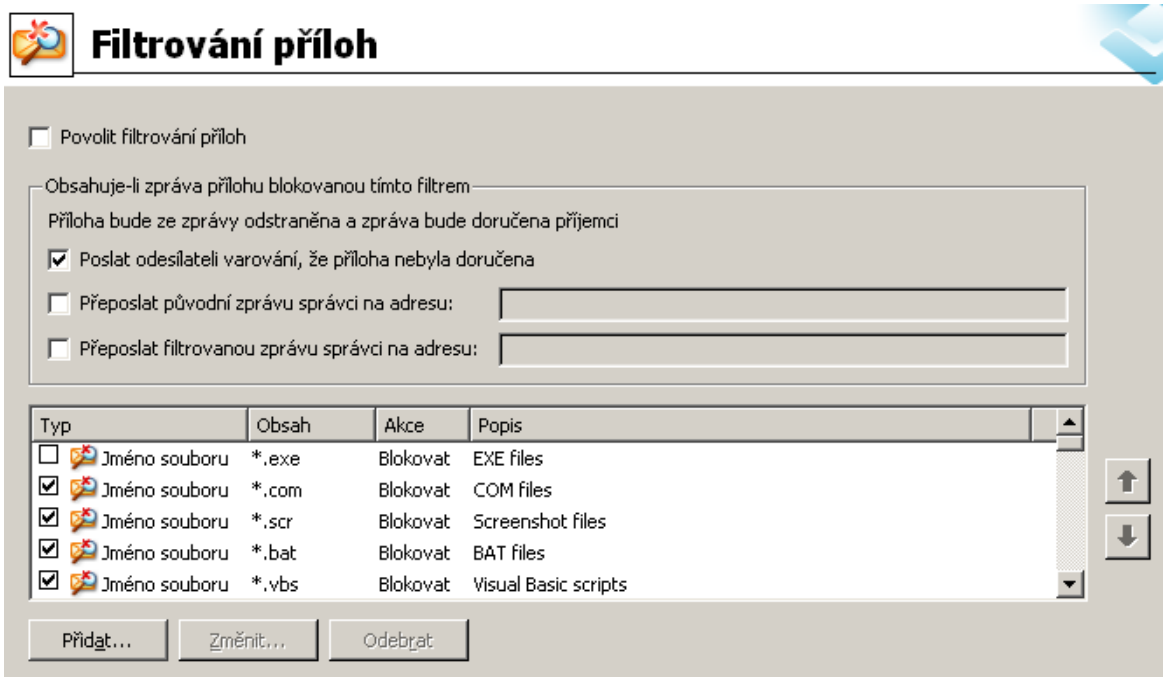


Umožňuje specifikovat akce pro soubory příloh, které nemohou být z jakéhokoli důvodu přečteny a otestovány:

- ***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.

6.1.2. 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:

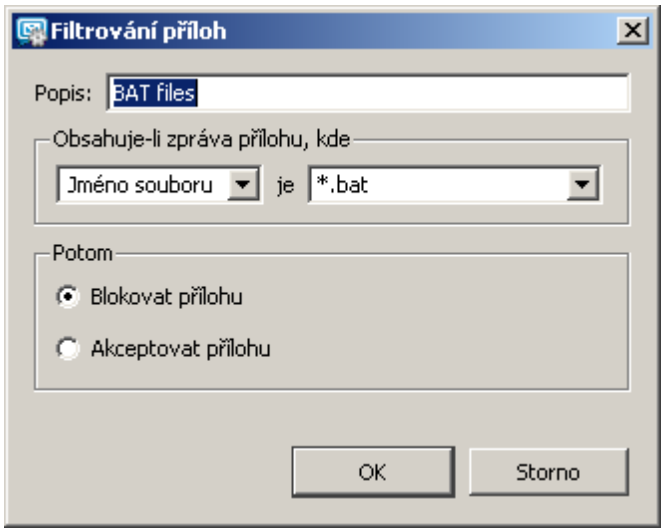
- ***Typ*** – specifikace druhu přílohy dané příponou zadanou v poli ***Obsah***. Možné typy jsou *Jméno souboru* nebo *MIME typ*. V příslušném poli můžete také zahrnout/ vyloučit daný typ přílohy do/z filtru.

- ***Obsah*** – zde můžete definovat příponu filtrovaných příloh. Pro zápis lze využít zástupné znaky 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.

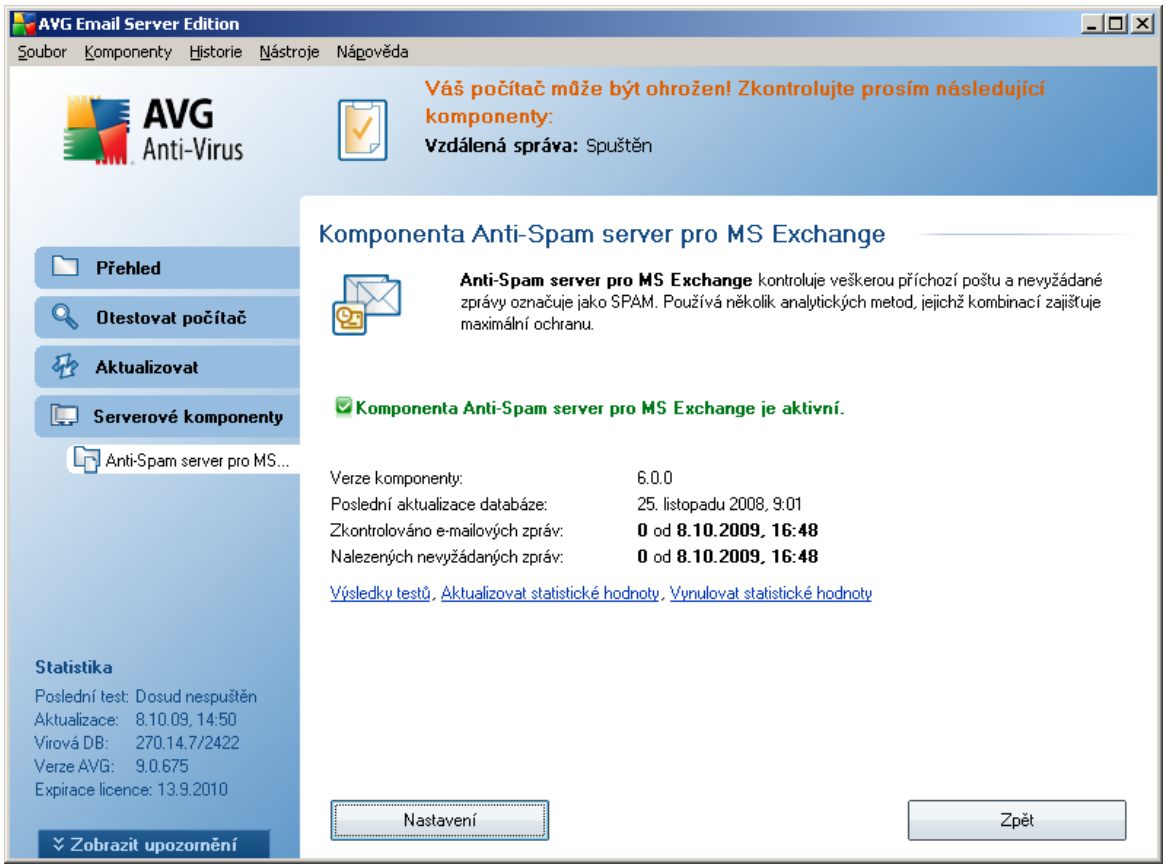
7. Nastavení komponenty Anti-Spam

7.1. 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.

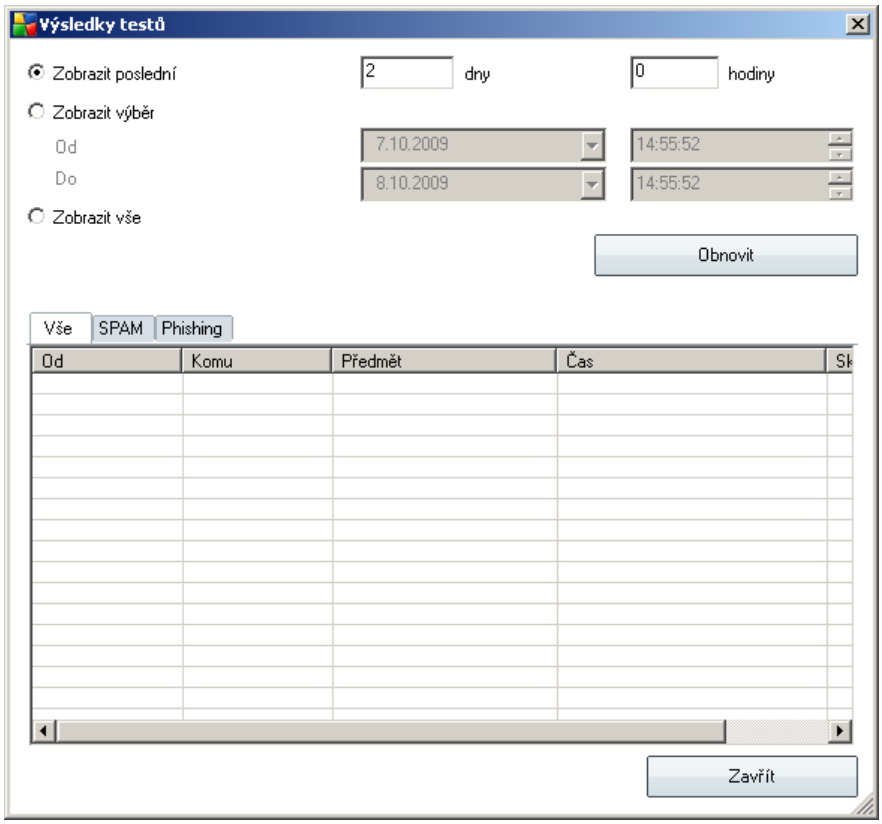
7.2. Anti-Spam rozhraní



V dialogu komponenty Anti-Spam server pro MS Exchange jsou dostupné následující ovládací prvky:

- ***Výsledky testů***

  Otevře nový dialog s přehledem výsledků testů:



Zde můžete zkontrolovat zprávy označené buď jako SPAM (nevyžádaná pošta) nebo pokus o Phishing (zcizení osobních údajů, identity, bankovních údajů atp.).

Ve výchozím nastavení jsou zobrazeny pouze výsledky za poslední dva dny. Interval pro zobrazení můžete změnit těmito volbami:

- ***Zobrazit poslední*** - vložte preferovaný počet dní a hodin.
- ***Zobrazit výběr*** - zvolte libovolný časový a datumový rozsah.
- ***Zobrazit vše*** - zobrazí výsledky za celé období.

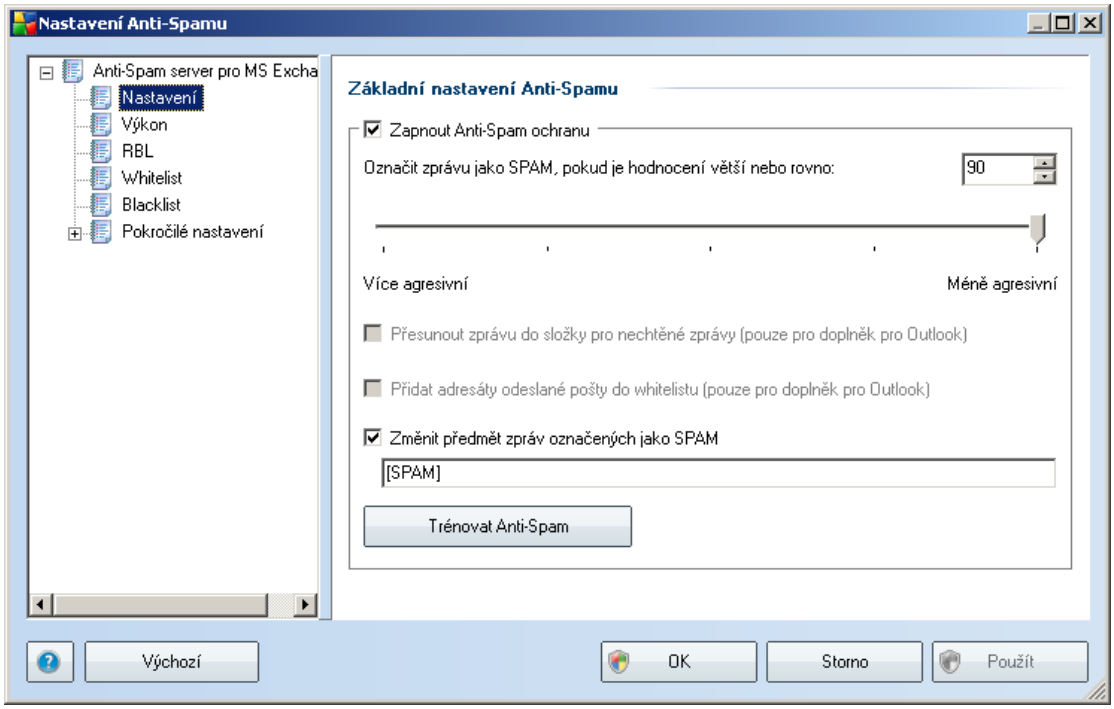
Tlačítkem ***Obnovit*** znovu načtete výsledky testů.

- ***Aktualizovat statistické hodnoty*** - aktualizuje statistiky uvedené v dialogu.
- ***Vynulovat statistické hodnoty*** - vynuluje všechny statistiky.

V rozhraní jsou k dispozici tato ovládací tlačítka:

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

7.3. 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.

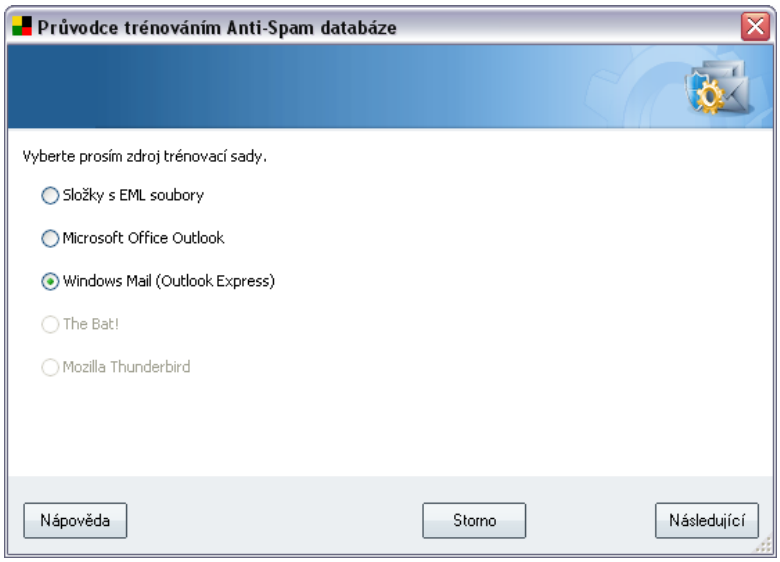
V dialogu ***Nastavení výkonu jádra*** můžete dále nastavit, jak se má zacházet s e-mailovými zprávami pozitivně detekovanými jako spam:

- ***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.

7.3.1. 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.

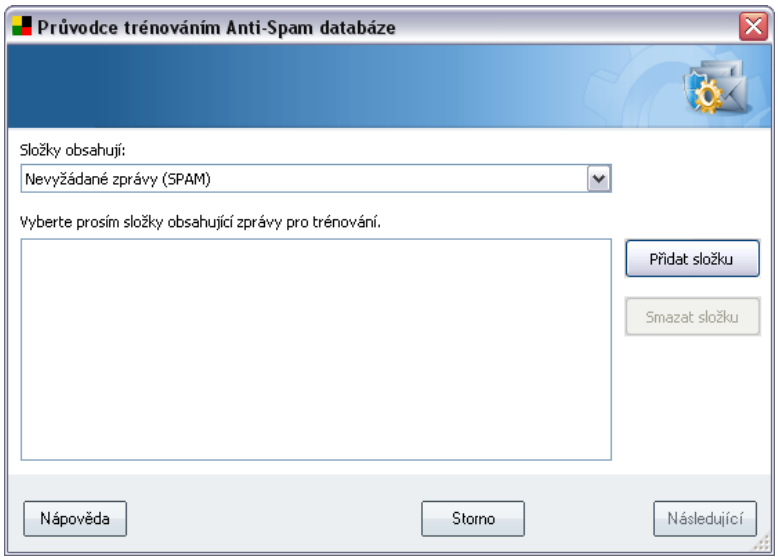
Chcete-li průběh trénování co nejvíce urychlit a zjednodušit, doporučujeme e-mailové zprávy dopředu vytřídit tak, aby ve zvolené složce byly umístěny pouze ty zprávy, které chcete použít pro trénink - žádané a nevyžádané zvlášť. Nicméně není to nutné, protože před zahájením samotného trénování budete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

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

7.3.2. Výběr složky se zprávami

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

Volba složky s EML soubory



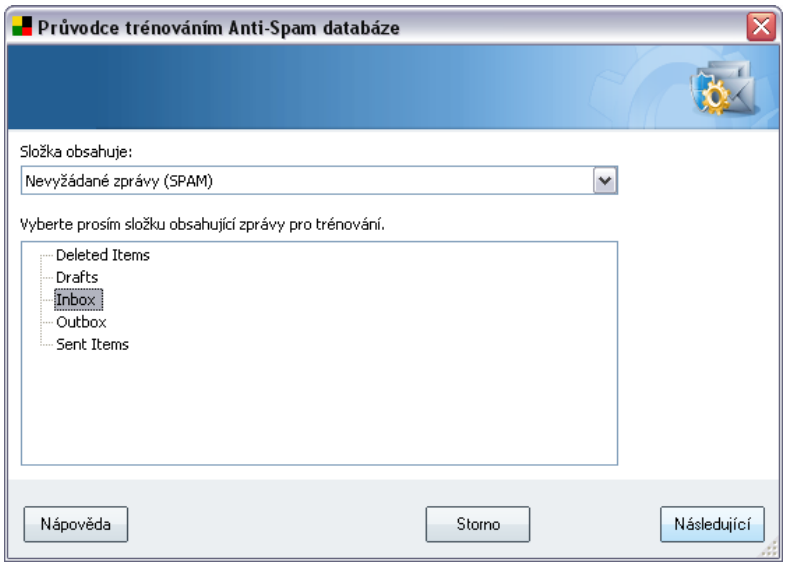
V tomto dialogu volíte složku se zprávami, které chcete pro trénování použít. Stiskněte tlačítko ***Přidat složku*** a určete umístění adresáře s .eml soubory (uloženými e-maily). Cesta k vybranému adresáři pak bude zobrazena v dialogu. Pro odebrání složky ze seznamu použijte tlačítko ***Smazat složku***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

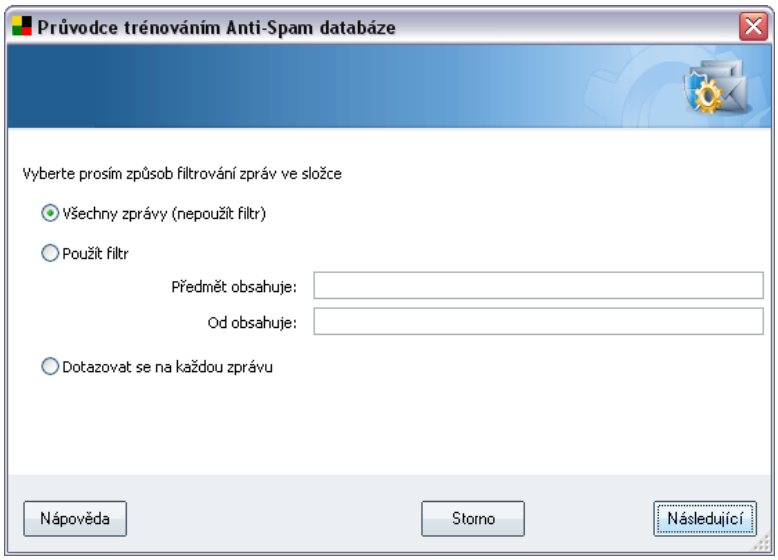


Poznámka: *V případě Microsoft Office Outlook bude nejprve potřeba zvolit MS Office Outlook profil.*

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***.

7.3.3. 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)***.

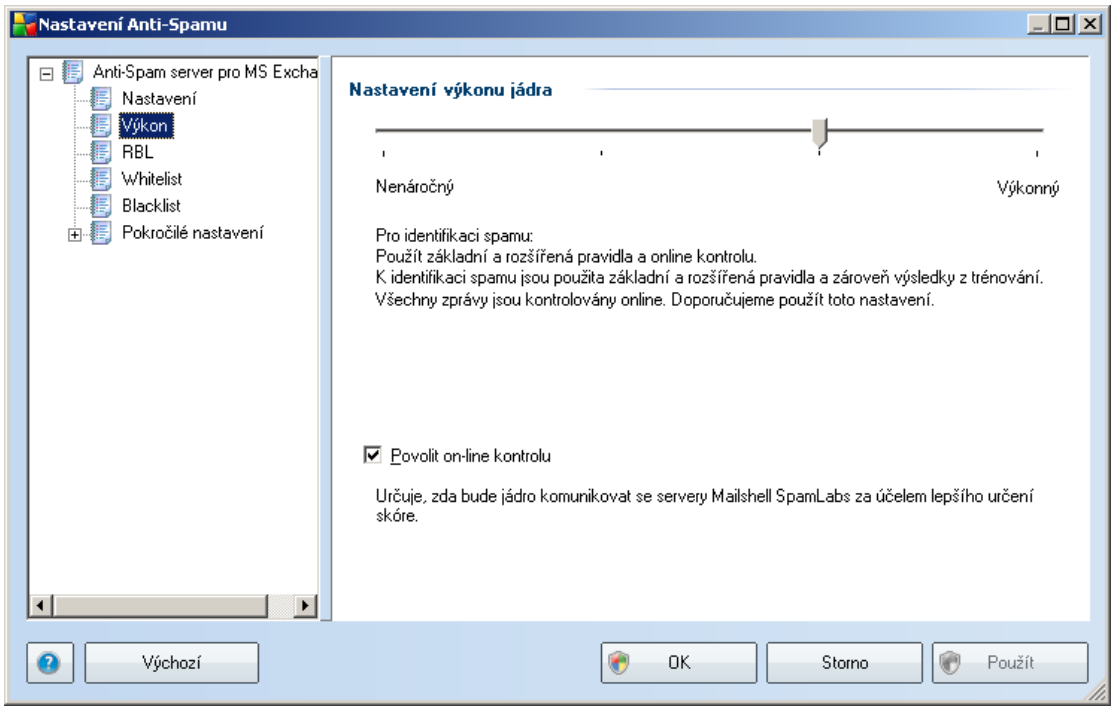
Pokud si nejste jisti, jaké zprávy složka obsahuje, a chcete, aby se průvodce u každé z nich zeptal, zda ji chcete nebo nechcete použít k trénování, pak zvolte možnost ***Dotazovat se na každou zprávu***.

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.

7.4. 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.

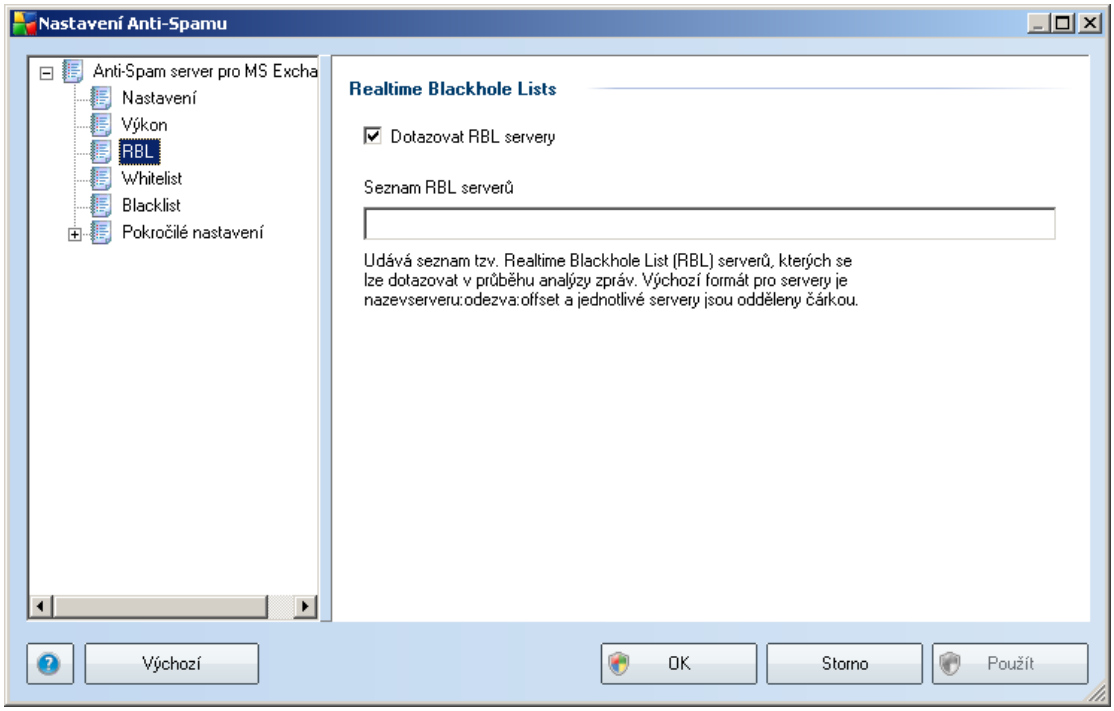
- ***Nenáročný režim*** znamená, že během testovacího procesu nebudou k identifikaci spamu použita žádná pravidla. Identifikace spamu bude založena výhradně na porovnání s testovacími daty. Tento režim pro běžné používání nedoporučujeme, nastavení lze doporučit výhradně u počítačů s velmi nízkou úrovní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

7.5. 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.

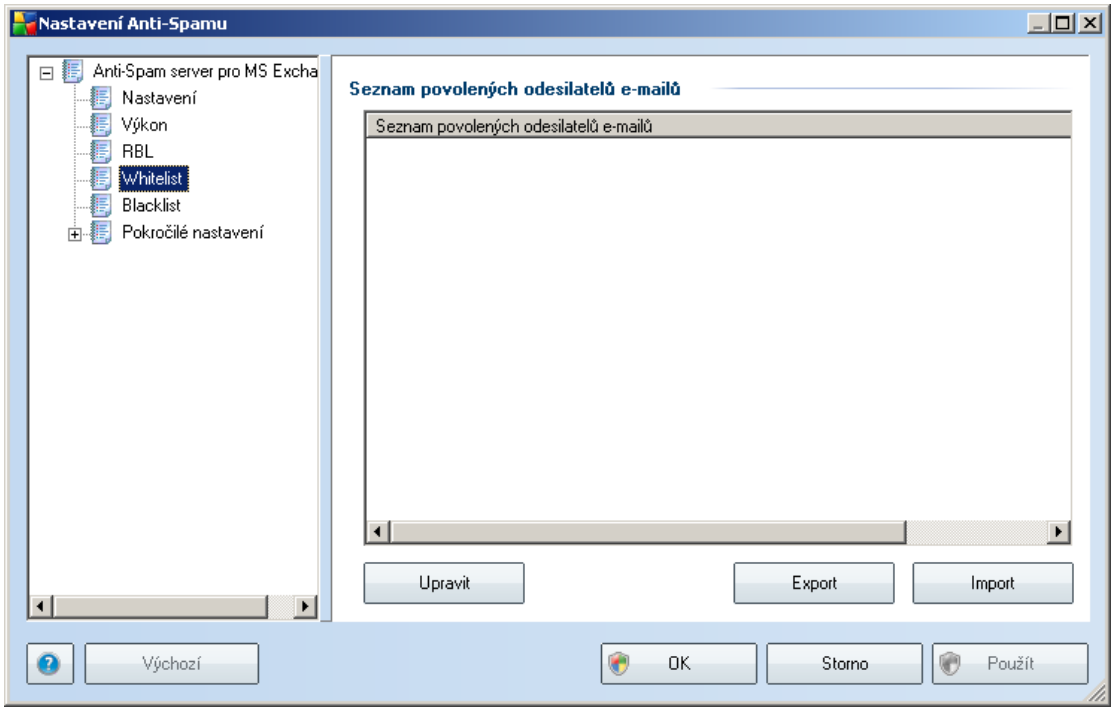
Položka ***Seznam RBL serverů*** vám dále umožní nastavit adresy konkrétních serverů, na nichž jsou tyto spamové databáze umístěny. Ve výchozím nastavení budou zprávy kontrolovány proti databázím na dvou RBL serverech. Doporučujeme ponechat toto nastavení, pokud nemáte skutečný důvod jej měnit - editace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

7.6. 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:

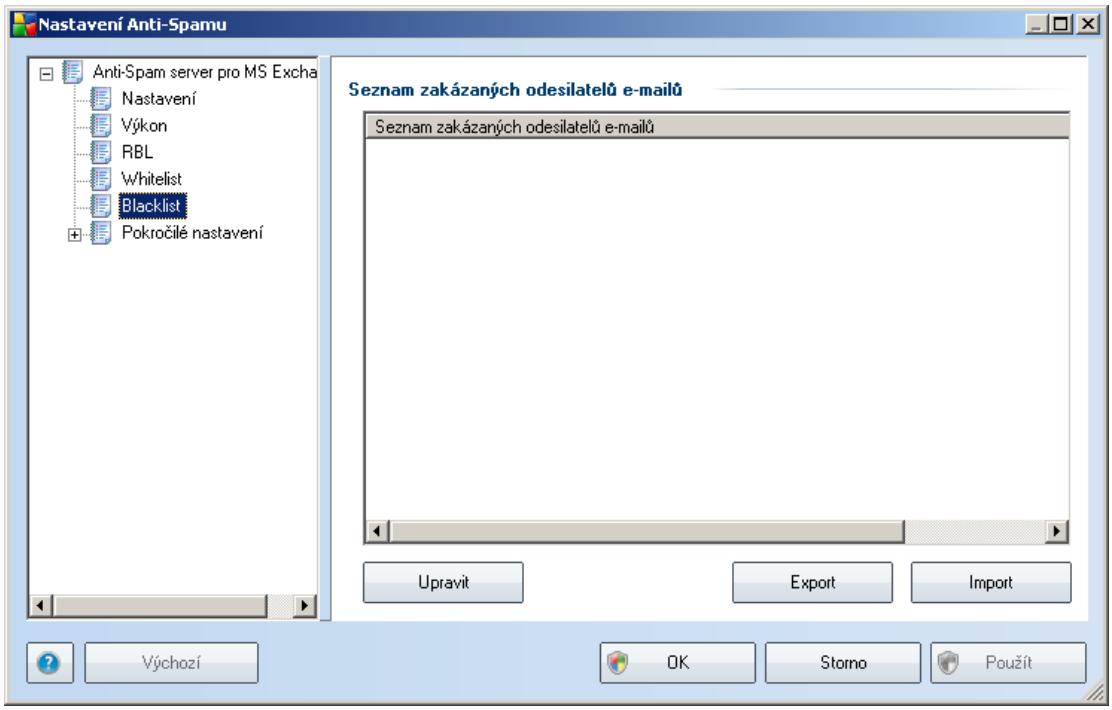
- ***Upravit*** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázově metodu *"kopírovat a vložit"*). Adresy/doménová jména vkládejte po jednom na každý řádek.

- ***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.

7.7. 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.

7.8. 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:

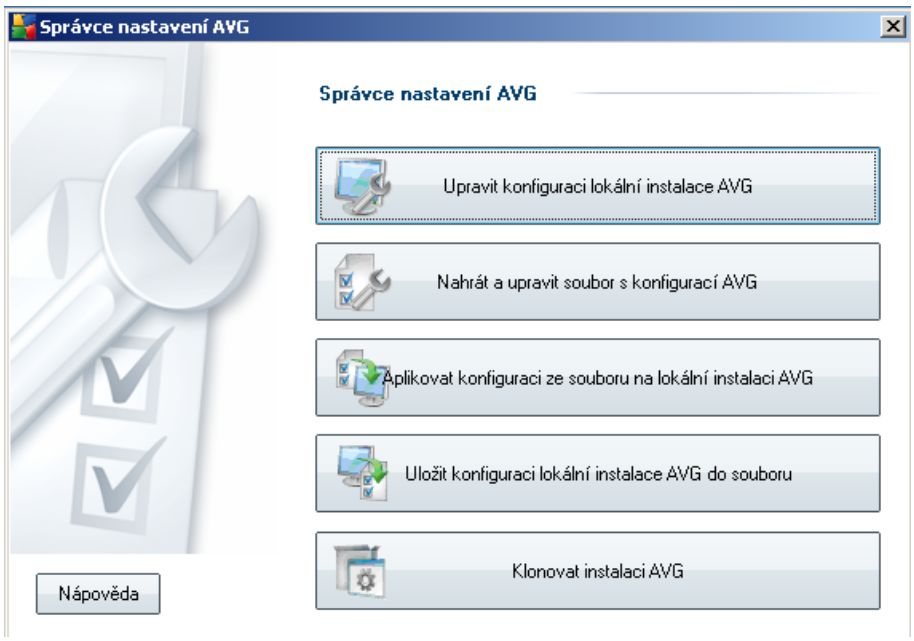
- ***Paměť*** - fingerprint, reputace domén, LegitRepute
- ***Trénování*** - slovní nastavení, historie skóre, vyrovnávání skóre, počet slovních záznamů, práh pro samotrénování, váha, zápisový buffer
- ***Filtrování*** - seznam jazyků, seznam zemí, povolené IP adresy, blokované IP adresy, blokované země,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

8. Správce nastavení AVG

Správce nastavení AVG je nástroj určený zejména pro menší sítě. Umožňuje kopírovat, upravovat a distribuovat konfiguraci AVG, kterou lze následně uložit na přenosné médium (např. USB flash disk) a aplikovat ručně na vybrané stanice.

Tento nástroj je volitelnou součástí instalace AVG a lze jej spustit z Windows nabídky Start skrze:

Všechny programy/AVG 9.0/Správce nastavení AVG



- ***Upravit konfiguraci lokální instalace AVG***

  Otevře dialog pokročilého nastavení vaší lokální instalace AVG. Všechny změny provedené v tomto dialogu se projeví v lokální instalaci AVG.

- ***Nahrát a upravit soubor s konfigurací AVG***

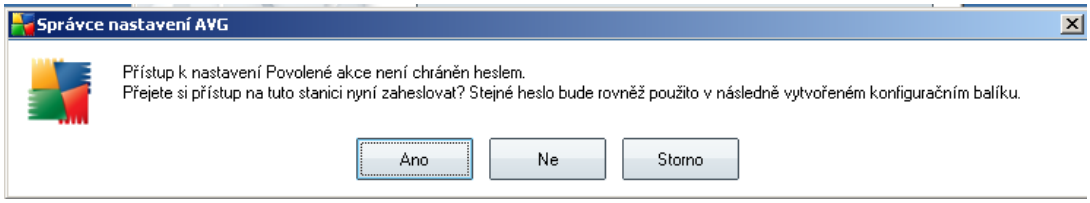
  Pokud již máte k dispozici dříve uložený soubor s konfigurací AVG (.pck), použijte toto tlačítko pro jeho otevření a následné úpravy. Otevře se opět dialog pokročilého nastavení AVG a provedené změny budou po stisku tlačítka ***OK*** nebo ***Použít***, uloženy do původního souboru.

- ***Aplikovat konfiguraci ze souboru na lokální instalaci AVG***

Tímto tlačítkem lze otevřít soubor s konfigurací AVG (.pck) a aplikovat jej na lokální instalaci AVG.

- ***Uložit konfiguraci lokální instalace AVG do souboru***

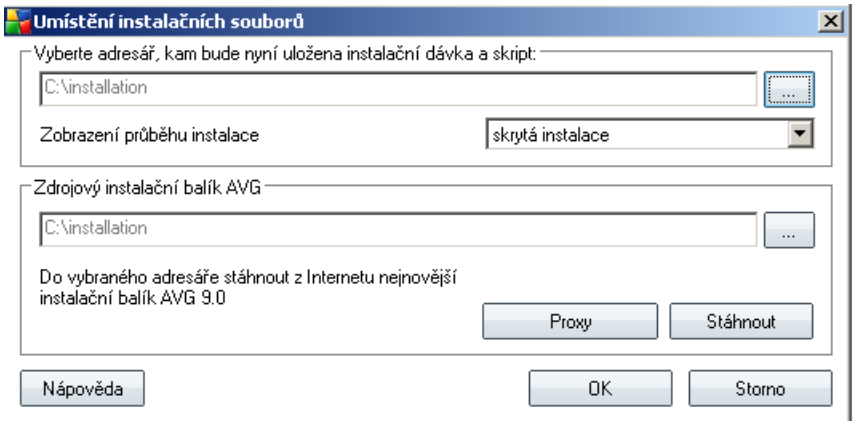
  Použijte toto tlačítko k uložení konfigurace místní instalace AVG do souboru (.pck). Pokud jste nenastavili heslo pro Povolené akce, zobrazí se následující dialog:



  Zvolte ***Ano***, pokud si nyní přejete nastavit heslo pro přístup k Povoleným položkám. Tlačítkem ***Ne*** vytvoření hesla přeskočíte a budete moci pokračovat v uložení konfigurace do souboru.

- ***Klonovat instalaci AVG***

  Tato volba umožňuje vytvořit instalační balík se stejným nastavením, jako má místní instalace AVG. Nejprve zvolte složku, do které si přejete instalační skript uložit:



  Z rolovací nabídky zvolte jednu z možností:

  - ***Skrytá instalace*** - na stanici nebude aktuálně přihlášenému uživateli zobrazeno žádné informační okno týkající se procesu instalace.

- ***Zobrazení průběhu instalace*** - instalace nebude vyžadovat žádnou interakci uživatele, nicméně bude moci průběh instalace sledovat.

- ***Zobrazit průvodce instalací*** - instalační průvodce bude na stanici viditelný a aktuálně přihlášený uživatel bude muset potvrdit všechny kroky ručně.

Tlačítkem ***Stáhnout*** lze spustit stahování nejnovějšího instalačního balíku AVG přímo ze stránek výrobce do vybraného adresáře. Alternativně můžete do zvolené složky instalační balík nakopírovat ručně.

Pro nastavení proxy serveru pro připojení k síti zvolte tlačítko ***Proxy*** a vyplňte požadované údaje.

Kliknutím na tlačítko ***OK*** zahájíte proces klonování instalace. Před zahájením se může zobrazit opět dialog pro zadání hesla pro přístup k povoleným položkám (viz výše). Jakmile proces skončí, ve zvoleném adresáři by se měl nacházet mj. také soubor ***AvgSetup.bat***. Spuštěním tohoto souboru dojde k instalaci AVG s vybraným nastavením.

9. FAQ a technická podpora

V případě problémů s AVG se pokuste vyhledat řešení na webu AVG (http://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***.