AVG E-mail Server Edice

Uživatelský manuál

Verze dokumentace 2013.09 (12/2/2013)

Obsah

1. Úvod

Tento uživatelský manuál je kompletní dokumentací programu ***AVG E-mail Server***.

AVG E-mail Server je jedním z produktů nové řady oceňovaného bezpečnostního software AVG, jež byl navržen pro klid vaší duše a stoprocentní bezpečnost vašeho serveru. Stejně jako všechny produkty nové řady AVG byl i ***AVG E-mail 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 E-mail 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 E-mail 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 E-mail Server je určen k ochraně e-mail serverů s těmito operačními systémy:

- Windows 2012 Server R2
- Windows 2012 Server (x64 a x86)
- Windows 2008 Server R2
- Windows 2008 Server (x64 a x86)
- Windows 2003 Server (x86, x64) SP1

2.2. Podporované e-mail servery

Podporovány jsou následující e-mail servery:

- MS Exchange Server 2003
- MS Exchange Server 2007
- MS Exchange Server 2010
- MS Exchange Server 2013
- Kerio MailServer – verze 6.7.2 a vyšší

2.3. Hardwarové požadavky

Minimální hardwarové požadavky pro ***AVG E-mail 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 E-mail 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 E-mail Serveru***, je nutné ji před zahájením instalace ***AVG E-mail Server*** odinstalovat. Odinstalaci je třeba provést ručně pomocí standardních funkcí Windows:

- V nabídce ***Start/Nastavení/Ovládací panel/Přidat nebo odebrat programy*** zvolte příslušný program (totéž lze také snadno provést z nabídky ***Start/Programy/AVG/Odinstalovat AVG***).

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

  Poznámka: *Při procesu odinstalace bude restartován proces store.*

  Doplněk pro Exchange - spusťe setupes.exe s parametrem /uninstall ze složky, kde je doplněk nainstalován:

  např. C:\AVG4ES2K\setupes.exe /uninstall

  Doplněk pro Lotus Domino/Notes - spusťe setupln.exe s parametrem /uninstall ze složky, kde je doplněk nainstalován:

  např. C:\AVG4LN\setupln.exe /uninstall

2.5. Servisní balíčky pro MS Exchange

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/en-us/download/details.aspx?id=9664

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

Servisní balík pro MS Exchange 2010 Server (instalace je volitelná):

http://www.microsoft.com/en-us/download/details.aspx?id=28190

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.

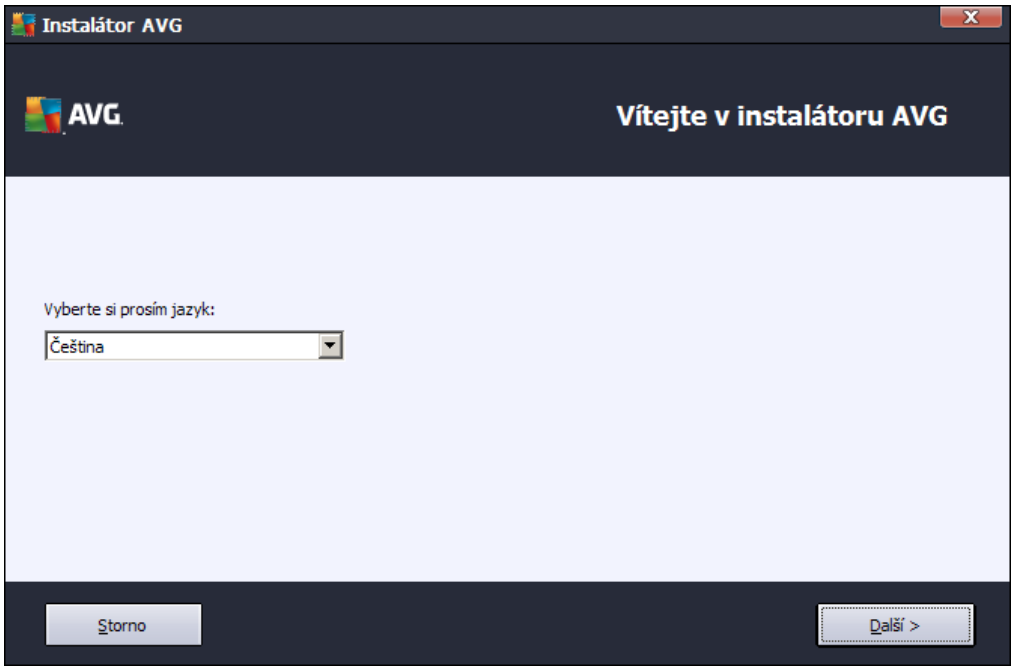
Doporučujeme vám proto navštívit web AVG: http://www.avg.cz/stahnout?prd=msw a nejnovější instalační soubor si odtud stáhnout.

K dispozici jsou dva instalační balíčky - jeden pro 32bitové operační systémy (s označením x86) a jeden pro 64bitové operační systémy (s označením x64). Při instalaci je tedy potřeba použít instalační balíček odpovídající vašemu operačnímu systému.

Během instalace budete požádáni o své licenční číslo. Ujistěte se proto prosím, že jej máte k dispozici. 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:

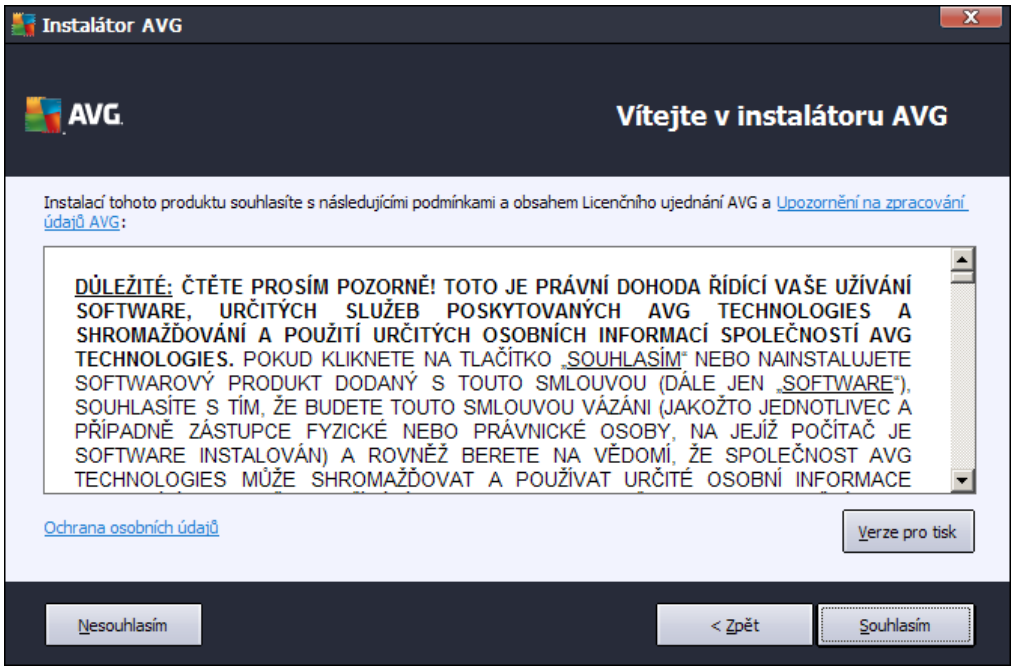
3.1. Spuštění instalace



Instalační proces je zahájen otevřením uvítacího dialogu. V něm máte možnost zvolit jazyk, v němž bude instalační proces probíhat. Do následující části procesu přejdete stiskem tlačítka ***Další***.

Později v průběhu instalace si budete také moci zvolit další jazyky pro rozhraní aplikace.

3.2. Licenční ujednání

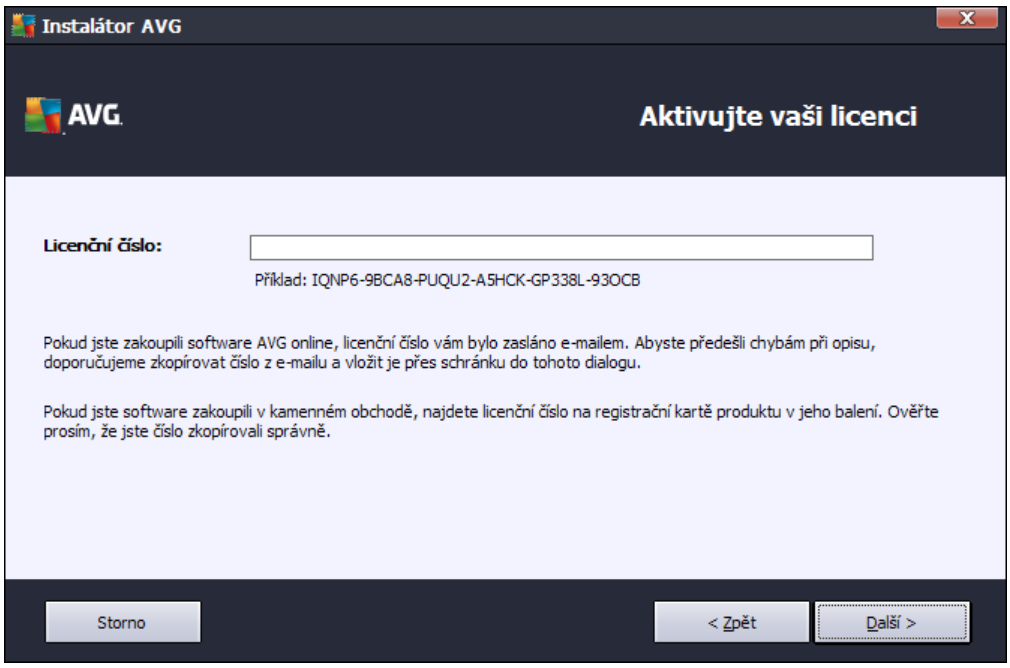


V tomto dialogu se nachází Licenční ujednání - tedy plné znění závazné licenční smlouvy AVG. Text si přečtěte a svůj souhlas s licenčním ujednáním potvrďte stiskem tlačítka ***Souhlasím***.

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

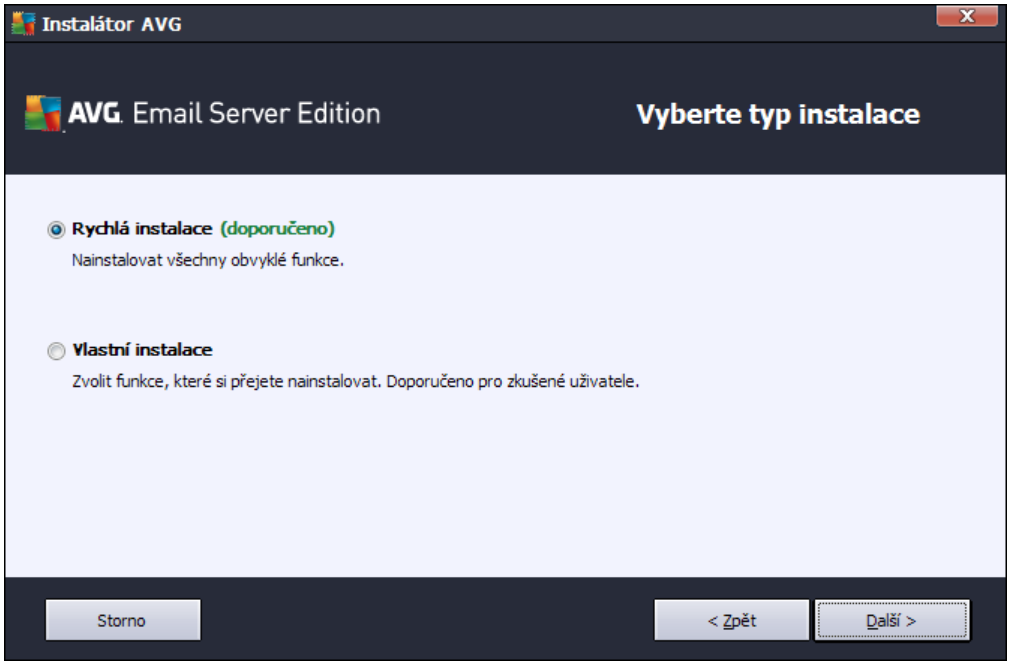
3.3. Aktivujte vaši licenci

V dialogu ***Aktivujte vaši licenci*** je třeba vyplnit vaše licenční číslo. Toto číslo najdete buďto na registrační kartě v krabicovém balení AVG, anebo v potvrzovacím e-mailu, 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***.

3.4. Zvolte typ instalace



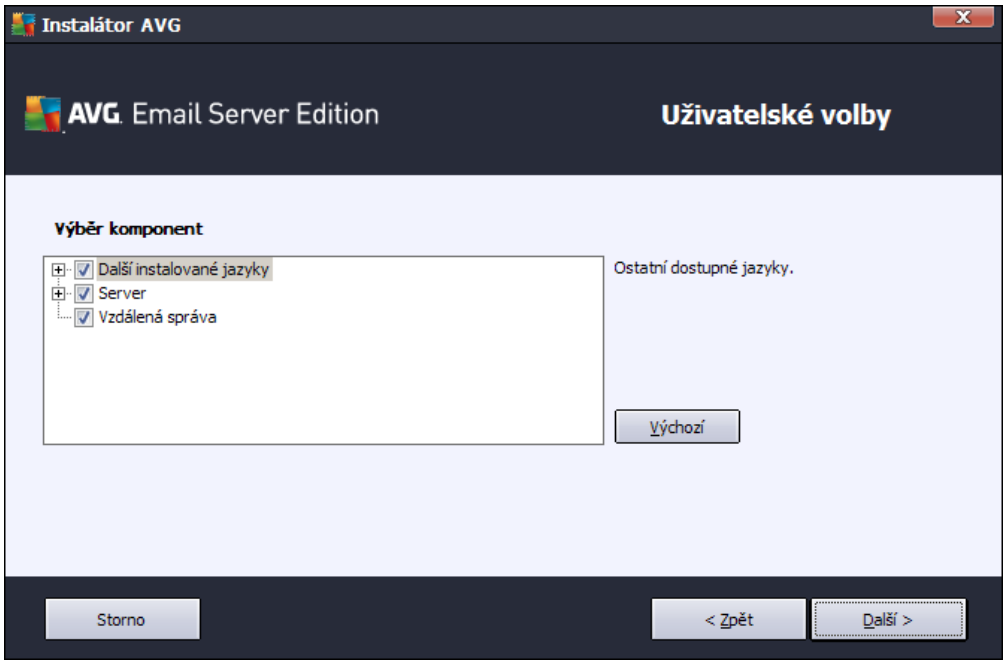
Dialog ***Vyberte typ instalace*** vám dává na výběr mezi ***Expresní*** a ***Uživatelskou*** instalací.

Většině uživatelů doporučujeme použít ***expresní 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.

Po zvolení Uživatelské instalace se ve spodní části dialogu zobrazí sekce ***Cílové umístění***. Ta vám umožní zvolit, kam má být program AVG nainstalován. 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.

3.5. Uživatelská instalace - uživatelské volby



V sekci ***Výběr 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!

- ***Vzdálená správa*** - pokud budete chtít tuto instalaci spravovat vzdáleně, zaškrtněte tuto volbu.
- ***Další instalované jazyky*** - zvolte si jazyky uživatelského rozhraní, které chcete nainstalovat.

Základní přehled jednotlivých serverových komponent (doplňků):

- ***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.

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

  Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange (lze nainstalovat na EDGE i HUB roli).

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

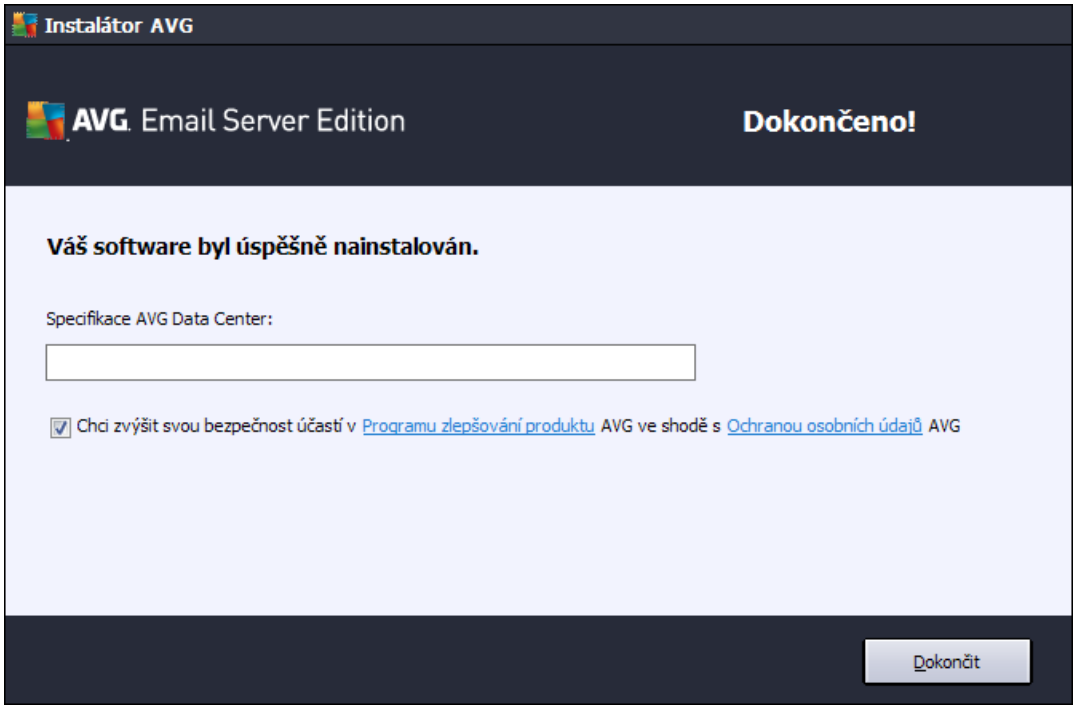
  Kontroluje e-mailové zprávy uložené v uživatelských schránkách. Při nalezení viru dojde k přesunu do virového trezoru nebo kompletnímu odstranění.

Pro MS Exchange 2003 jsou k dispozici pouze komponenty Anti-Spam a Kontrola pošty (VSAPI).

Pokračujte stiskem tlačítka ***Další***.

3.6. Dokončení instalace

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



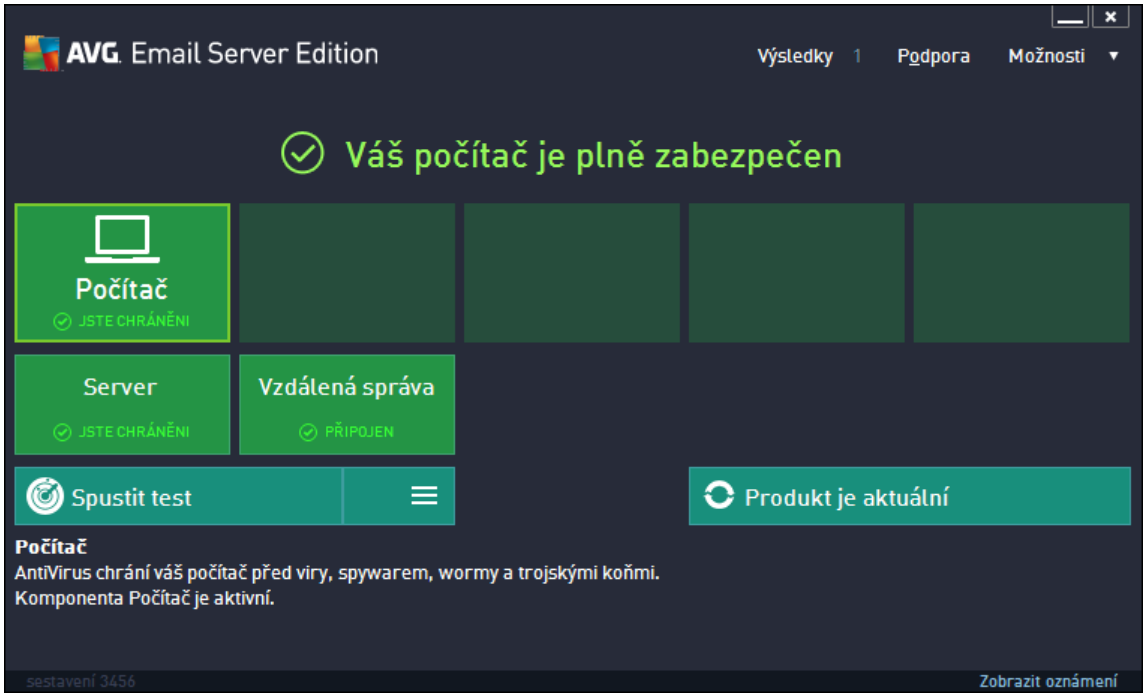
Ve výchozím nastavení je zaškrtnuta také volba ***Chci zvýšit svou bezpečnost účastí v AVG Product Improvement Program ve shodě s AVG Privacy Policy***. Označením této volby dáváte najevo svůj souhlas s účastí v Programu zlepšování produktu (a umožníte tak reportování informací o detekovaných hrozbách týmu expertů společnosti AVG). V rámci tohoto programu probíhá sběr anonymních informací o detekovaných hrozbách s cílem zvýšit celkovou úroveň bezpečnosti na Internetu.

Své volby potvrďte stiskem tlačítka ***Dokončit***.

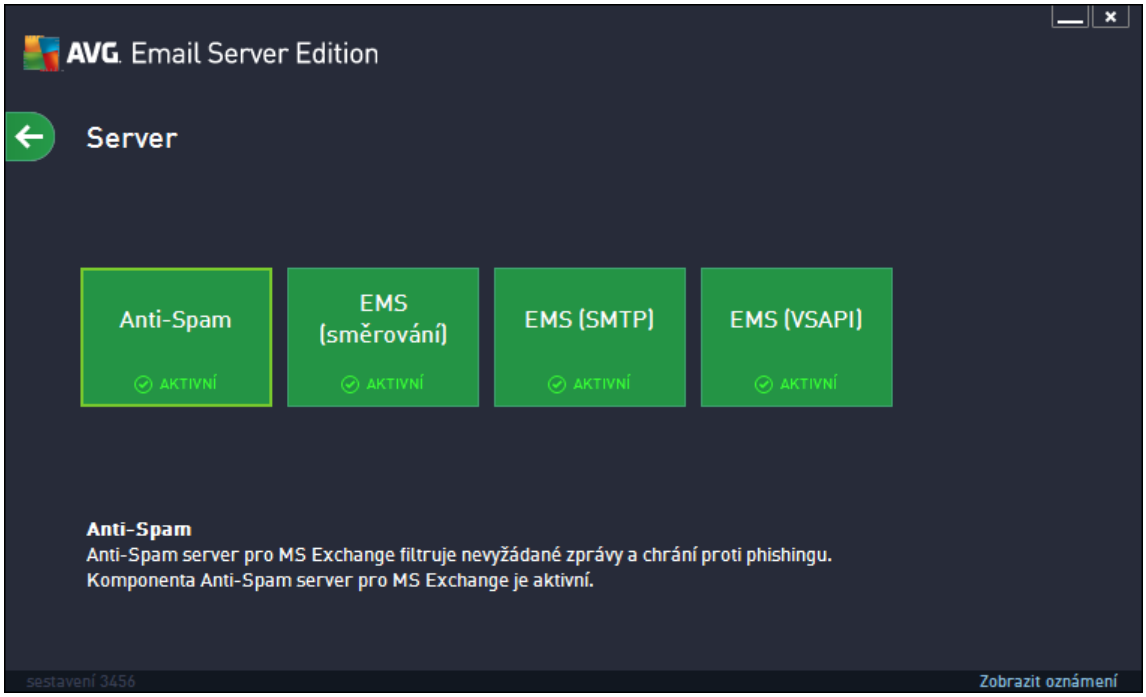
Program AVG je nyní nainstalován na vašem počítači/serveru a plně funkční. Program běží ve výchozím nastavení na pozadí a nevyžaduje vaši pozornost.

4. Po instalaci

Ihned po skončení instalace se objeví hlavní obrazovka ***AVG E-mail Server***:



Tento manuál se věnuje pouze těm bezpečnostním prvkům, které jsou unikátní v rámci ***AVG E-mail Server***; všechny ostatní komponenty a možnosti nastavení jsou podrobně popsány v manuálu pro AVG Desktop. Pro zobrazení hlavního dialogu serverových komponent (jakéhosi rozcestníku) klikněte na tlačítko ***Server***. Objeví se před vámi následující obrazovka:



Upozorňujeme, že všechny serverové komponenty (samozřejmě jen pokud jste předtím některou z nich sami neodebrali z instalace) budou dostupné pouze v tom případě, že používáte MS Exchange verze 2007 či novější. MS Exchange 2003 podporuje výhradně komponenty Anti-Spam a Kontrola pošty (VSAPI).

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

- ***Komponenty Kontroly pošty pro MS Exchange***
- ***Anti-Spam Server pro MS Exchange***
- ***AVG pro Kerio MailServer***

5. Komponenty Kontroly pošty pro MS Exchange

5.1. Přehled

Základní přehled jednotlivých komponent Kontroly pošty:

- ***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 2007/2010/2013 a lze nainstalovat pouze na HUB roli.

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

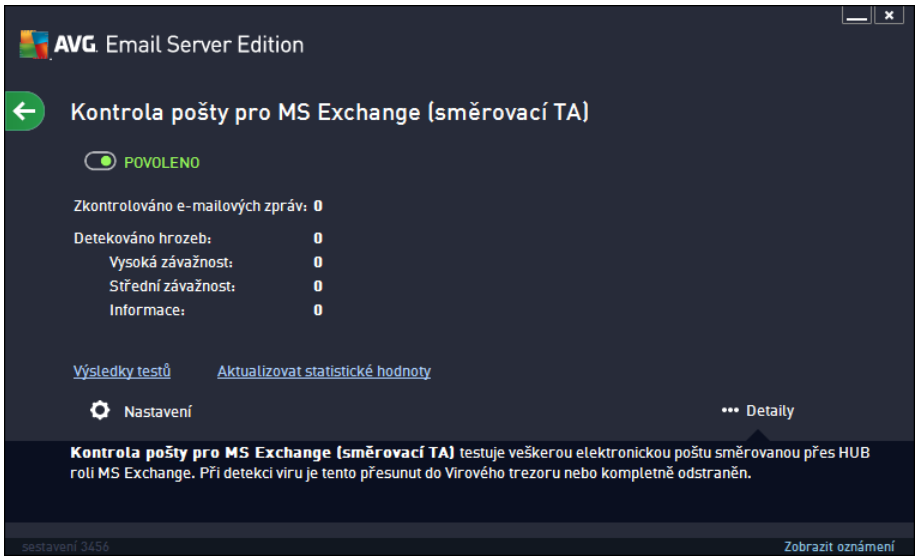
  Kontroluje e-mailové zprávy procházející skrze SMTP rozhraní MS Exchange.

  Dostupné pouze pro MS Exchange 2007/2010/2013 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.

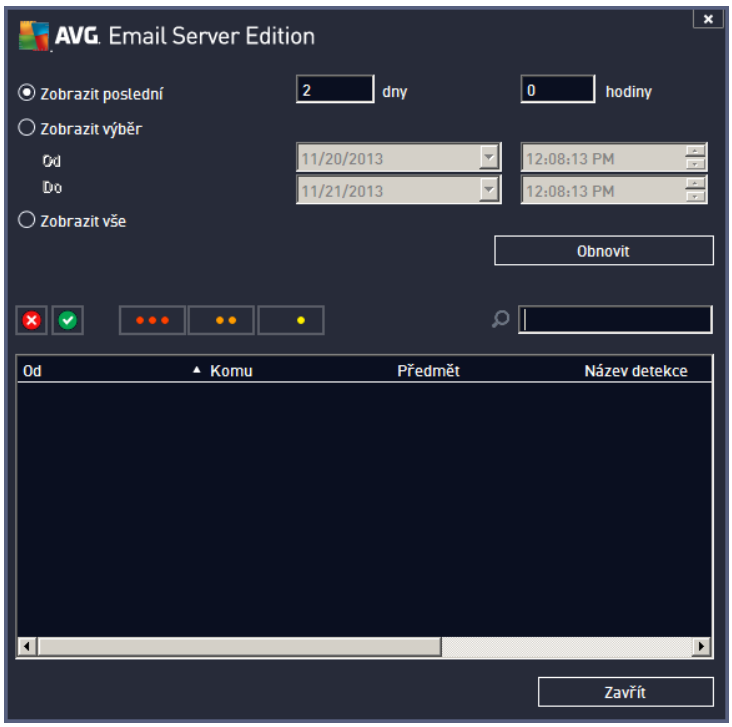
Kliknutím myši na ikonu požadované komponenty zobrazíte její rozhraní. Všechny komponenty Kontroly pošty sdílejí společné ovládací prvky:



- ***POVOLENO/ZAKÁZÁNO*** - kliknutí na toto tlačítko vypíná a zapíná danou komponentu (je-li komponenta zapnutá, jsou tlačítko i text zelené, je-li vypnutá, zobrazují se červeně).

- ***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.

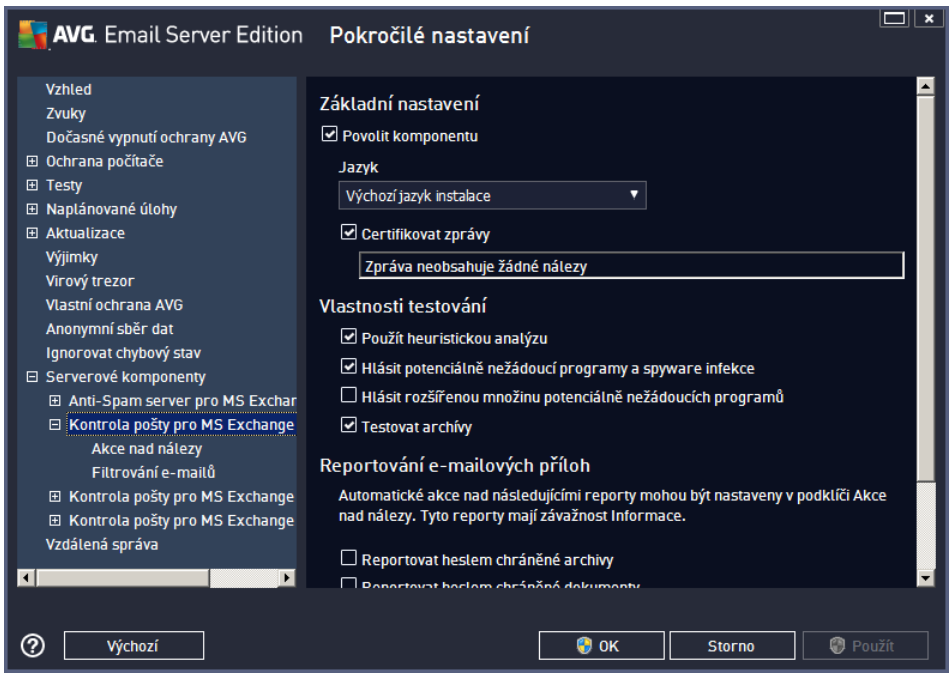
- ***Aktualizovat statistické hodnoty*** - aktualizuje statistiky uvedené v dialogu.

Stiskem funkčního tlačítka ***Nastavení*** otevřete nastavení dané komponenty (bližší nastavení jednotlivých komponent naleznete v kapitolách níže).

5.2. Kontrola pošty pro MS Exchange (směrovací TA)

Pro otevření možností nastavení komponenty ***Kontrola pošty pro MS Exchange (směrovací transportní agent)***, klikněte v jejím rozhraní na tlačítko **Nastavení**.

V seznamu ***Serverových komponent*** pak zvolte položku ***Kontrola pošty pro MS Exchange (směrovací TA)***.



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 ***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.
- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtěžující programy (různé doplňky do prohlížeče atd.). Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je doplňkem předchozí možnosti, samostatně tedy není dostačující: pokud chcete ochranu před základními typy spyware, pak ponechte vždy označené předchozí políčko, a toto pak označte volitelně k němu.
- ***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***

5.3. 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.

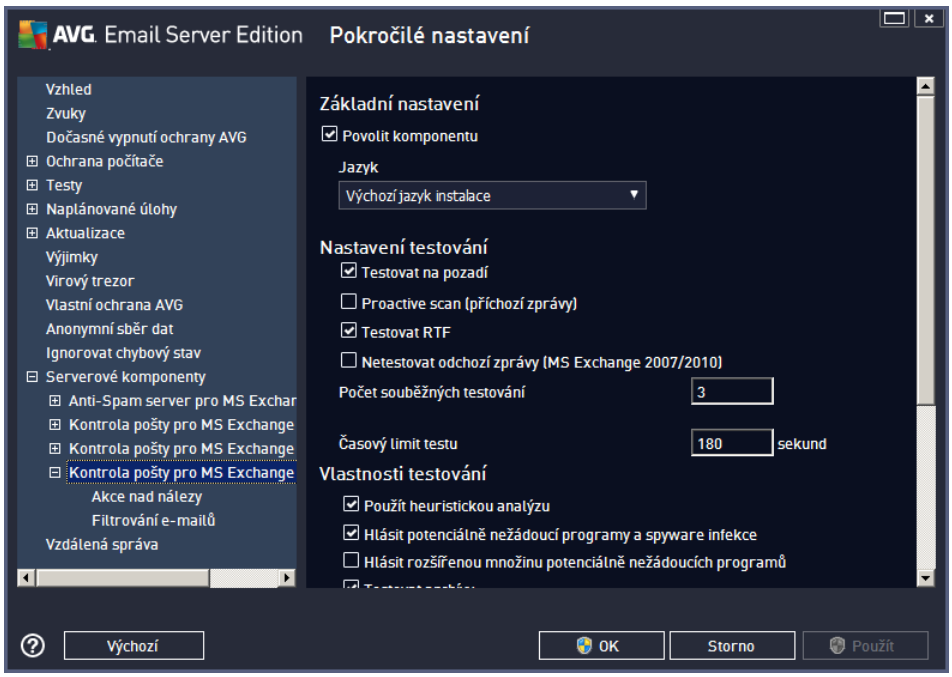
Součástí nastavení jsou také tyto podpoložky ve stromové struktuře:

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

5.4. Kontrola pošty pro MS Exchange (VSAPI)

Pro otevření možností nastavení komponenty ***Kontrola pošty pro MS Exchange (VSAPI)***, klikněte v jejím rozhraní na tlačítko **Nastavení**.

V seznamu ***Serverových komponent*** pak zvolte položku ***Kontrola 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 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.

Nadbytečné zprávy jsou přesunuty do úložiště bez otestování.

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.

- ***Netestovat odchozí zprávy (MS Exchange 2007/2010/2013)*** - používáte-li zároveň serverové komponenty VSAPI a směrovací TA (tj. Routing Transport Agent), přičemž nezáleží na tom, zda jsou nainstalovány na jednom serveru, anebo na dvou různých, může se stát, že bude odchozí pošta prověřována dvakrát: nejprve kontrolou v reálném čase (VSAPI On-access scanner), podruhé prostřednictvím směrovacího TA. To může zapříčinit určitá zpomalení běhu serveru a mírné prodlevy při odesílání e-mailů. Pokud si jste jistí, že jsou obě serverové komponenty správně nainstalovány a aktivní, můžete se tomuto dvojímu testování odchozí pošty vyhnout zablokováním kontroly v reálném čase (VSAPI). Stačí pouze zaškrtnout toto políčko.

- ***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.

- ***Hlásit rozšířenou množinu potenciálně nežádoucích programů*** - zaškrtnutím tohoto políčka aktivujete detekci rozšířené sady spyware: programů, které jsou v původní podobě od výrobce neškodné a v pořádku, ale mohou být snadno zneužity ke škodlivým účelům, případně jde o zásadně neškodné, avšak poněkud obtěžující programy (různé doplňky do prohlížeče atd.). Jde o dodatečné opatření, které zlepšuje zabezpečení vašeho počítače na další úrovni, nicméně může blokovat také některé legální programy, proto je ve výchozím nastavení tato možnost vypnuta. Tato detekce je doplňkem předchozí možnosti, samostatně tedy není dostačující: pokud chcete ochranu před základními typy spyware, pak ponechte vždy označené předchozí políčko, a toto pak označte volitelně k němu.

- ***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. 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***

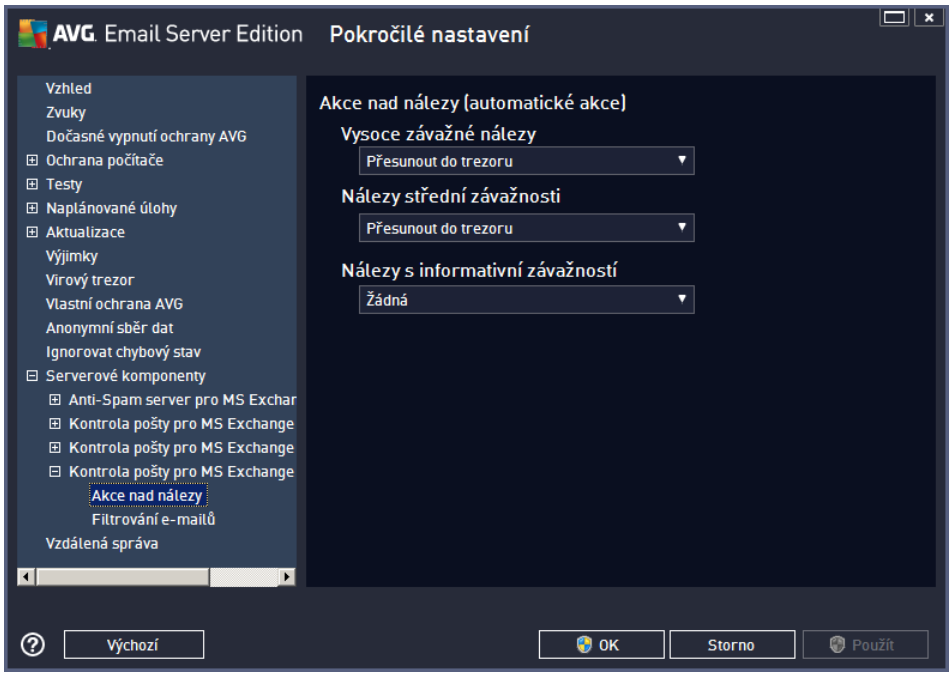
Některé prvky v tomto nastavení tvoří uživatelské rozšíření aplikačního rozhraní Microsoft VSAPI 2.0/2.5. Pokud se chcete blíže informovat o tomto rozhraní, následujte tyto odkazy:

- 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***

5.5. 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:

- ***Vysoce závažné nálezy*** – nebezpečné kódy, které se kopírují a šíří se, často nepozorovaně, aby napáchaly škody v systému uživatele.
- ***Nálezy střední závažnosti*** – různé druhy programů, které mohou, ale také nemusí představovat hrozbu.

- ***Nálezy s informativní závažností*** – zahrnuje všechny nalezené potenciální hrozby, které nelze zařadit ani do jedné z výše uvedených kategorií.

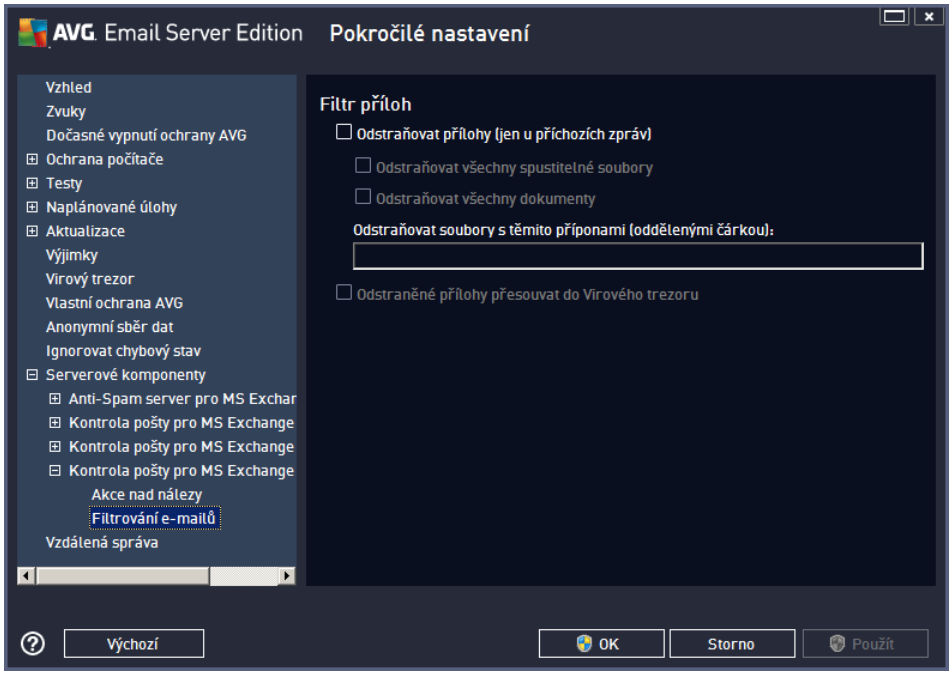
Z rolovací nabídky zvolte pro každou položku vždy jednu akci:

- ***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.

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

5.6. 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.

- ***Odstraněné přílohy přesouvat do virového trezoru*** - zaškrtněte, pokud nechcete, aby byly filtrované přílohy odstraňovány rovnou. Je-li toto políčko zaškrnuté, budou všechny přílohy zvolené prostřednictvím tohoto dialogu automaticky přesouvány do karanténního prostředí Virového trezoru. Jedná se o bezpečné místo pro ukládání potenciálně škodlivých souborů - můžete k nim přistupovat a zkoumat je, aniž by mohly ohrozit váš systém. Do Virového trezoru se dostanete z hlavní obrazovky aplikace **AVG E-mail Server**. V horní nabídce klikněte levým tlačítkem myši na položku ***Možnosti*** a následně z kontextového menu zvolte ***Virový trezor***.

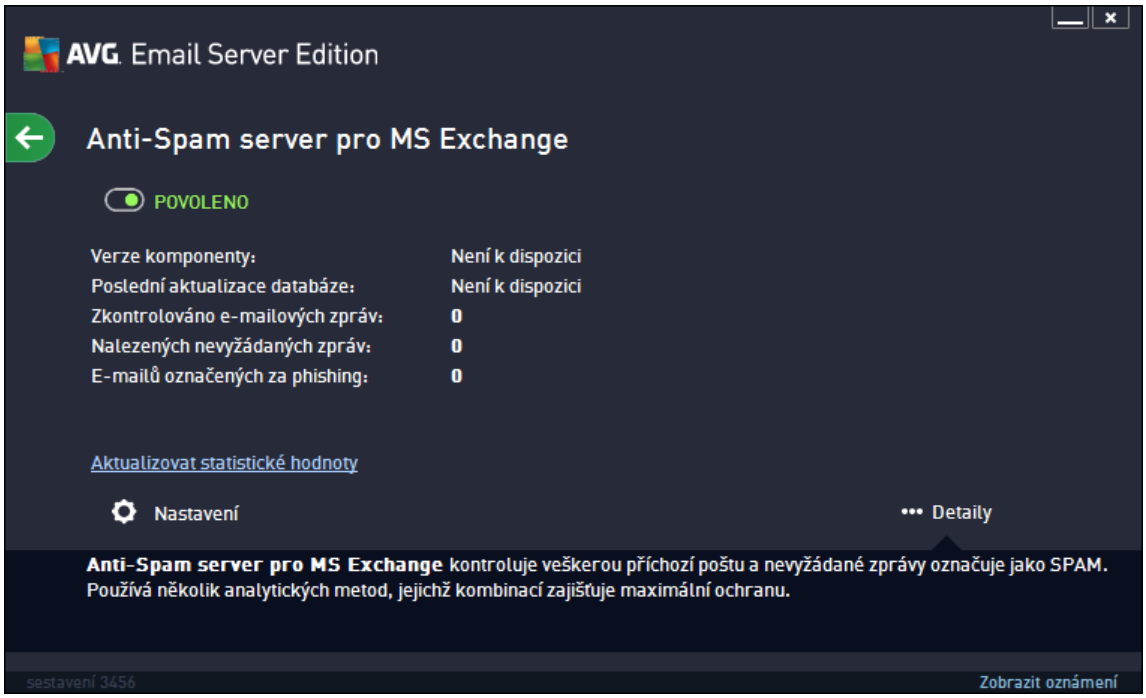
6. Komponenta Anti-Spam server pro MS Exchange

6.1. Princip komponenty Anti-Spam

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.

6.2. Rozhraní komponenty Anti-Spam



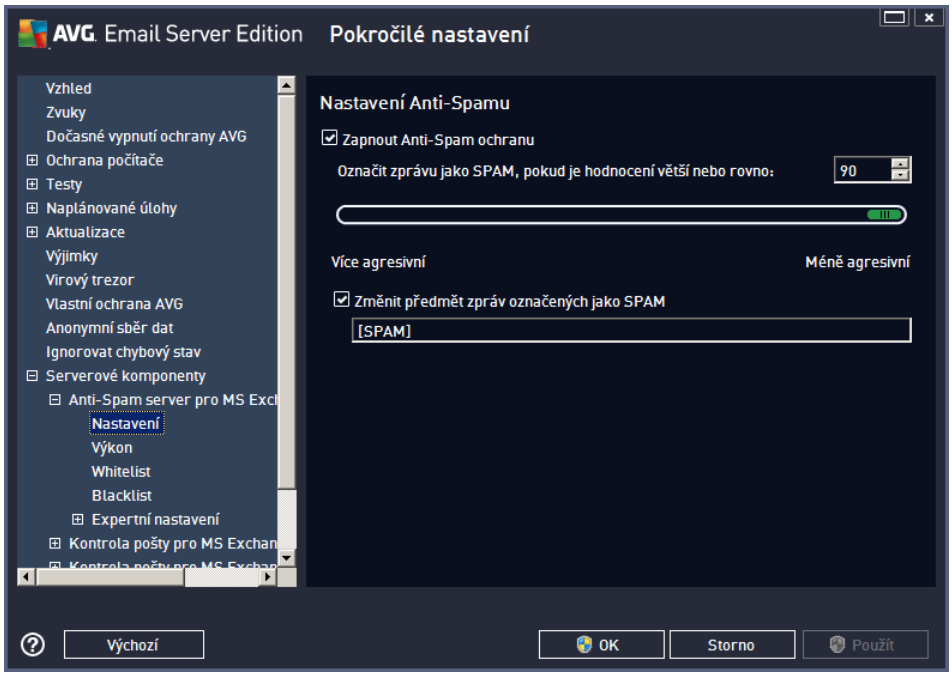
Tento dialog obsahuje základní informace o fungování komponenty, dále pak oznámení o jejím aktuálním statutu (*Povoleno/Zakázáno*) a stručný statistický přehled.

Dostupná tlačítka a odkazy:

- ***POVOLENO/ZAKÁZÁNO*** - kliknutí na toto tlačítko vypíná a zapíná danou komponentu (je-li komponenta zapnutá, jsou tlačítko i text zelené, je-li vypnutá, zobrazují se červeně).
- ***Aktualizovat statistické hodnoty*** - aktualizuje statistiky uvedené v dialogu.
- ***Nastavení*** - otevře pokročilé nastavení komponenty Anti-Spam.

6.3. Anti-Spam nastavení

6.3.1. Nastavení



V tomto dialogu 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 (*50 až 90*) do příslušného pole nebo pomocí posuvníku.

Přehled úrovní ochrany, jež odpovídají jednotlivým hodnotám:

- ***Hodnota 90*** - 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 50-59*** - Velmi agresivní konfigurace. Nespamové e-mailové zprávy budou ve větší míře odfiltrovány spolu se zprávami pozitivně detekovanými jako spam. ***Tato konfigurace už není***

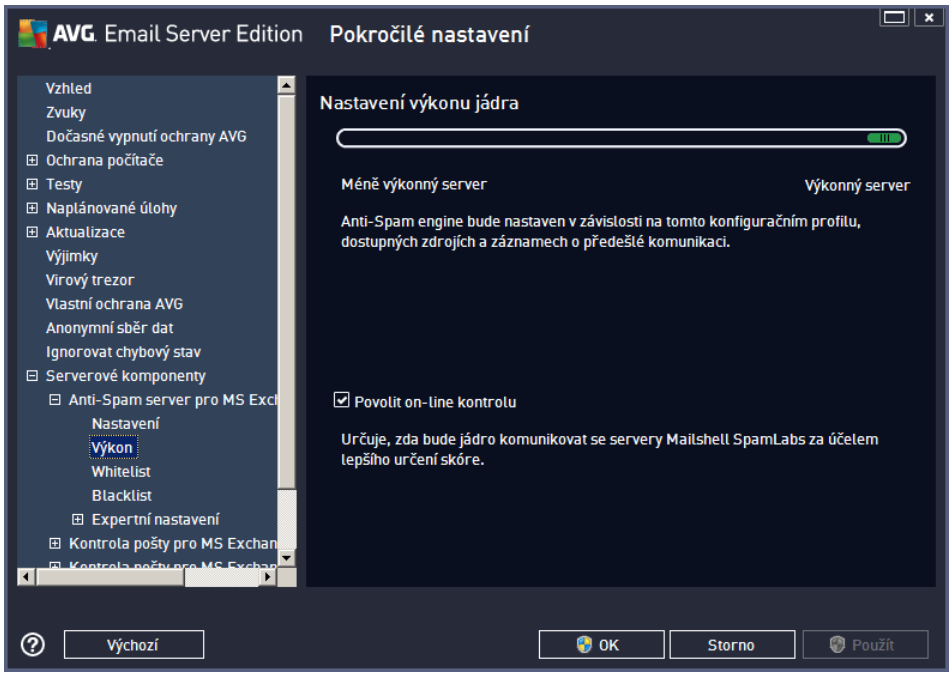
doporučeným nastavením pro běžné uživatele.

V dialogu 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.

- ***Zeptat se před ohlášením nesprávného nálezu*** - pokud jste během instalace potvrdili svou účast v Programu zlepšování produktu (program slouží ke shromažďování nejčerstvějších informací o virech, spywaru i škodlivých webových stránkách a vylepšování ochrany pro všechny naše uživatele), povolili jste odesílání reportů o detekovaných hrozbách do AVG. Tato hlášení jsou odesílána automaticky. Pokud si však přejete mít možnost zkontrolovat, že detekovaná zpráva má být skutečně klasifikována jako spam, označte položku Zeptat se před ohlášením nesprávného dotazu a před odesláním reportu vám bude zobrazen dotazovací dialog vyžadujícií vaše potvrzení.

6.3.2. 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.

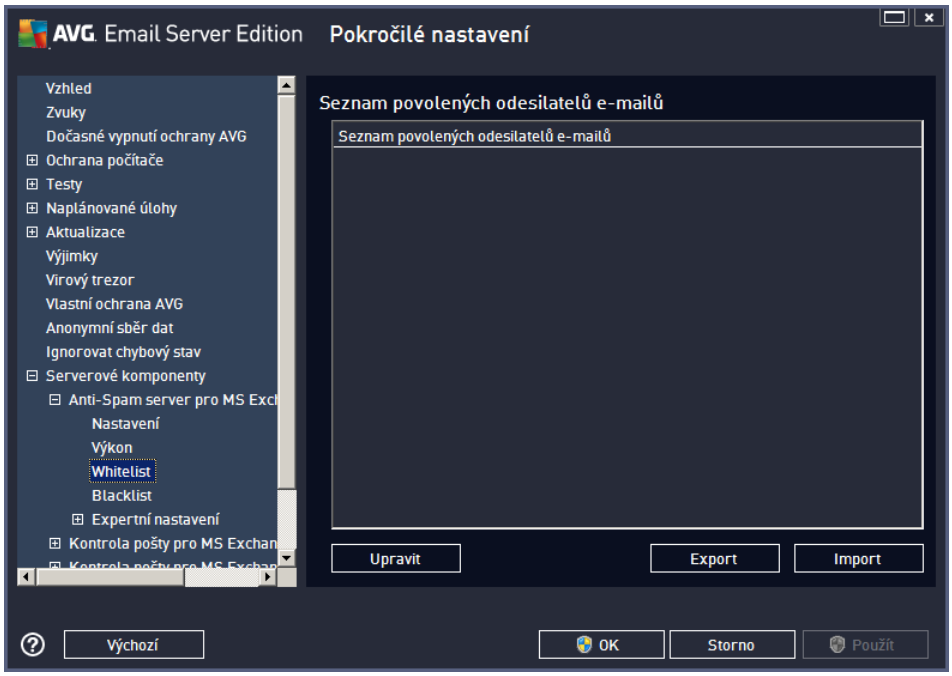
- ***Nenáročný režim*** znamená, že během testovacího procesu nebudou k identifikaci spamu použita žádná pravidla. Identifikace spamu bude založena výhradně na porovnání s testovacími daty. Tento režim pro běžné používání nedoporučujeme, nastavení lze doporučit výhradně u počítačů s velmi nízkou úrovní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

6.3.3. Whitelist

Položka ***Whitelist*** otevírá dialog se seznamem e-mailových 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:

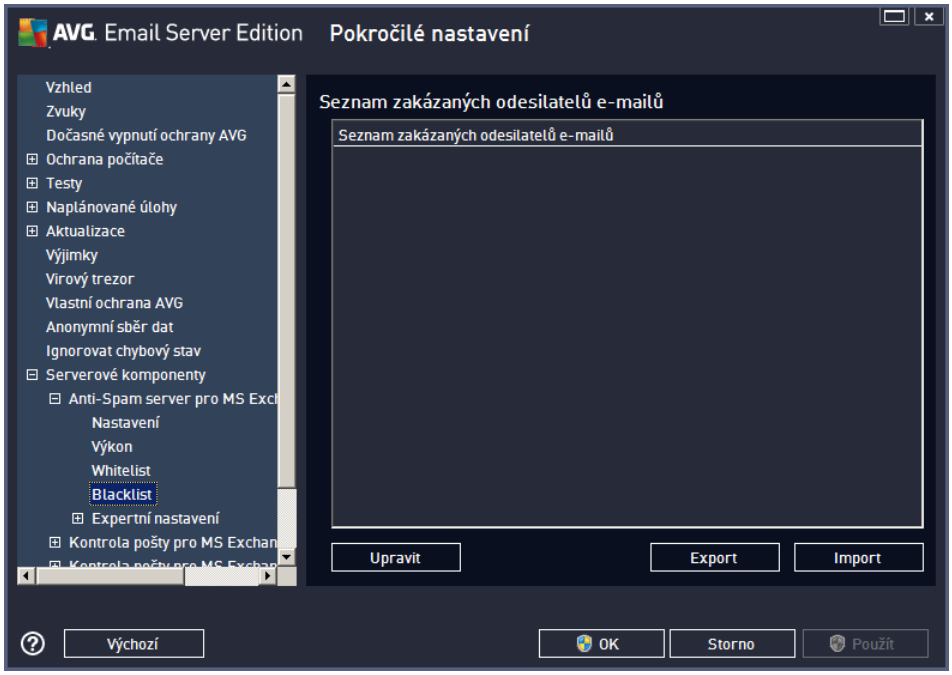
- ***Upravit*** - stiskem tohoto tlačítka otevřete dialog, v němž můžete manuálně přidávat adresy ze seznamu (můžete také použít jednorázově metodu *„kopírovat a vložit“*). Adresy/doménová jména vkládejte po jednom na každý řádek.

- ***Import*** - pokud již máte seznam adres/doménových jmen uložený v textovém souboru, můžete jej snadno importovat za použití tohoto tlačítka. Import lze provést buď z textového souboru (musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku - adresu nebo doménové jméno), z WAB souboru či přímo z adresáře Windows nebo Microsoft Office Outlooku.

- ***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.

6.3.4. Blacklist

Položka ***Blacklist*** otevírá dialog se seznamem e-mailových 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.

- ***Import*** - existující e-mail adresy můžete snadno importovat za použití tohoto tlačítka. Import lze provést buď z textového souboru (musí být ve formátu prostého textu a obsah musí být rozdělen tak, že každý řádek obsahuje pouze jedinou položku - adresu nebo doménové jméno), z WAB souboru či přímo z adresáře Windows nebo Microsoft Office Outlooku.

- ***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.

6.3.5. Expertní nastavení

Tato větev obsahuje rozsáhlé možnosti nastavení komponenty Anti-Spam. Tato nastavení jsou určena výhradně pokročilým uživatelům, jako jsou správci sítí, kteří potřebují antispamovou ochranu nastavit do detailů pro co nejlepší ochranu e-mailových serverů. Z tohoto důvodu není v dialozích pokročilého nastavení dostupná běžná nápověda, pouze stručný popis příslušné funkce přímo v dialogu.

Doporučujeme neměnit žádná pokročilá nastavení, pokud nejste dobře obeznámeni se všemi funkcemi nástroje Spamcatcher (MailShell Inc.). Nevhodné změny nastavení by mohly vyústit v nespolehlivost až nefunkčnost celé komponenty.

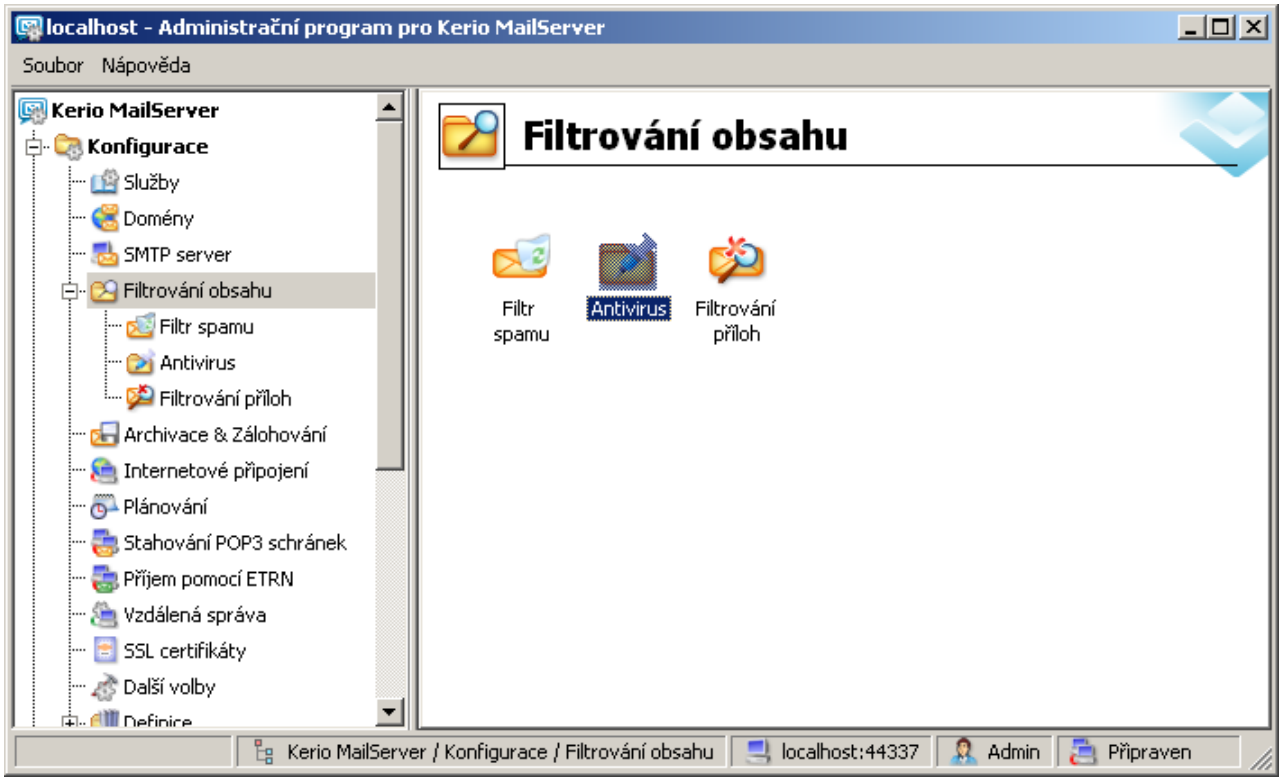
Pokud se přesto domníváte, že je nutné měnit konfiguraci služby Anti-Spam na úrovni vysoce pokročilého nastavení, pokračujte prosím podle instrukcí uvedených přímo v dialogu. Obecně platí, že v každém dialogu máte možnost zapnout jednu konkrétní funkci služby Anti-Spam a její popis je uveden přímo v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

- ***Filtrování*** - seznam jazyků, seznam zemí, povolené IP adresy, blokované IP adresy, blokované země, blokované znakové sady, falešní odesilatelé
- ***RBL*** - RBL servery, práh, časový limit, maximum IP adres, ignorované IP adresy
- ***Internetové připojení*** - časový limit, proxy server, autentifikace proxy

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***.

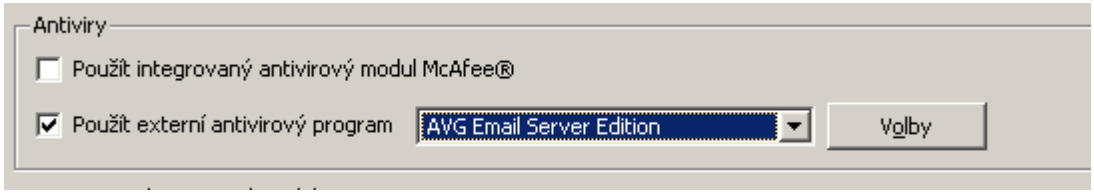


Na hlavním panelu aplikace se zobrazí dialogové okno ***Filtrování obsahu***. V rámci tohoto okna je možné volit ze tří nabídek:

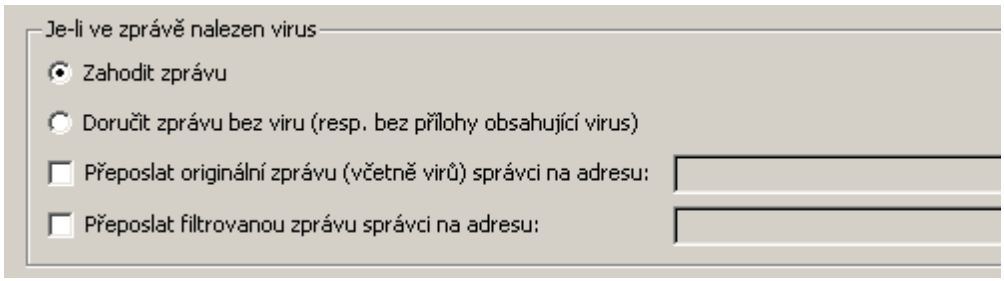
- ***Filtr spamu***
- ***Antivirus*** (viz kapitola ***Antivirus***)
- ***Filtrování příloh*** (viz kapitola ***Filtrování příloh***)

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:

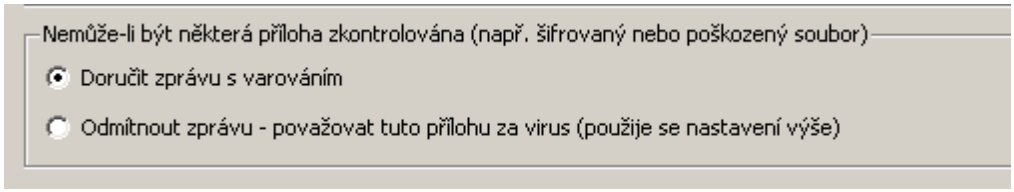


V následující části můžete specifikovat pravidla pro akce provedené v rámci detekce infikované zprávy nebo filtrování příloh:



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.

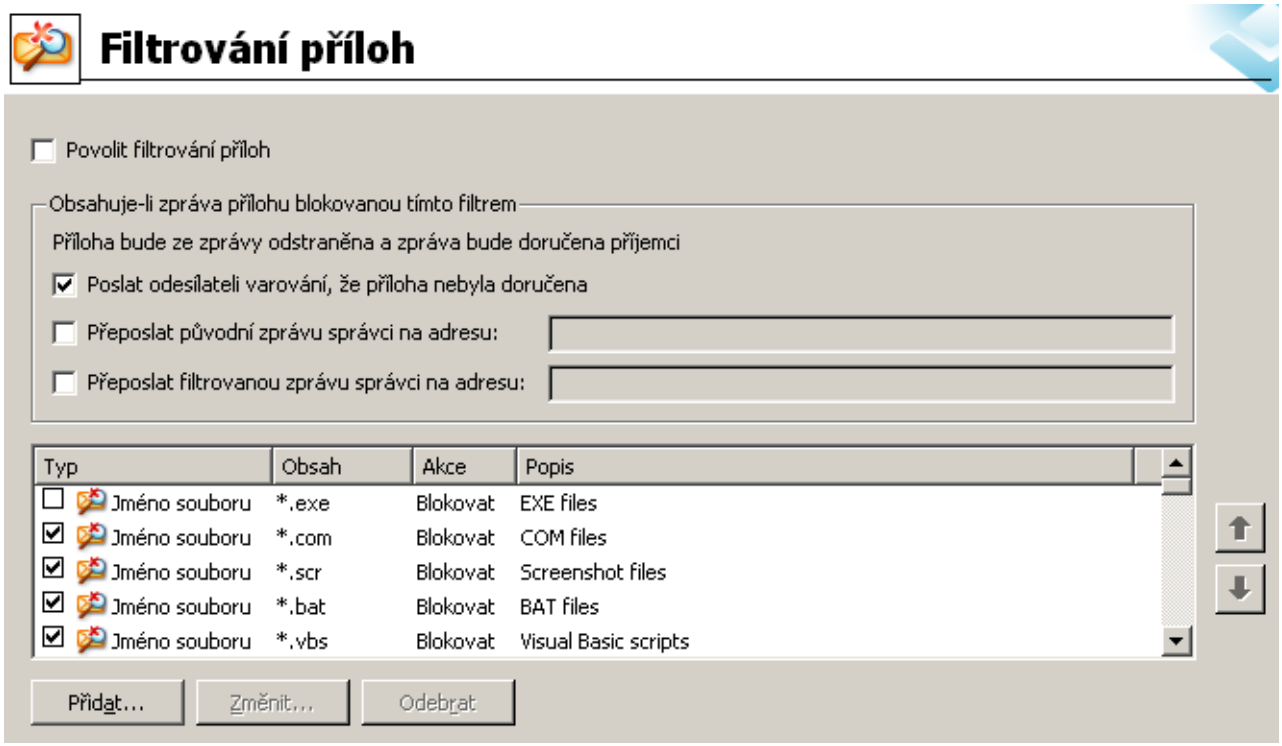


Umožňuje specifikovat akce pro soubory příloh, které nemohou být z jakéhokoli důvodu přečteny a otestovány:

- ***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. (tj. zpráva bude doručena bez přílohy, nebo zahozena). Tato možnost je nejbezpečnější, ovšem je potřeba vzít na vědomí, že v podstatě znemožňuje zasílání zaheslovaných archivů.

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:

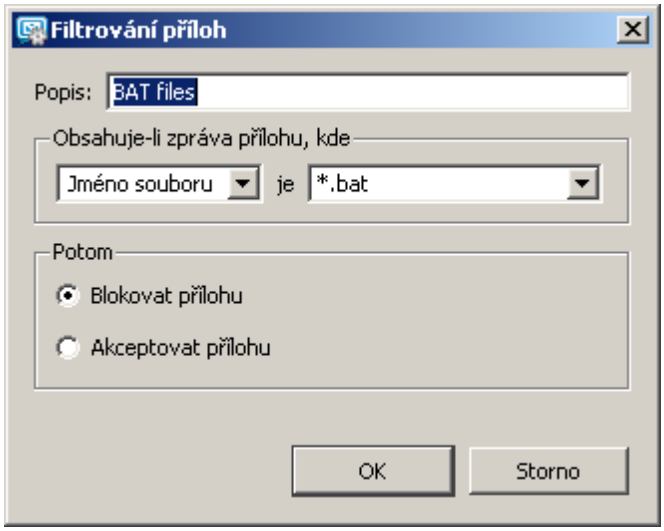
- ***Poslat odesílateli varování, že příloha nebyla doručena*** - odesílateli bude ***Kerio Mailserverem*** zasláno varování, že odeslal zprávu s infikovanou nebo nepovolenou přílohou.
- ***Přeposlat původní zprávu správci na adresu*** - zpráva bude přeposlána v původním tvaru, tedy i s infikovanou nebo zakázanou přílohou, na zadanou e-mailovou 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 e-mailovou 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*** (bude provedena akce definovaná nad seznamem zakázaných příloh).

- ***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. 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***.