AVG Email Server Edition 2011

Podrecznik uzytkownika

Wersja dokumentu 2011.01 (22. 9. 2010)

Spis tresci

1. Wprowadzenie

Ten podrecznik uzytkownika zawiera kompleksowa dokumentacje systemu **AVG Email Server Edition 2011**.

Gratulujemy zakupu systemu AVG Email Server Edition 2011!

System **AVG Email Server Edition 2011** nalezy do linii uznanych i nagradzanych produktów AVG, które zapewniaja uzytkownikom spokój ducha, a ich komputerom - pelne bezpieczenstwo. Podobnie jak pozostale produkty, system **AVG Email Server Edition 2011** zaprojektowano od podstaw pod katem zapewnienia slynnego juz poziomu ochrony w nowy, bardziej przyjazny dla uzytkownika sposób.

System AVG zaprojektowano i zbudowano tak, by chronil uzytkownika podczas pracy na komputerze i w sieci. Ciesz sie pelna ochrona AVG.

Uwaga: *Ta dokumentacja zawiera opis funkcji charakterystycznych dla wersji E-mail Server Edition. Aby uzyskac wiecej informacji na temat innych funkcji systemu AVG, zajrzyj do podrecznika uzytkownika AVG Internet Security, który zawiera wszystkie niezbedne szczegóły. Podrecznik ten moze zostac pobrany ze strony http://www.avg.com.*

2. Wymagania instalacyjne AVG

2.1. Obslugiwane systemy operacyjne

AVG Email Server Edition 2011 sluzy do ochrony serwerów pocztowych dzialajacych pod nastepujacymi systemami operacyjnymi:

- Windows 2008 Server Edition (x86 i x64)
- Windows 2003 Server (x86, x64) z dodatkiem SP1

2.2. Obslugiwane serwery poczty e-mail

Obslugiwane sa nastepujace serwery poczty e-mail:

- MS Exchange 2003 Server
- MS Exchange 2007 Server
- MS Exchange 2010 Server
- AVG dla Kerio MailServer - wersja 6.7.2 lub nowsza

2.3. Minimalne wymagania sprzetowe

Minimalne wymagania sprzetowe dla systemu **AVG Email Server Edition 2011**:

- Procesor Intel Pentium 1.5 GHz,
- 500 MB wolnego miejsca na dysku twardym (w celu instalacji),
- 512 MB pamieci RAM.

Zalecane wymagania sprzetowe dla systemu **AVG Email Server Edition 2011**:

- Procesor Intel Pentium 1.8 GHz,
- 600 MB wolnego miejsca na dysku twardym (w celu instalacji),
- 512 MB pamieci RAM.

2.4. Dezinstalacja poprzednich wersji

W przypadku korzystania ze starej wersji aplikacji AVG Email Server przed zainstalowaniem produktu **AVG Email Server Edition 2011** konieczne bedzie jej reczne odinstalowanie. Deinstalacja poprzedniej wersji musi zostac wykonana recznie przy uzyciu standardowych funkcji systemu Windows.

- Z menu Start nalezy kolejno wybrac opcje ***Ustawienia/Panel sterowania/ Dodaj lub Usun programy***, a nastepnie z listy zainstalowanego oprogramowania wybrac odpowiedni program. Nalezy sie upewnic, czy do deinstalacji zostal wybrany wlasciwy program AVG. Przed deinstalacja aplikacji AVG File Server Edition nalezy równiez odinstalowac program Email Server Edition.

- Po odinstalowaniu aplikacji Email Server Edition, mozna kontynuowac deinstalacje poprzedniej wersji programu AVG File Server Edition. Mozna to zrobic, kolejno wybierajac z menu Start opcje ***Wszystkie programy/AVG/Odinstaluj AVG.***

- Jesli poprzednio uzywano systemu AVG w wersji 8.x lub starszej, nie nalezy zapomniec o osobnym odinstalowaniu pluginów serwera.

  Uwaga: *Podczas procesu deinstalacji konieczne bedzie ponowne uruchomienie serwera.*

  Plugin Exchange - uruchom plik setupes.exe z parametrem /uninstall w folderze, w którym zainstalowany zostal plugin.

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

  Plugin Lotus Domino/Notes - uruchom plik setupes.exe z parametrem /uninstall w folderze, w którym zainstalowany zostal plugin.

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

2.5. Dodatki Service Pack dla MS Exchange

Dla serwera MS Exchange 2003 nie jest wymagany zaden dodatek Service Pack; jednak zaleca sie zaktualizowanie systemu i instalacje najnowszych dodatków Service Pack i poprawek w celu zapewnienia maksymalnego bezpieczenstwa.

Dodatek Service Pack dla serwera MS Exchange 2003 Server (opcjonalnie):

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

Na poczatku procesu instalacji zostana sprawdzone wersje wszystkich bibliotek systemowych. Jesli zajdzie potrzeba instalacji nowszych bibliotek, instalator zmieni rozszerzenie starszych plików na .delete. Biblioteki zostana usuniete po ponownym uruchomieniu systemu.

Dodatek Service Pack dla serwera MS Exchange 2007 Server (opcjonalnie):

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

3. Proces instalacji systemu AVG

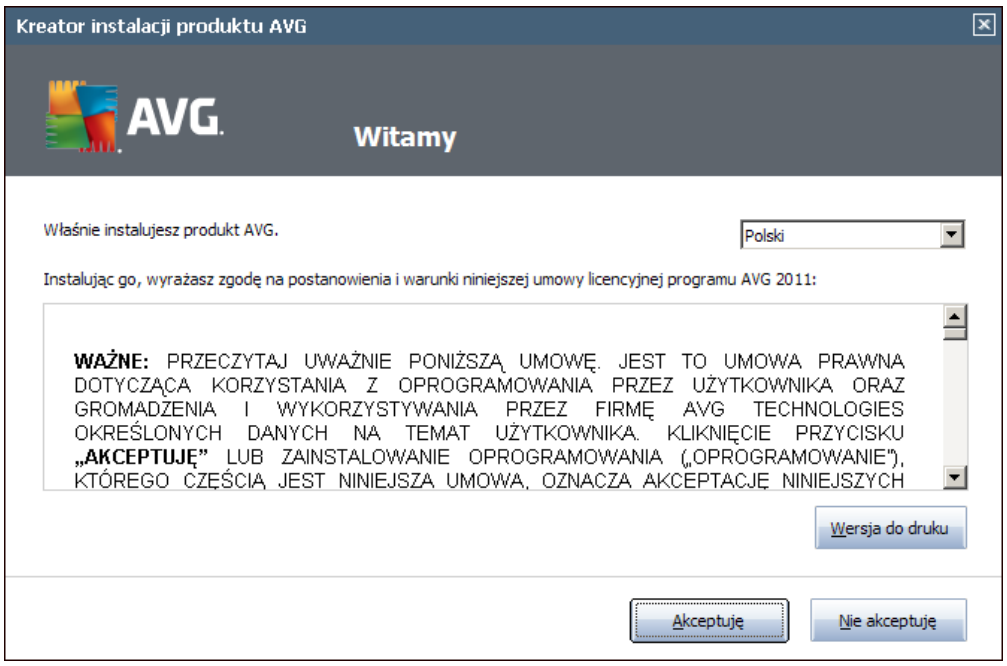
Aby zainstalowac na komputerze system AVG, nalezy najpierw zdobyc najnowszy plik instalacyjny programu. Mozna znalezc go na dysku CD bedacym czescia dystrybucyjnej edycji programu - istnieje jednak ryzyko, ze bedzie on nieaktualny. Dlatego zaleca sie pobranie najnowszego pliku instalacyjnego z internetu. Plik mozna pobrac z witryny internetowej firmy AVG (pod adresem http://www.avg.com/download?prd=msw)

Uwaga: *Dla tego produktu dostepne sa dwa pakiety instalacyjne: dla 32-bitowych systemów operacyjnego (oznaczony jako x86) i dla systemów 64-bitowych (oznaczonych jako x64). Upewnij sie, ze uzywasz pakietu instalacyjnego odpowiedniego dla danego systemu operacyjnego..*

Podczas procesu instalacji konieczne jest podanie numeru licencji. Nalezy wiec przygotowac go przed rozpoczeciem instalacji. Numer ten znajduje sie na opakowaniu dysku CD. Przy zakupie systemu AVG przez internet, numer licencji jest dostarczany poczta e-mail.

Po pobraniu i zapisaniu pliku instalatora na dysku, mozna uruchomic proces instalacji. Instalacja to sekwencja okien dialogowych zawierajacych krótkie opisy poszczególnych etapów. Ponizej znajduja sie objasnienia kazdego z nich:

3.1. Uruchamianie instalacji



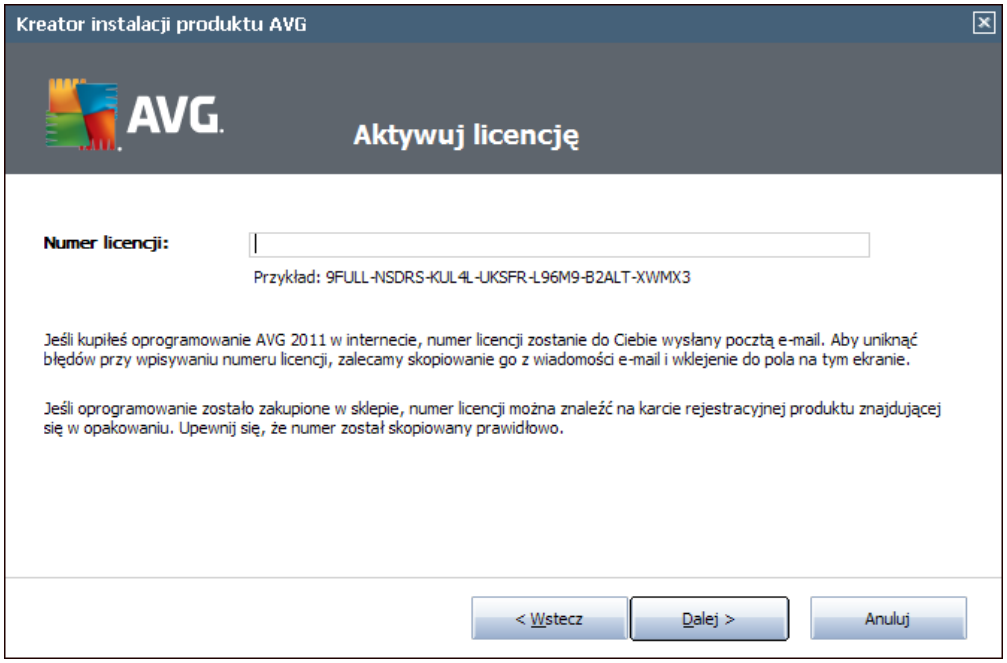
Proces instalacji rozpoczyna sie od wyswietlenia ***okna powitalnego***. Mozna w nim wybrac jezyk uzywany podczas procesu instalacji i przeczytac warunki umowy. Aby wyswietlic tresc umowy licencyjnej w nowym oknie, kliknij przycisk ***Wersja do druku***. Kliknij przycisk ***Akceptuje***, aby potwierdzic wybór i przejsc do kolejnego ekranu.

Uwaga: *Podczas procesu instalacji mozliwe bedzie również wybranie innych dodatkowych jezyków interfejsu aplikacji.*

3.2. Aktywacja licencji

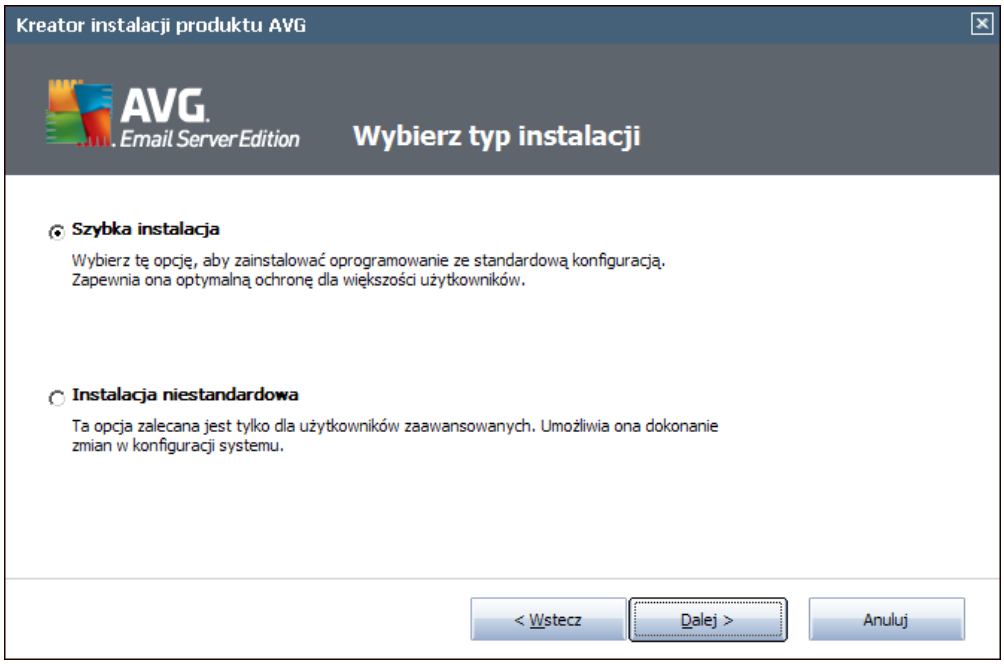
W oknie dialogowym ***Aktywacja licencji*** nalezy wprowadzic swój numer licencji.

Wprowadz numer licencji w polu tekstowym ***Numer licencji***. Numer licencji jest wysylany poczta e-mail po zakupieniu oprogramowania AVG w internecie. Wazne jest dokladne wprowadzenie wspomnianego numeru. Jesli numer jest dostepny w formie cyfrowej (w wiadomosci e-mail), zaleca sie skopiowanie i wklejenie go w odpowiednim polu.



Aby kontynuowac instalacje, kliknij przycisk ***Dalej***.

3.3. Wybór typu instalacji

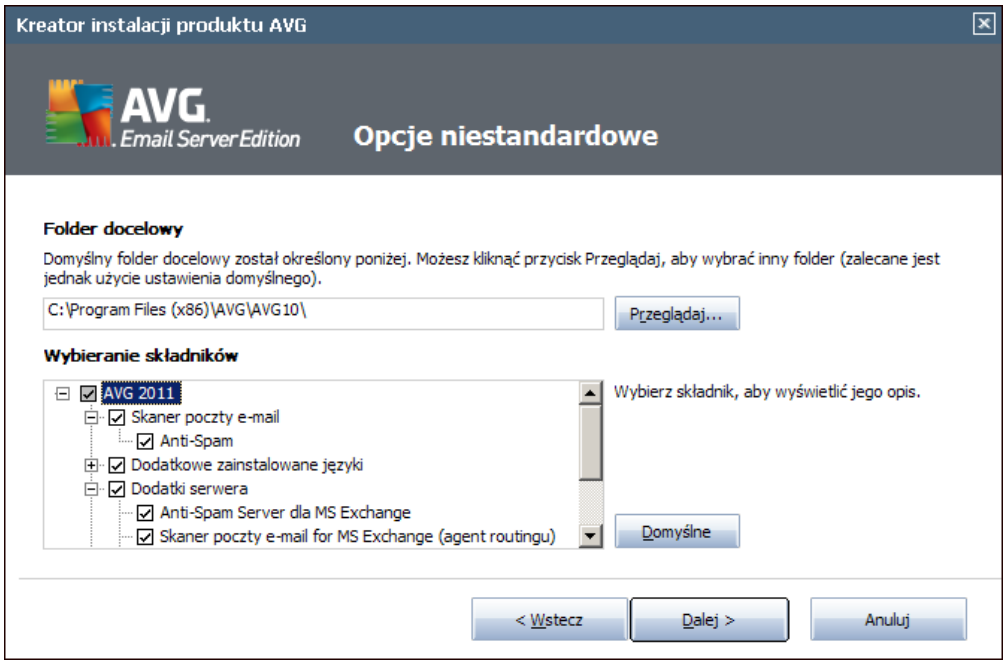


Okno dialogowe ***Wybierz typ instalacji*** umozliwia wybranie jednej z dwóch opcji instalacji: ***Instalacja szybka*** lub ***Instalacja niestandardowa***.

Wiekszosc uzytkowników zdecydowanie powinna wybrac opcje ***Instalacja szybka***, która pozwala zainstalowac system AVG w sposób calkowicie zautomatyzowany, z ustawieniami wstepnie zdefiniowanymi przez dostawce oprogramowania AVG. Taka konfiguracja zapewnia maksymalne bezpieczenstwo oraz optymalne wykorzystanie zasobów. Jesli w przyszlosci zajdzie potrzeba zmiany konfiguracji, mozna bedzie to zrobic bezposrednio z poziomu interfejsu AVG.

Opcje ***Instalacja niestandardowa*** powinni wybierac tylko doswiadczeni uzytkownicy, którzy maja uzasadnione powody, aby nie instalowac systemu AVG z ustawieniami domyslnymi, (np. po to, aby dostosowac go do specyficznych wymagan systemowych.

3.4. Instalacja niestandardowa - opcje niestandardowe



Okno ***Folder docelowy*** pozwala okreslic lokalizacje dla plików systemu AVG. Domyslnie pakiet AVG jest instalowany w folderze Program Files na dysku C:. Aby zmienic te lokalizacje, kliknij przycisk ***Przegladaj*** i w wyswietlonym oknie wybierz odpowiedni folder.

Sekcja ***Wybór skladników*** zawiera przeglad wszystkich skladników systemu AVG, które mozna zainstalowac. Jesli ustawienia domyslne nie sa dla Ciebie odpowiednie, mozesz dodac lub usunac zadane skladniki.

Wybierac mozna jednak tylko skladniki dostepne w zakupionej edycji systemu AVG. Tylko one beda widoczne w oknie dialogowym Wybór skladników!

- ***Klient Administracji zdalnej AVG*** - jesli system AVG ma miec mozliwosc laczenia sie z baza AVG DataCenter (edycje AVG Network), konieczne jest wybranie tej opcji

  Uwaga: *Tylko skladniki serwera dostepne na liscie moge byc zarzadzane zdalnie!*

- ***Menedzer ustawien systemu*** - narzedzie przeznaczone przede wszystkim dla administratorów sieci, pozwalajace na kopiowanie, edycje i dystrybucje konfiguracji systemu AVG. Konfiguracja moze zostac zapisana na urzadzeniu przenosnym (dysk USB itp.), a nastepnie zastosowana recznie (lub w dowolny inny sposób) na wybranych stacjach roboczych.

- ***Instalacja dodatkowych jezyków*** - ta opcja umozliwia okreslenie, jakie jezyki interfejsu systemu AVG maja zostac zainstalowane. Nalezy w tym celu zaznaczyc opcje ***Dodatkowe zainstalowane jezyki*** i wybrac je z odpowiedniego menu.

Podstawowy przeglad poszczególnych skladników serwera (***dodatki serwera***):

- ***Anti-Spam Server for MS Exchange***

  Sprawdza wszystkie przychodzace wiadomosci e-mail i oznacza niepozadana poczte jako SPAM. Podczas przetwarzania kazdej wiadomosci wykorzystywanych jest kilka metod analizy oferujacych najskuteczniejsza dostepna na rynku ochrone.

- ***Skaner poczty e-mail dla MS Exchange (agent routingu)***

  Sprawdza wszystkie przychodzace, wychodzace i wewnetrzne wiadomosci e-mail przechodzace przez serwer MS Exchange w roli HUB.

  Skladnik dostepny dla serwera MS Exchange 2007/2010 moze zostac zainstalowany tylko dla serwera w roli HUB.

- ***Skaner poczty e-mail dla MS Exchange (agent SMTP)***

  Sprawdza wszystkie wiadomosci e-mail przechodzace przez interfejs MS Exchange SMTP.

  Skladnik dostepny dla MS Exchange 2007/2010 moze zostac zainstalowany dla serwera w roli EDGE lub HUB.

- ***Skaner poczty e-mail dla MS Exchange (VSAPI)***

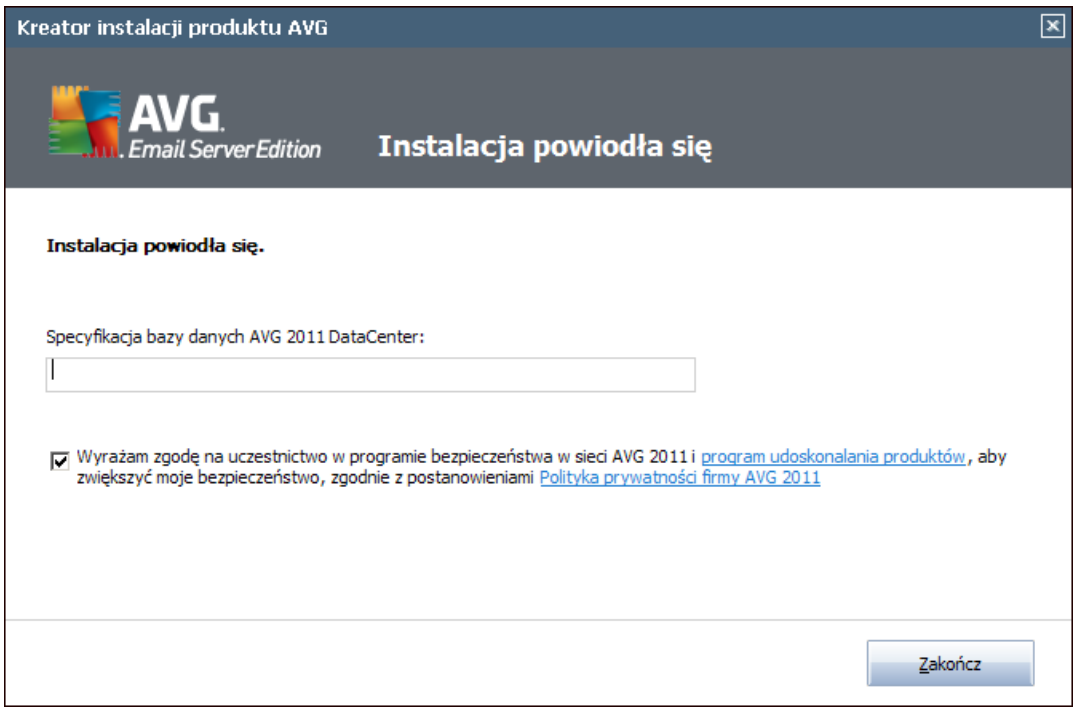
  Sprawdza wszystkie wiadomosci e-mail przechowywane w skrzynkach pocztowych uzytkownika. Wszystkie wykryte wirusy sa przenoszone do Przechowalni lub usuwane.

Uwaga: *Dla róznych wersji serwera MS Exchange dostepne sa rózne opcje.*

Aby kontynuowac, kliknij przycisk ***Dalej***.

3.5. Ukonczenie instalacji

Jesli przy wyborze skladników zostal wybrany modul ***Administracja zdalna***, na ostatnim ekranie mozliwe bedzie okreslenie parametrów polaczenia z baza AVG DataCenter.



Program AVG jest zainstalowany na komputerze i w pelni funkcjonalny. System ten dziala w tle, calkowicie automatycznie.

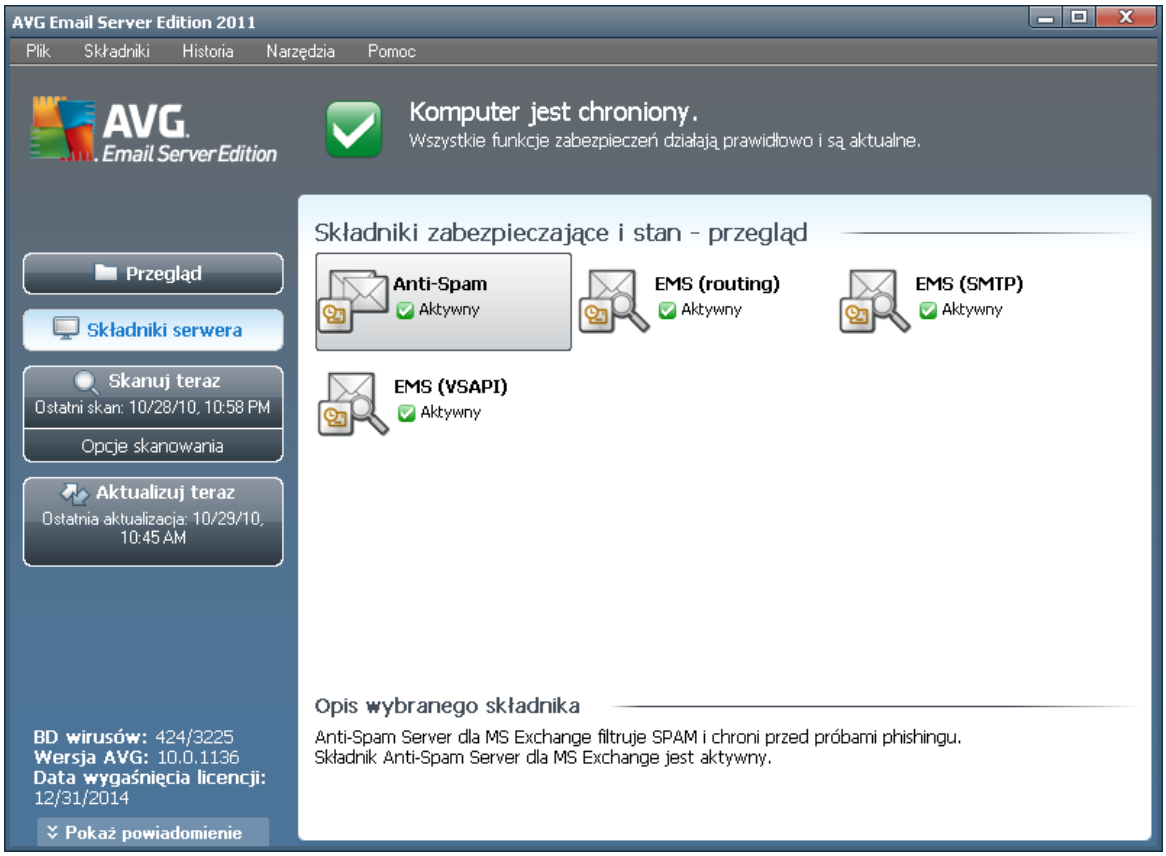
Aby skonfigurowac opcje ochrony serwera poczty e-mail, nalezy przejsc do odpowiedniego rozdzialu:

- ***Skaner poczty e-mail dla serwera MS Exchange Server 2007/2010***
- ***Skaner poczty e-mail dla serwera MS Exchange Server 2003***
- ***AVG dla Kerio MailServer***

4. Skaner poczty e-mail dla serwera MS Exchange Server 2007/20

4.1. Przeglad

Opcje konfiguracji produktu AVG dla MS Exchange Server 2007/2010 sa w pelni zintegrowane z produktem AVG Email Server Edition 2011 jako skladniki serwera.



Podstawowy przeglad poszczególnych skladników serwera:

- ***Anti-Spam - Anti-Spam Server dla MS Exchange***

  Sprawdza wszystkie przychodzace wiadomosci e-mail i oznacza niepozadana poczte jako SPAM. Podczas przetwarzania kazdej wiadomosci wykorzystywanych jest kilka metod analizy, oferujacych najskuteczniejsza dostepna na rynku ochrone.

- ***EMS (routing) - Skaner poczty e-mail dla MS Exchange (agent routingu)***

  Sprawdza wszystkie przychodzace, wychodzace i wewnetrzne wiadomosci e-mail przechodzace przez serwer MS Exchange w roli HUB.

  Skladnik dostepny dla serwera MS Exchange 2007/2010; moze zostac

zainstalowany tylko dla serwera w roli HUB.

- ***EMS (SMTP) - Skaner poczty e-mail dla MS Exchange (agent SMTP)***

  Sprawdza wszystkie wiadomosci e-mail przechodzace przez interfejs MS Exchange SMTP.

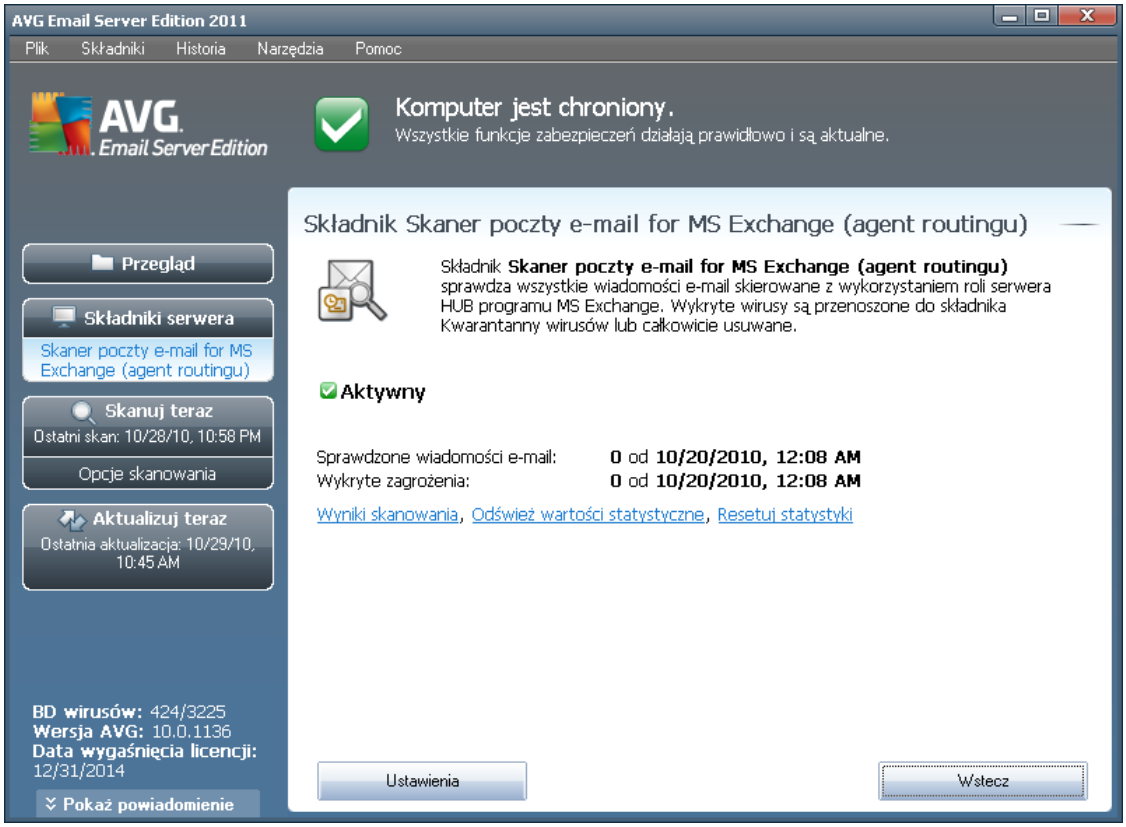
  Skladnik dostepny tylko dla serwera MS Exchange 2007/2010; moze zostac zainstalowany dla serwera w roli EDGE lub HUB.

- ***EMS (VSAPI) - Skaner poczty e-mail dla MS Exchange (VSAPI)***

  Sprawdza wszystkie wiadomosci e-mail przechowywane w skrzynkach pocztowych uzytkownika. Wszystkie wykryte wirusy sa przenoszone do Przechowalni lub usuwane.

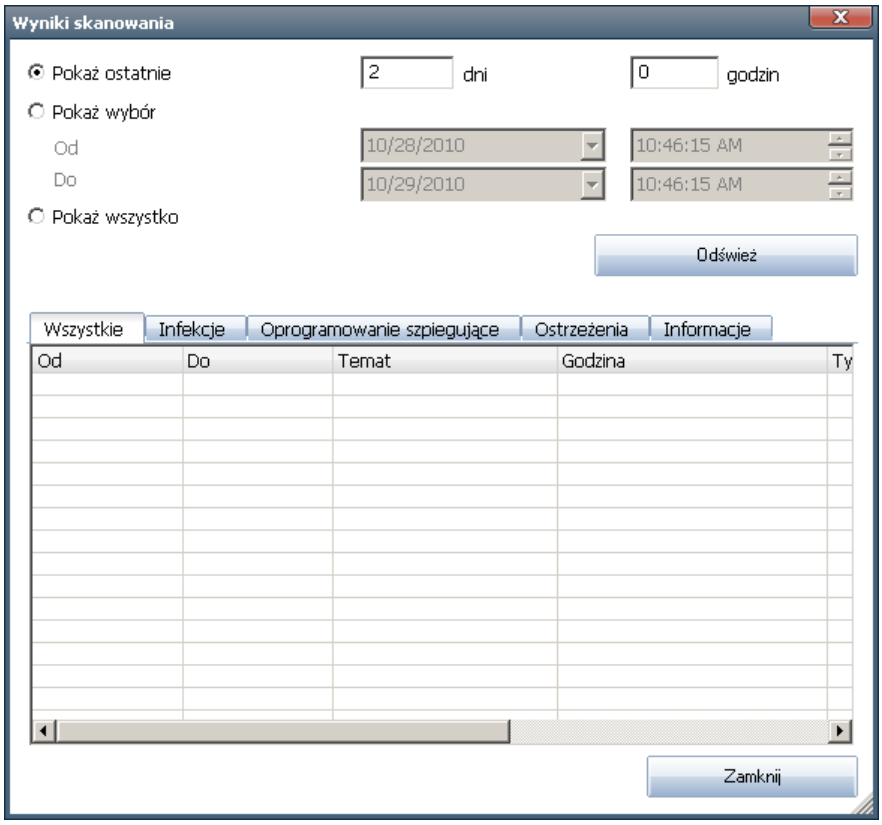
Wazna informacja: *Jesli podczas instalacji uzywany jest jednoczesnie interfejs VSAPI i agent transportowy routingu w roli Hub Exchange, wiadomosci e-mail beda skanowane dwukrotnie. Sposób unikniecia tej sytuacji zostal opisany w ponizszym rozdziale* ***Uwaga techniczna****.*

Dwukrotnie kliknij wybrany skladnik, aby otworzyc jego interfejs. Z wyjatkiem skladnika Anti-Spam wszystkie skladniki posiadaja wspólne przyciski i lacza:



- ***Wyniki skanowania***

Otwiera nowe okno dialogowe, w którym dostepny jest przeglad wyników skanowania:



W tym miejscu mozna sprawdzic wiadomosci podzielone na kilka kart wedlug poziomu zagrozenia. Poziomy zagrozenia i raportowania mozna dostosowac w konfiguracji indywidualnych skladników.

Domyslnie wyswietlane sa tylko wyniki z ostatnich dwóch dni. Okres, dla którego wyswietlane sa wyniki, mozna dostosowac za pomoca nastepujacych opcji:

- ***Pokaz ostatnie*** - wprowadz preferowana ilosc dni i godzin.
- ***Pokaz wybrane*** - wprowadz niestandardowy przedzial czasu i daty.
- ***Pokaz wszystko*** - wyswietla wszystkie dostepne wyniki.

Przycisk ***Odswiez*** sluzy do ponownego zaladowania wyników.

- ***Odswiez wartosci statystyczne*** - aktualizuje powyzsze statystyki.
- ***Resetuj wartosci statystyczne*** - zeruje wszystkie statystyki.

Dostepne przyciski:

- ***Ustawienia*** - ten przycisk pozwala otworzyc ustawienia skladnika.

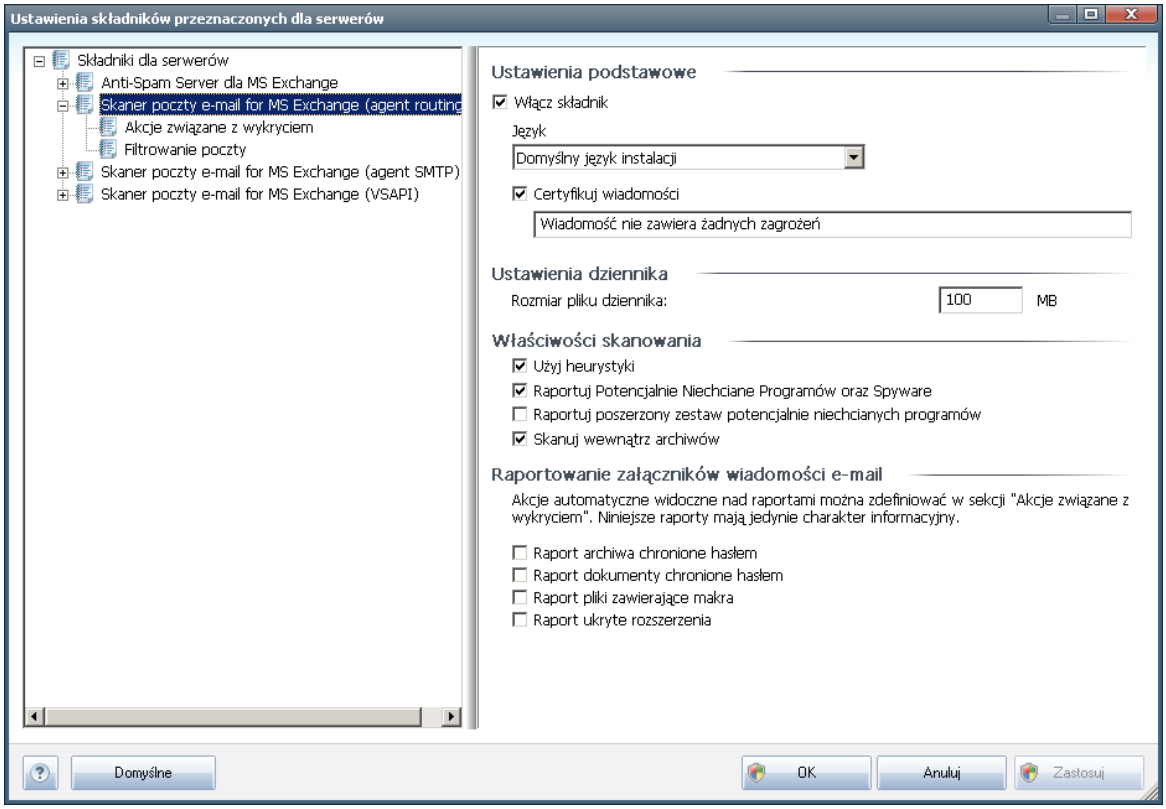
- ***Wstecz*** - ten przycisk umozliwia powrót do okna Przeglad skladników serwera.

Wiecej informacji na temat indywidualnych ustawien wszystkich skladników mozna znalezc w rozdzialach ponizej.

4.2. Skaner poczty e-mail dla MS Exchange (routing TA)

Aby otworzyc ustawienia ***Skanera poczty e-mail dla serwera MS Exchange (agent routingu)***, kliknij przycisk ***Ustawienia*** w interfejsie tego skladnika.

Z listy ***Skladniki serwera*** wybierz pozycje ***Skaner poczty e-mail dla serwera MS Exchange (routing TA)***:



Sekcja ***Ustawienia podstawowe*** zawiera nastepujace opcje:

- ***Wlacz skladnik*** - usuniecie zaznaczenia tej opcji spowoduje wylaczenie calego skladnika.
- ***Jezyk*** - wybierz preferowany jezyk skladnika.
- ***Certyfikuj wiadomosci*** - zaznacz to pole, aby do wszystkich skanowanych wiadomosci dolaczac certyfikacje. Jej tresc mozna dostosowac w kolejnym polu.

Sekcja ***Ustawienia dziennika***:

- ***Rozmiar pliku dziennika*** - wybierz preferowany rozmiar pliku dziennika. Wartosc domyslna: 100 MB.

Sekcja ***Wlasciwosci skanowania***:

- ***Uzyj heurystyki*** - zaznacz to pole, aby wlaczyc analize heurystyczna podczas skanowania.
- ***Raportowanie potencjalnie niechcianych programów i programów typu spyware*** - te opcje nalezy zaznaczyc, aby raportowana byla obecnosc potencjalnie niechcianych programów i programów typu spyware.
- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - zaznaczenie tego pola umozliwi wykrycie wiekszych ilosci oprogramowania szpiegujacego, tj. programów, które przy zakupie bezposrednio od producenta sa calkowicie nieszkodliwe, lecz pózniej moga zostac uzyte niezgodnie z przeznaczeniem lub w celu wyrzadzenia szkody (np. rózne paski narzedzi). To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera oraz podniesienie komfortu pracy. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona. Uwaga: Ta funkcja detekcji stanowi uzupelnienie poprzedniej opcji, dlatego w celu zapewnienia ochrony przed podstawowymi rodzajami oprogramowania szpiegujacego poprzednie pole wyboru powinno byc zawsze zaznaczone.
- ***Skanuj wewnatrz archiwów*** - opcje te nalezy zaznaczyc, aby umozliwic skanerowi skanowanie równiez wewnatrz archiwów (zip, rar itp.)

W sekcji ***Raportowanie zalaczników wiadomosci e-mail*** mozliwe jest wybranie pozycji, które maja byc raportowane podczas skanowania. Jesli to pole jest zaznaczone, kazda wiadomosc e-mail z taka pozycja bedzie zawierac znacznik [INFORMATION]. Ta domyslna konfiguracja moze zostac latwo dostosowana w obszarze ***Informacje*** sekcji ***Akcje zwiazane z wykryciem*** (patrz nizej).

Dostepne sa nastepujace opcje:

- ***Powiadamiaj o archiwach chronionych haslem***
- ***Powiadamiaj o dokumentach chronionych haslem***
- ***Powiadamiaj o plikach zawierajacych makra***
- ***Powiadamiaj o ukrytych rozszerzeniach***

W strukturze drzewa dostepne sa nastepujace pozycje:

- ***Akcje zwiazane z wykrywaniem***
- ***Filtrowanie poczty***

4.3. Skaner poczty e-mail dla MS Exchange (SMTP TA)

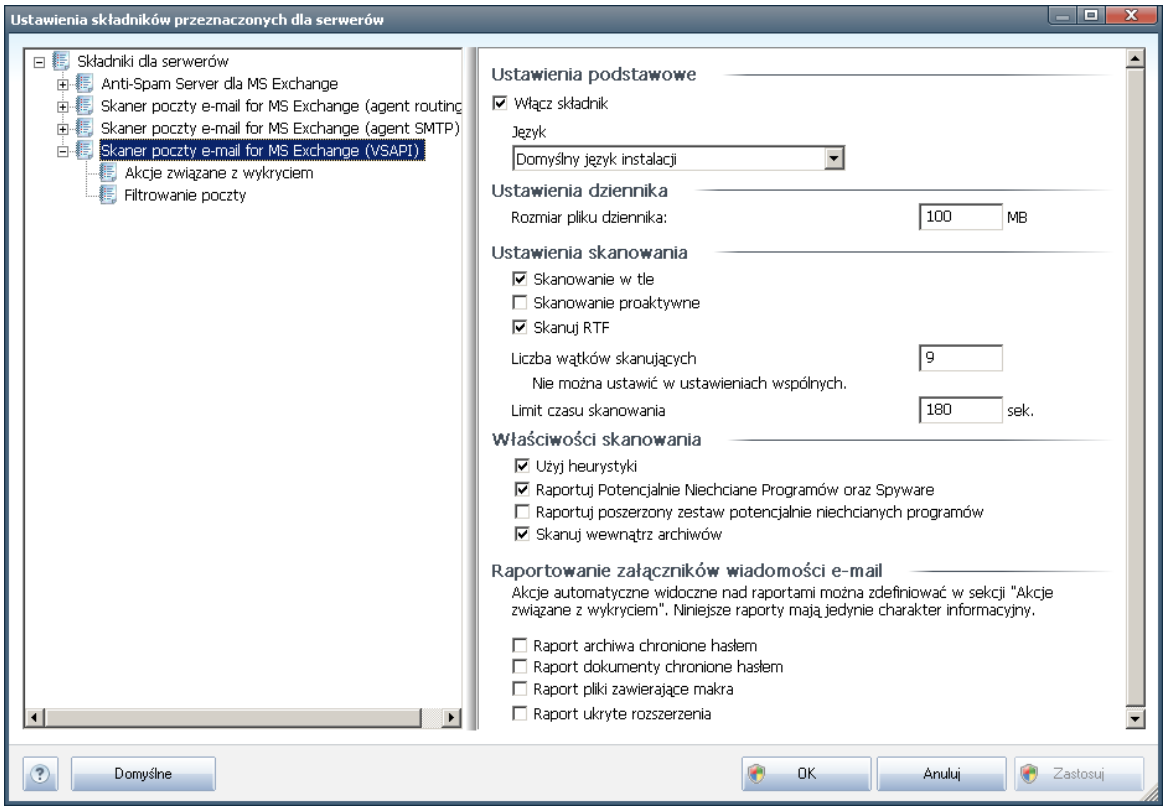
Konfiguracja ***Skanera poczty e-mail dla MS Exchange (agenta SMTP)*** jest dokladnie taka sama jak w przypadku agenta routingu. Wiecej informacji na ten temat mozna znalezc w rozdziale ***Skaner poczty e-mail dla MS Exchange (routing TA)*** powyzej.

W strukturze drzewa dostepne sa nastepujace podpozycje:

- ***Akcje zwiazane z wykryciem***
- ***Filtrowanie poczty***

4.4. Skaner poczty e-mail dla MS Exchange (VSAPI)

Ta pozycja zawiera ustawienia ***Skanera dokumentów dla serwera MS Exchange (VSAPI)***.



Sekcja ***Ustawienia podstawowe*** zawiera nastepujace opcje:

- ***Wlacz skladnik*** - usuniecie zaznaczenia tej opcji spowoduje wylaczenie calego skladnika.
- ***Jezyk*** - wybierz preferowany jezyk skladnika.

Sekcja ***Ustawienia dziennika***:

- ***Rozmiar pliku dziennika*** - wybierz preferowany rozmiar pliku dziennika. Wartosc domyslna: 100 MB.

Sekcja ***Ustawienia skanowania***:

- ***Skanowanie w tle*** - to pole wyboru umozliwia wlaczenie lub wylaczenie mozliwosci skanowania w tle. Skanowanie w tle jest jedna z funkcji interfejsu aplikacji VSAPI 2.0/2.5. Zapewnia wielowatkowe skanowanie baz danych serwera Exchange. Zawsze gdy w folderach skrzynki pocztowej uzytkownika pojawi sie element, który nie byl skanowany przy uzyciu najnowszej wersji bazy danych, jest on przesylany do programu AVG dla serwera Exchange Server. Skanowanie i wyszukiwanie obiektów, które nie zostaly jeszcze przeskanowane odbywa sie równolegle.

  Dla kazdej bazy danych stosowany jest okreslony watek o niskim priorytecie, co gwarantuje, ze inne zadania (np. magazynowanie wiadomosci e-mail w bazie danych Microsoft Exchange) zawsze sa realizowane jako pierwsze.

- ***Skanowanie proaktywne (wiadomosci przychodzace)***

  W tym miejscu mozliwe jest wlaczenie lub wylaczenie funkcji proaktywnego skanowania przy uzyciu interfejsu VSAPI 2.0/2.5. Skanowanie to ma miejsce, gdy wiadomosc zostala juz zapisana w folderze, lecz klient nie zazadal jeszcze jej przeskanowania.

  Po przeslaniu do serwera Exchange, wiadomosci zostaja umieszczone w globalnej kolejce skanowania i otrzymuja niski priorytet (maksymalnie 30 pozycji). Skanowanie opiera sie w oparciu o schemat FIFO (first in, first out). Jesli uzytkownik chce uzyskac dostep do danej wiadomosci podczas gdy jest ona umieszczona w kolejce, jej priorytet zostaje zmieniony na wysoki.

  Uwaga: *Wiadomosci niemieszczace sie w kolejce zostana przekazane na serwer bez skanowania.*

Uwaga: *Nawet jesli zostana wylaczone obie opcje -* ***Skanowanie w tle*** *i* ***Skanowanie proaktywne****, skaner dostepowy bedzie wciaz aktywny przy próbie pobrania wiadomosci za pomoca klienta MS Outlook.*

- ***Skanowanie plików RTF*** - w tym miejscu mozliwe jest okreslenie, czy maja byc skanowane pliki RTF.
- ***Liczba watków skanujacych*** - proces skanowania jest domyslnie podzielony na okreslona liczbe jednoczesnie wykonywanych watków (w celu zwiekszenia ogólnej wydajnosci skanowania). W tym polu mozna zmienic liczbe watków.

  Domyslna liczba watków jest obliczana wedlug wzoru: 2 * liczba procesorów + 1.

  Minimalna liczba watków jest obliczana wedlug wzoru: (liczba procesorów + 1) podzielona przez 2.

  Maksymalna liczba watków jest obliczana wedlug wzoru: (liczba procesorów pomnozona przez 5) + 1.

W przypadku, gdy wartosc jest równa minimalnej (lub od niej mniejsza) badz równa maksymalnej (lub od niej wieksza), uzyta zostanie wartosc domyslna.

- ***Limit czasu skanowania*** - maksymalny czas (w sekundach) dostepu jednego watku do skanowanej wiadomosci (wartosc domyslna to 180 sekund).

Sekcja ***Wlasciwosci skanowania***:

- ***Uzyj heurystyki*** - zaznacz to pole, aby wlaczyc analize heurystyczna podczas skanowania.

- ***Raportowanie potencjalnie niechcianych programów i programów typu spyware*** - te opcje nalezy zaznaczyc, aby raportowana byla obecnosc potencjalnie niechcianych programów i programów typu spyware.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - zaznaczenie tego pola umozliwi wykrycie wiekszych ilosci oprogramowania szpiegujacego, tj. programów, które przy zakupie bezposrednio od producenta sa calkowicie nieszkodliwe, lecz pózniej moga zostac uzyte niezgodnie z przeznaczeniem lub w celu wyrzadzenia szkody (np. rózne paski narzedzi). To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera oraz podniesienie komfortu pracy. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona. Uwaga: Ta funkcja detekcji stanowi uzupelnienie poprzedniej opcji, dlatego w celu zapewnienia ochrony przed podstawowymi rodzajami oprogramowania szpiegujacego poprzednie pole wyboru powinno byc zawsze zaznaczone.

- ***Skanuj wewnatrz archiwów*** - opcje te nalezy zaznaczyc, aby umozliwic skanerowi skanowanie równiez wewnatrz archiwów (zip, rar itp.)

W sekcji ***Raportowanie zalaczników wiadomosci e-mail*** mozliwe jest wybranie pozycji, które maja byc raportowane podczas skanowania. Domyslna konfiguracja moze zostac latwo dostosowana w obszarze ***Informacje*** w sekcji ***Akcje zwiazane z wykryciem*** (patrz nizej).

Dostepne sa nastepujace opcje:

- ***Powiadamiaj o archiwach chronionych haslem***

- ***Powiadamiaj o dokumentach chronionych haslem***

- ***Powiadamiaj o plikach zawierajacych makra***

- ***Powiadamiaj o ukrytych rozszerzeniach***

Generalnie niektóre sposród funkcji sa rozszerzeniami uslug interfejsu aplikacji Microsoft VSAPI 2.0/2.5. Szczególowe informacje na temat interfejsu VSAPI 2.0/2.5 mozna znalezc po kliknieciu ponizszych laczy (a takze laczy znajdujacych sie na tych stronach):

- http://support.microsoft.com/default.aspx?scid=kb;pl-pl;328841&Product=exch2k - informacje na temat wspólpracy serwera

Exchange i oprogramowania antywirusowego.

- http://support.microsoft.com/default.aspx?scid=kb;pl-pl;823166 - informacje na temat dodatkowych funkcji interfejsu VSAPI 2.5 serwera Exchange 2003.

W strukturze drzewa dostepne sa nastepujace pozycje:

- ***Akcje zwiazane z wykrywaniem***
- ***Filtrowanie poczty***

4.5. Uwaga techniczna

Ta informacja dotyczy sytuacji, w której podczas instalacji uzywany jest jednoczesnie interfejs VSAPI i agent transportowy routingu w roli Hub Exchange. Wówczas wiadomosci e-mail beda skanowane dwukrotnie (najpierw przez skaner dostepowy interfejsu VSAPI, a nastepnie przez agenta transportowego routingu).

Z powodu sposobu dzialania interfejsu VSAPI mozliwe jest wystapienie niezgodnosci wyników skanowania i niepotrzebne obciazenia systemu. Dlatego tez aby uniknac podwójnego skanowania zaleca sie wprowadzenie malej poprawki (patrz ponizej), która pozwoli rozwiazac ten problem.

Uwaga: *Dostosowywanie rejestru powinno byc przeprowadzane tylko przez zaawansowanych uzytkowników. Przed kazdym edytowaniem rejestru zaleca sie utworzenie kopii zapasowej rejestru i sprawdzenie, w jaki sposób mozna przywrócic poprzednie ustawienia na wypadek wystapienia problemów.*

Otwórz edytor rejestru (po wybraniu menu ***Start/Uruchom*** wprowadz wartosc ***regedit*** i nacisnij klawisz enter). Przejdz do nastepujacej galezi:

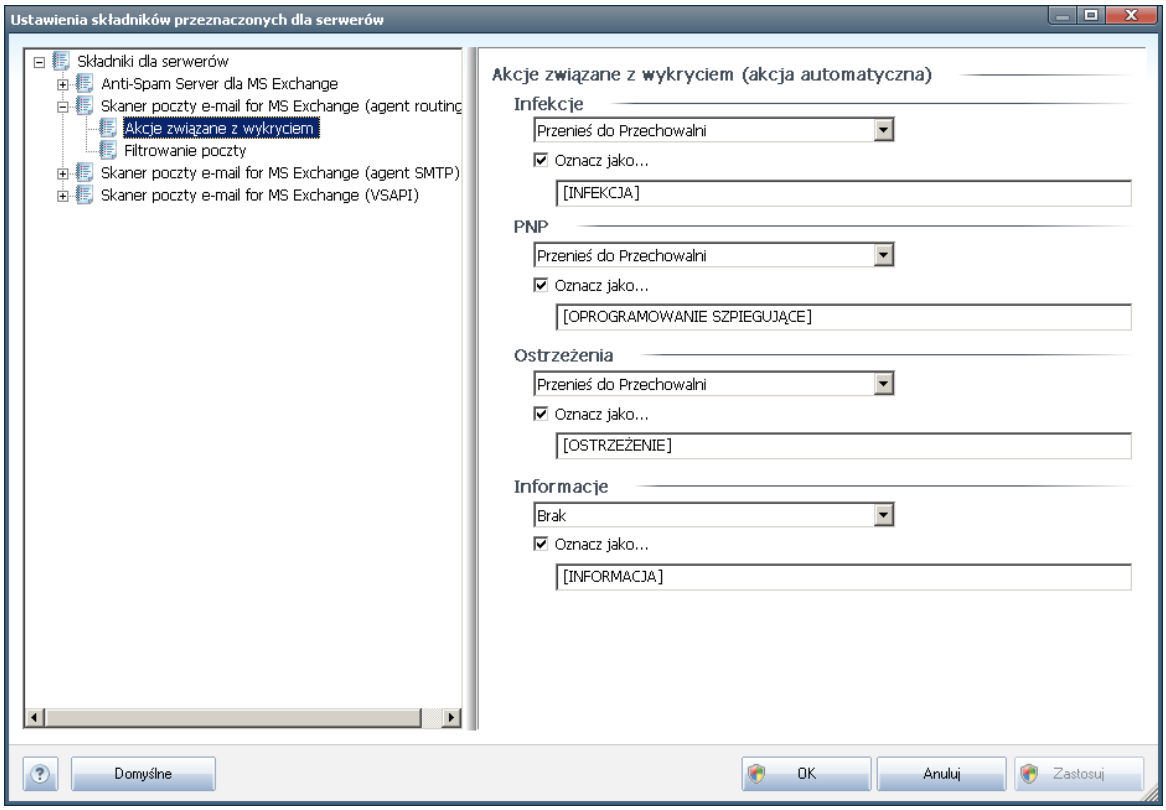
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan

Prawym przyciskiem myszy kliknij prawa czesc okna i z menu kontekstowego wybierz opcje ***Nowy/Wartosc DWORD (32-bitowa)***. Nazwij nowa wartosc ***TransportExclusion***. Po jej utworzeniu kliknij ja dwukrotnie, a nastepnie zmien wartosc na ***1***.

Na koniec, aby zastosowac zmiany dla serwera MS Exchange, ustaw wartosc „1” dla opcji ***ReloadNow***. Aby to zrobic, dwukrotnie ja kliknij i zmien jej wartosc.

Dzieki temu wylaczysz dostepowy skaner wychodzacych wiadomosci interfejsu VSAPI. Zmiana powinna zostac zastosowana w ciagu kilku minut.

4.6. Akcje zwiazane z wykrywaniem



Z sekcji ***Akcje zwiazane z wykryciem*** mozna wybrac automatyczne akcje, które maja byc wykonywane podczas procesu skanowania.

Akcje te sa dostepne dla nastepujacych pozycji:

- ***Infekcje***
- ***PNP (Potencjalnie Niechciane Programy)***
- ***Ostrzezenia***
- ***Informacje***

Z menu rozwijanego mozna wybrac akcje dla kazdej pozycji:

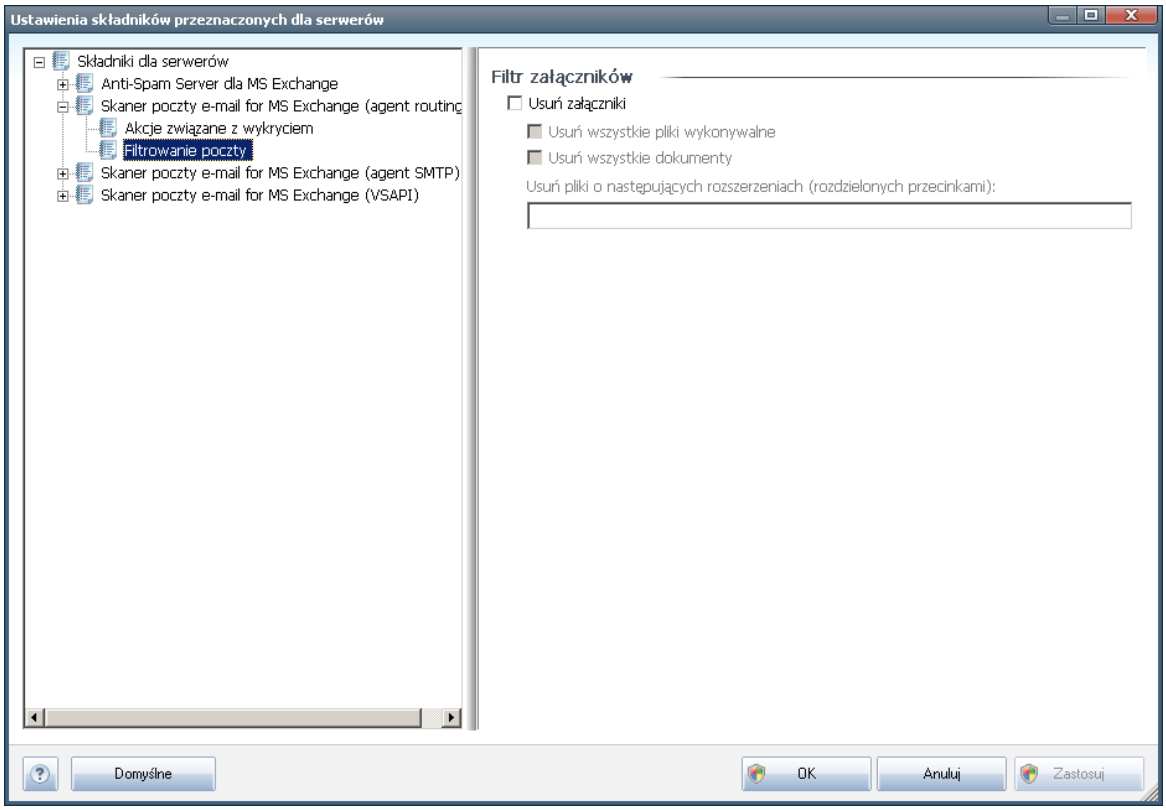
- ***Brak*** - nie zostanie podjeta zadna akcja.
- ***Przenies do Przechowalni*** - dane zagrozenie zostanie przeniesione do Przechowalni wirusów.
- ***Usun*** - dane zagrozenie zostanie usuniete.

Aby wybrac niestandardowy temat dla wiadomosci zawierajacych okreslona pozycje

lub zagrozenie, zaznacz pole ***Oznacz temat...*** i wprowadz odpowiednia wartosc.

Uwaga: *Ostatnia wymieniona funkcja nie jest dostepna dla Skanera poczty e-mail dla MS Exchange VSAPI.*

4.7. Filtrowanie poczty



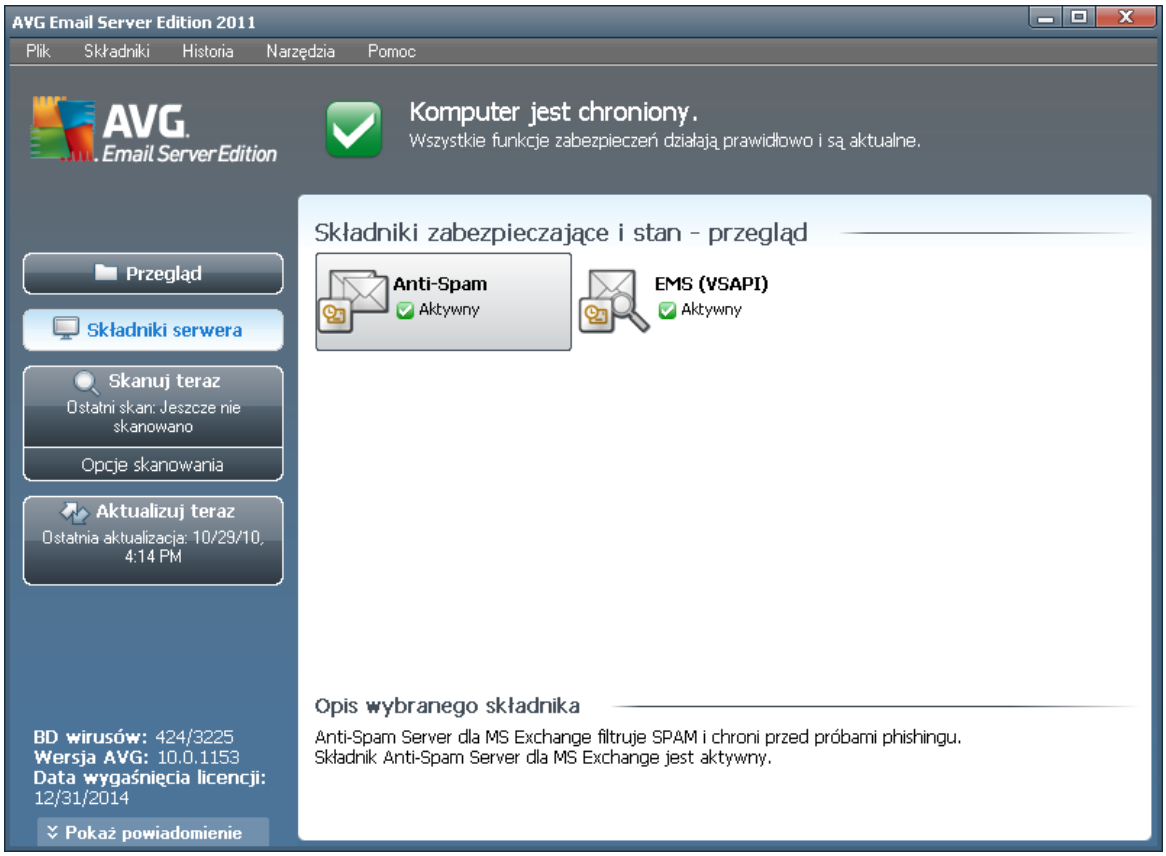
Pozycja ***Filtrowanie poczty*** umozliwia wybór zalaczników, które beda automatycznie usuwane. Dostepne sa nastepujace opcje:

- ***Usuwaj zalaczniki*** - zaznacz to pole wyboru, aby wlaczyc te funkcje.
- ***Usun wszystkie pliki wykonywalne*** - usuwa wszystkie pliki wykonywalne.
- ***Usun wszystkie dokumenty*** - usuwa wszystkie dokumenty.
- ***Usun pliki o nastepujacych rozszerzeniach (rozdzielonych przecinkami)*** - w tym polu nalezy wprowadzic rozszerzenia plików, które maja byc automatycznie usuwane. Rozszerzenia nalezy rozdzielac przecinkami.

5. Skaner poczty e-mail dla serwera MS Exchange Server 2003

5.1. Przeglad

Opcje konfiguracji Skanera poczty-email dla MS Exchange Server 2003 sa w pelni zintegrowane z produktem AVG Email Server Edition 2011 (jako skladnik serwera.



Dostepne sa nastepujace skladniki serwera:

Podstawowy przeglad poszczególnych skladników serwera:

- ***Anti-Spam - Anti-Spam Server dla MS Exchange***

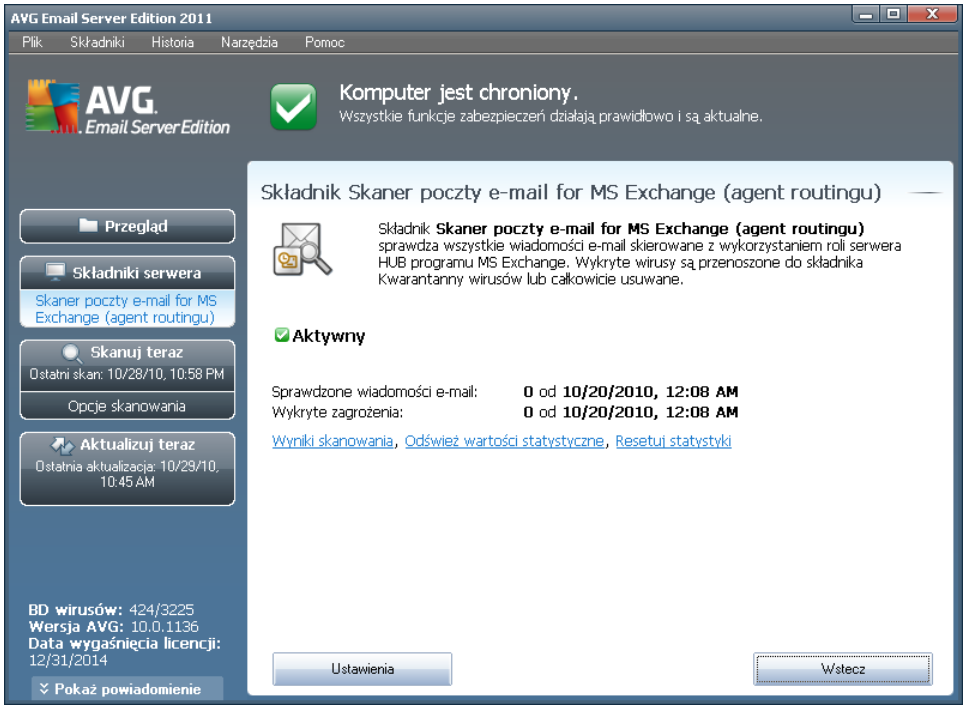
  Sprawdza wszystkie przychodzace wiadomosci e-mail i oznacza niepozadana poczte jako SPAM. Podczas przetwarzania kazdej wiadomosci wykorzystywanych jest kilka metod analizy, oferujacych najskuteczniejsza dostepna na rynku ochrone.

- ***EMS (VSAPI) - Skaner poczty e-mail dla MS Exchange (VSAPI)***

  Sprawdza wszystkie wiadomosci e-mail przechowywane w skrzynkach pocztowych uzytkownika. Wszystkie wykryte wirusy sa przenoszone do

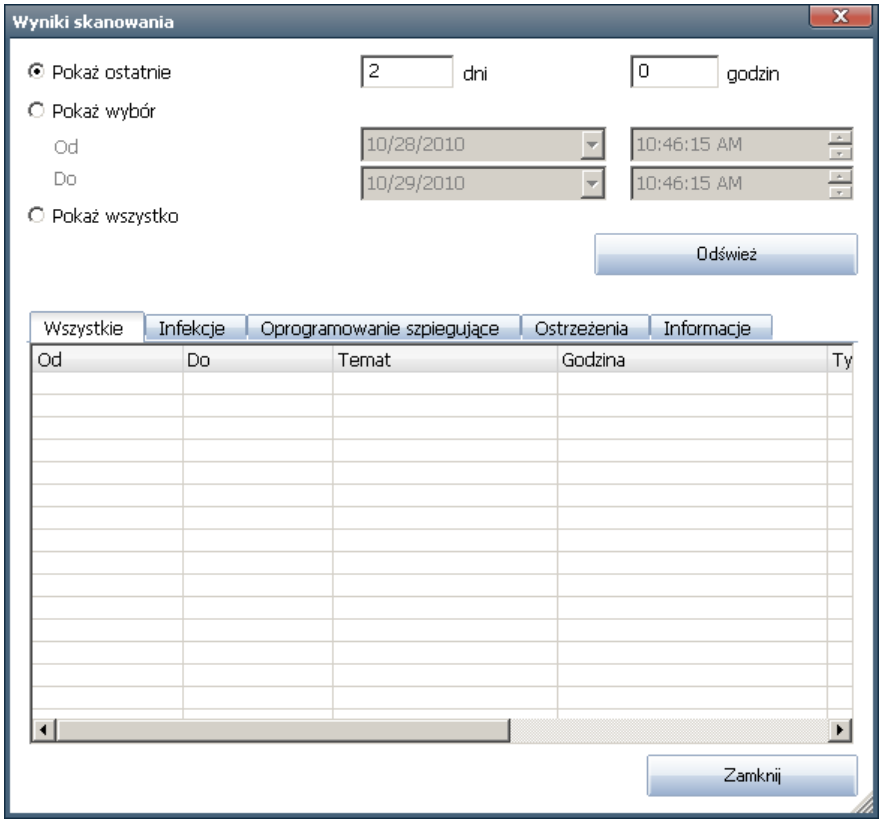
Przechowalni lub usuwane.

Dwukrotnie kliknij wybrany skladnik, aby otworzyc jego interfejs. Z wyjatkiem skladnika Anti-Spam wszystkie skladniki posiadaja wspólne przyciski i linki:



- ***Wyniki skanowania***

  Otwiera nowe okno dialogowe, w którym dostepny jest przeglad wyników skanowania:



W tym miejscu mozna sprawdzic wiadomosci podzielone na kilka kart - wedlug poziomu zagrozenia. Poziomy zagrozenia i raportowania mozna dostosowac w konfiguracji indywidualnych skladników.

Domyslnie wyswietlane sa tylko wyniki z ostatnich dwóch dni. Okres, dla którego wyswietlane sa wyniki, mozna dostosowac za pomoca nastepujacych opcji:

- ***Pokaz ostatnie*** - wprowadz preferowana ilosc dni i godzin.
- ***Pokaz wybrane*** - wprowadz niestandardowy przedzial czasu i daty.
- ***Pokaz wszystko*** - wyswietla wszystkie dostepne wyniki.

Przycisk ***Odswiez*** sluzy do ponownego zaladowania wyników.

- ***Odswiez wartosci statystyczne*** - aktualizuje powyzsze statystyki.
- ***Resetuj wartosci statystyczne*** - zeruje wszystkie statystyki.

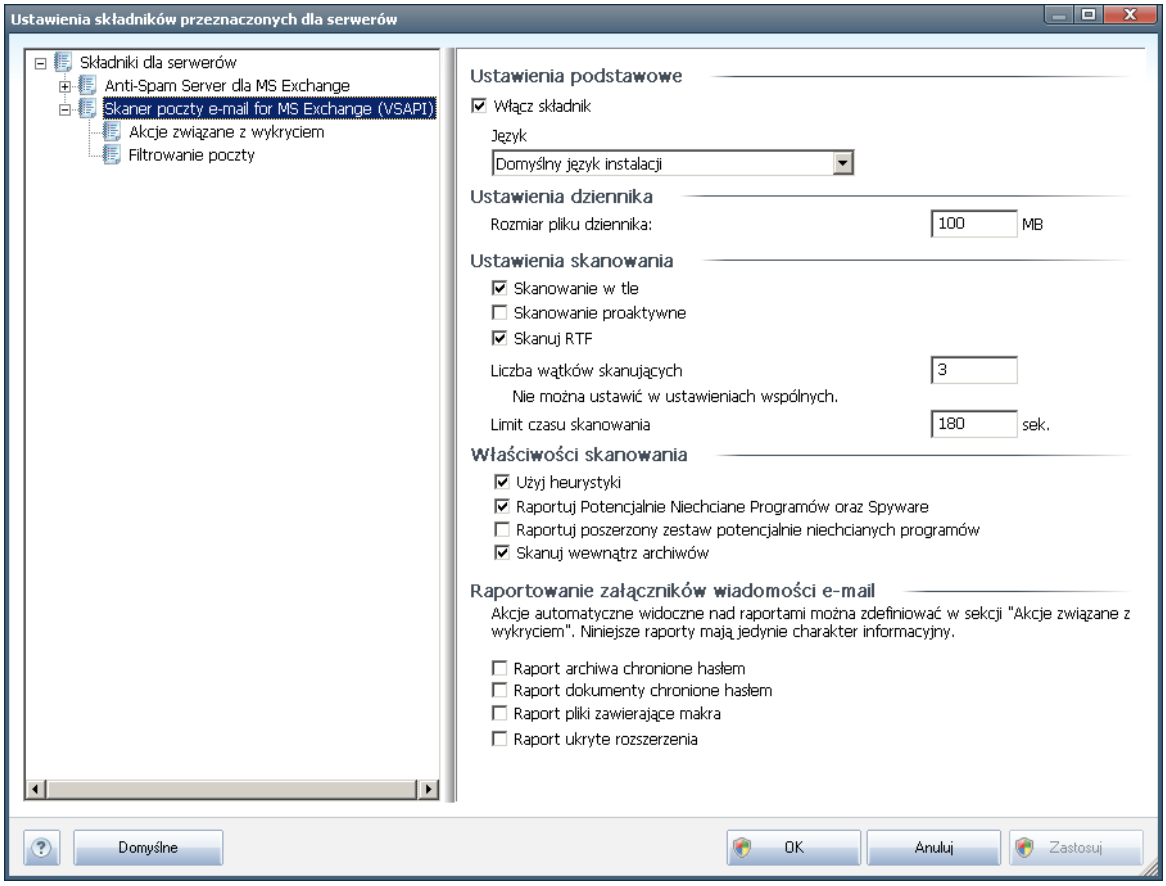
Dostepne przyciski:

- ***Ustawienia*** - ten przycisk pozwala otworzyc ustawienia skladnika.
- ***Wstecz*** - ten przycisk umozliwia powrót do okna Przeglad skladników serwera.

Wiecej informacji na temat indywidualnych ustawien wszystkich skladników mozna znalezc w rozdzialach ponizej.

5.2. Skaner poczty e-mail dla MS Exchange (VSAPI)

Ta pozycja zawiera ustawienia ***Skanera dokumentów dla serwera MS Exchange (VSAPI)***.



Sekcja ***Ustawienia podstawowe*** zawiera nastepujace opcje:

- ***Wlacz skladnik*** - usuniecie zaznaczenia tej opcji spowoduje wylaczenie calego skladnika.
- ***Jezyk*** - wybierz preferowany jezyk skladnika.

Sekcja ***Ustawienia dziennika***:

- ***Rozmiar pliku dziennika*** - wybierz preferowany rozmiar pliku dziennika. Wartosc domyslna: 100 MB.

Sekcja ***Ustawienia skanowania***:

- ***Skanowanie w tle*** - to pole wyboru umozliwia wlaczenie lub wylaczenie mozliwosci skanowania w tle. Skanowanie w tle jest jedna z funkcji interfejsu aplikacji VSAPI 2.0/2.5. Zapewnia wielowatkowe skanowanie baz danych serwera Exchange. Zawsze gdy w folderach skrzynki pocztowej uzytkownika pojawi sie element, który nie byl skanowany przy uzyciu najnowszej wersji bazy danych, jest on przesylany do programu AVG dla serwera Exchange Server. Skanowanie i wyszukiwanie obiektów, które nie zostaly jeszcze przeskanowane odbywa sie równolegle.

  Dla kazdej bazy danych stosowany jest okreslony watek o niskim priorytecie, co gwarantuje, ze inne zadania (np. magazynowanie wiadomosci e-mail w bazie danych Microsoft Exchange) zawsze sa realizowane jako pierwsze.

- ***Skanowanie proaktywne (wiadomosci przychodzace)***

  W tym miejscu mozliwe jest wlaczenie lub wylaczenie funkcji proaktywnego skanowania przy uzyciu interfejsu VSAPI 2.0/2.5. Skanowanie to ma miejsce, gdy wiadomosc zostala juz zapisana w folderze, lecz klient nie zazadal jeszcze jej przeskanowania.

  Po przeslaniu do serwera Exchange, wiadomosci zostaja umieszczone w globalnej kolejce skanowania i otrzymuja niski priorytet (maksymalnie 30 pozycji). Skanowanie opiera sie w oparciu o schemat FIFO (first in, first out). Jesli uzytkownik chce uzyskac dostep do danej wiadomosci podczas gdy jest ona umieszczona w kolejce, jej priorytet zostaje zmieniony na wysoki.

  Uwaga: *Wiadomosci niemieszczace sie w kolejce zostana przekazane na serwer bez skanowania.*

Uwaga: *Nawet jesli zostana wylaczone obie opcje -* ***Skanowanie w tle*** *i* ***Skanowanie proaktywne****, skaner dostepowy bedzie wciaz aktywny przy próbie pobrania wiadomosci za pomoca klienta MS Outlook.*

- ***Skanowanie plików RTF*** - w tym miejscu mozliwe jest okreslenie, czy maja byc skanowane pliki RTF.
- ***Liczba watków skanujacych*** - proces skanowania jest domyslnie podzielony na okreslona liczbe jednoczesnie wykonywanych watków (w celu zwiekszenia ogólnej wydajnosci skanowania). W tym polu mozna zmienic liczbe watków.

  Domyslna liczba watków jest obliczana wedlug wzoru: 2 * liczba procesorów + 1.

  Minimalna liczba watków jest obliczana wedlug wzoru: (liczba procesorów + 1) podzielona przez 2.

  Maksymalna liczba watków jest obliczana wedlug wzoru: (liczba procesorów pomnozona przez 5) + 1.

  W przypadku, gdy wartosc jest równa minimalnej (lub od niej mniejsza) badz równa maksymalnej (lub od niej wieksza), uzyta zostanie wartosc domyslna.

- ***Limit czasu skanowania*** - maksymalny czas (w sekundach) dostepu jednego watku do skanowanej wiadomosci (wartosc domyslna to 180 sekund).

Sekcja ***Wlasciwosci skanowania***:

- ***Uzyj heurystyki*** - zaznacz to pole, aby wlaczyc analize heurystyczna podczas skanowania.
- ***Raportowanie potencjalnie niechcianych programów i programów typu spyware*** - te opcje nalezy zaznaczyc, aby raportowana byla obecnosc potencjalnie niechcianych programów i programów typu spyware.
- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - zaznaczenie tego pola umozliwi wykrycie wiekszych ilosci oprogramowania szpiegujacego, tj. programów, które przy zakupie bezposrednio od producenta sa calkowicie nieszkodliwe, lecz pózniej moga zostac uzyte niezgodnie z przeznaczeniem lub w celu wyrzadzenia szkody (np. rózne paski narzedzi). To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera oraz podniesienie komfortu pracy. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona. Uwaga: Ta funkcja detekcji stanowi uzupelnienie poprzedniej opcji, dlatego w celu zapewnienia ochrony przed podstawowymi rodzajami oprogramowania szpiegujacego poprzednie pole wyboru powinno byc zawsze zaznaczone.
- ***Skanuj wewnatrz archiwów*** - opcje te nalezy zaznaczyc, aby umozliwic skanerowi skanowanie równiez wewnatrz archiwów (zip, rar itp.)

W sekcji ***Raportowanie zalaczników wiadomosci e-mail*** mozliwe jest wybranie pozycji, które maja byc raportowane podczas skanowania. Domyslna konfiguracja moze zostac latwo dostosowana w obszarze ***Informacje***, w sekcji ***Akcje zwiazane z wykrywaniem*** (patrz nizej).

Dostepne sa nastepujace opcje:

- ***Powiadamiaj o archiwach chronionych haslem***
- ***Powiadamiaj o dokumentach chronionych haslem***
- ***Powiadamiaj o plikach zawierajacych makra***
- ***Powiadamiaj o ukrytych rozszerzeniach***

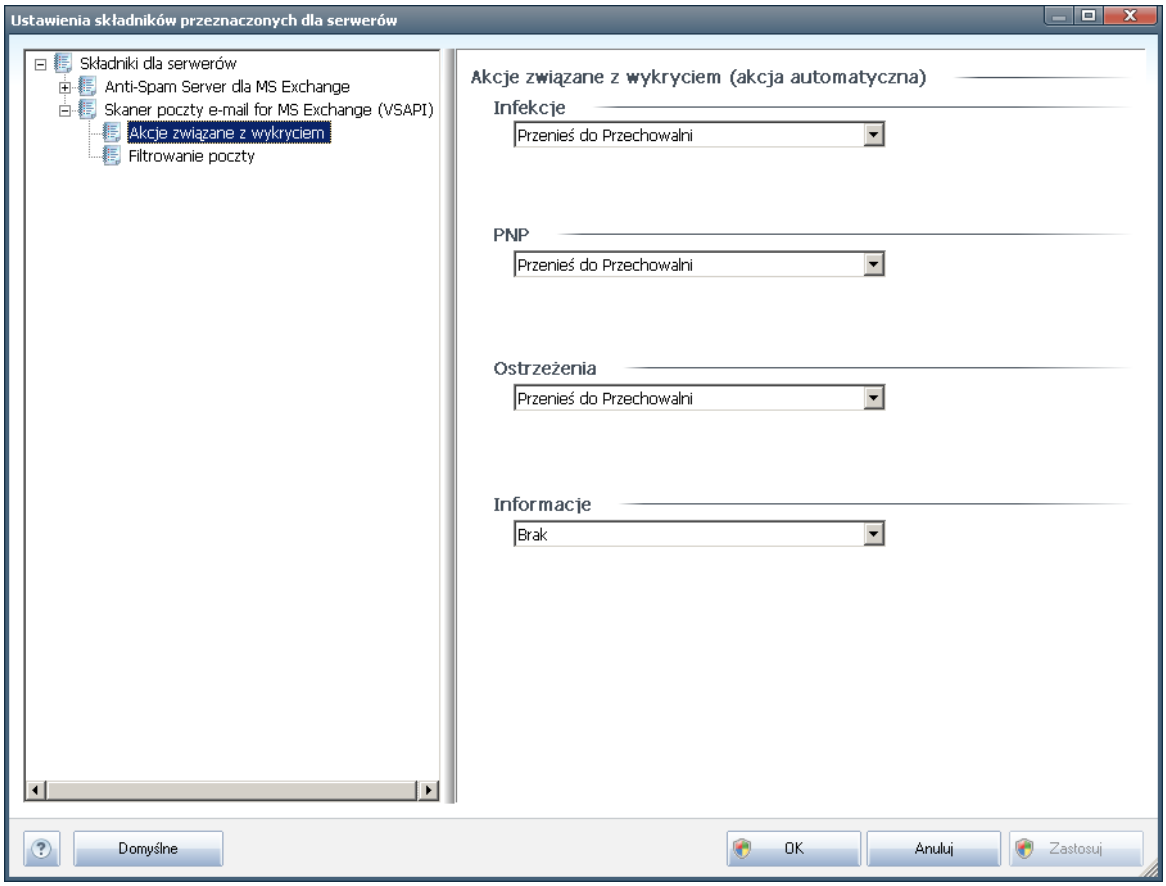
Generalnie, wszystkie te funkcje sa rozszerzeniami uslug interfejsu Microsoft VSAPI 2.0/2.5. Szczególowe informacje na temat interfejsu VSAPI 2.0/2.5 mozna znalezc, odwiedzajac ponizsze linki (oraz linki znajdujace na tych stronach):

- http://support.microsoft.com/default.aspx?scid=kb;pl-pl;328841&Product=exch2k - informacje na temat wspólpracy serwera Exchange i oprogramowania antywirusowego.
- http://support.microsoft.com/default.aspx?scid=kb;pl-pl;823166 - informacje na temat dodatkowych funkcji interfejsu VSAPI 2.5 serwera Exchange 2003.

W strukturze drzewa dostepne sa nastepujace pozycje:

- ***Akcje zwiazane z wykrywaniem***
- ***Filtrowanie poczty***

5.3. Akcje zwiazane z wykrywaniem



Z sekcji ***Akcje zwiazane z wykryciem*** mozna wybrac automatyczne akcje, które maja byc wykonywane podczas procesu skanowania.

Akcje te sa dostepne dla nastepujacych pozycji:

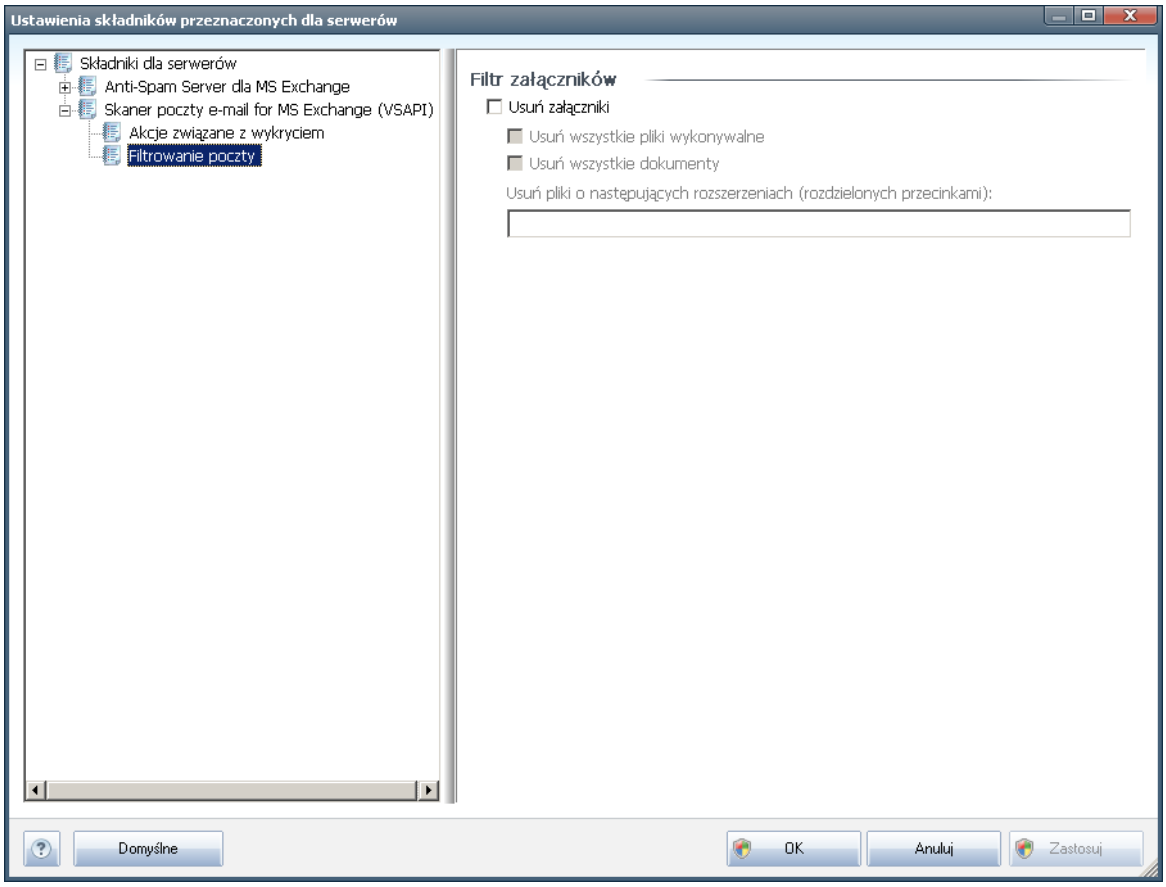
- ***Infekcje***
- ***PNP (Potencjalnie Niechciane Programy)***
- ***Ostrzezenia***
- ***Informacje***

Z menu rozwijanego mozna wybrac akcje dla kazdej pozycji:

- ***Brak*** - nie zostanie podjeta zadna akcja.

- ***Przenies do Przechowalni*** - dane zagrozenie zostanie przeniesione do Przechowalni wirusów.
- ***Usun*** - dane zagrozenie zostanie usuniete.

5.4. Filtrowanie poczty



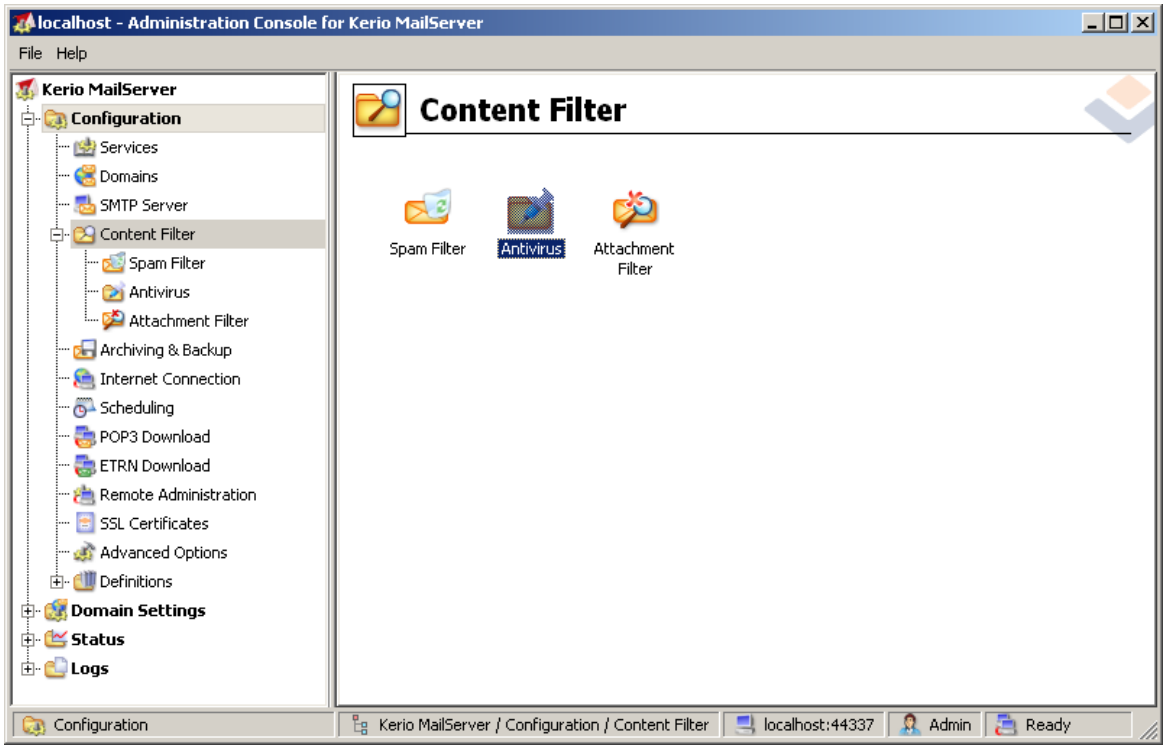
Pozycja ***Filtrowanie poczty*** umozliwia wybór zalaczników, które beda automatycznie usuwane. Dostepne sa nastepujace opcje:

- ***Usuwaj zalaczniki*** - zaznacz to pole wyboru, aby wlaczyc te funkcje.
- ***Usun wszystkie pliki wykonywalne*** - usuwa wszystkie pliki wykonywalne.
- ***Usun wszystkie dokumenty*** - usuwa wszystkie dokumenty.
- ***Usun pliki o nastepujacych rozszerzeniach (rozdzielonych przecinkami)*** - w tym polu nalezy wprowadzic rozszerzenia plików, które maja byc automatycznie usuwane. Rozszerzenia nalezy rozdzielac przecinkami.

6. AVG dla Kerio MailServer

6.1. Konfiguracja

Mechanizm ochrony antywirusowej jest wbudowany w aplikacje Kerio MailServer. W celu aktywowania ochrony poczty e-mail w programie Kerio MailServer za pomoca silnika skanujacego AVG, nalezy uruchomic aplikacje Kerio Administration Console. W drzewie nawigacji po lewej stronie okna nalezy wybrac galaz Filtr zawartosci (znajdujaca sie w galezi Konfiguracja):

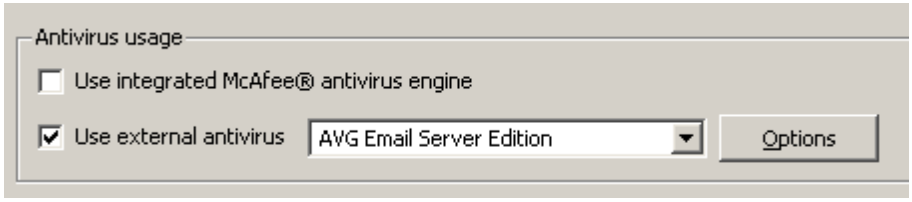


Kliknięcie pozycji Filtr zawartosci wyswietli okno dialogowe zawierajace trzy pozycje:

- ***Filtr antyspamowy***
- ***Program antywirusowy*** (patrz sekcja ***Program antywirusowy***)
- ***Filtr zalaczników*** (patrz sekcja ***Filtr zalaczników***)

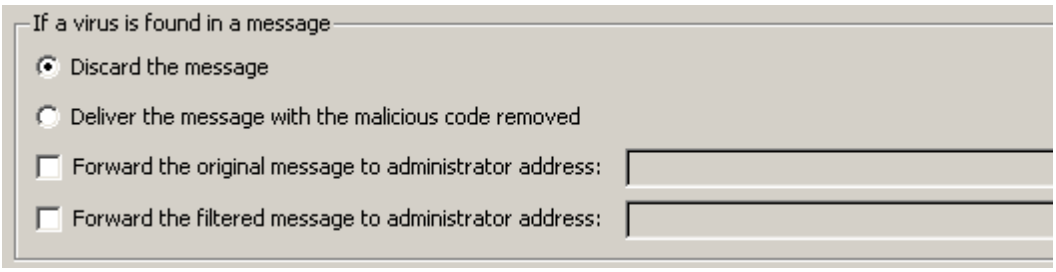
6.1.1. Ochrona antywirusowa

Aby aktywowac program AVG dla Kerio MailServer, nalezy zaznaczyc pole wyboru Uzywaj zewnetrznego programu antywirusowego, a nastepnie z menu wybrac program AVG Email Server Edition w oknie konfiguracyjnym:



W nastepnej sekcji mozna okreslic, jakie akcje maja zostac podjete w stosunku do wiadomosci zainfekowanych lub spelniajacych kryteria filtrowania:

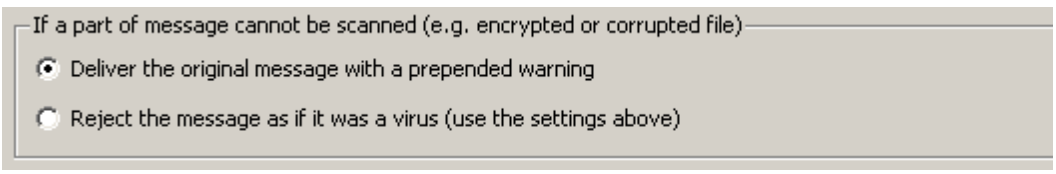
- ***W przypadku wykrycia wirusa w wiadomosci e-mail***



W tej ramce mozna okreslic akcje, które maja zostac wykonane w przypadku wykrycia wirusa w wiadomosci lub wyfiltrowania wiadomosci z zalacznikiem na podstawie ustawien filtru zalaczników:

  - ***Usun wiadomosc*** - po wybraniu tej opcji wiadomosc zainfekowana lub spelniajaca kryteria filtrowania bedzie usuwana.
  - ***Dostarcz wiadomosc z usunietym szkodliwym kodem*** - po wybraniu tej opcji wiadomosc zostanie dostarczona do odbiorcy bez potencjalnie szkodliwego zalacznika.
  - ***Przekaz oryginalna wiadomosc na adres administratora*** - po wybraniu tej opcji wiadomosc zainfekowana wirusem bedzie przekazywana na adres okreslony w polu tekstowym.
  - ***Przekaz wiadomosc spelniajaca kryteria filtrowania na adres administratora*** - po wybraniu tej opcji wiadomosc spelniajaca kryteria filtrowania bedzie przekazywana na adres okreslony w polu tekstowym.

- ***W przypadku gdy nie mozna przeskanowac czesci wiadomosci (np. uszkodzony lub zaszyfrowany plik)***



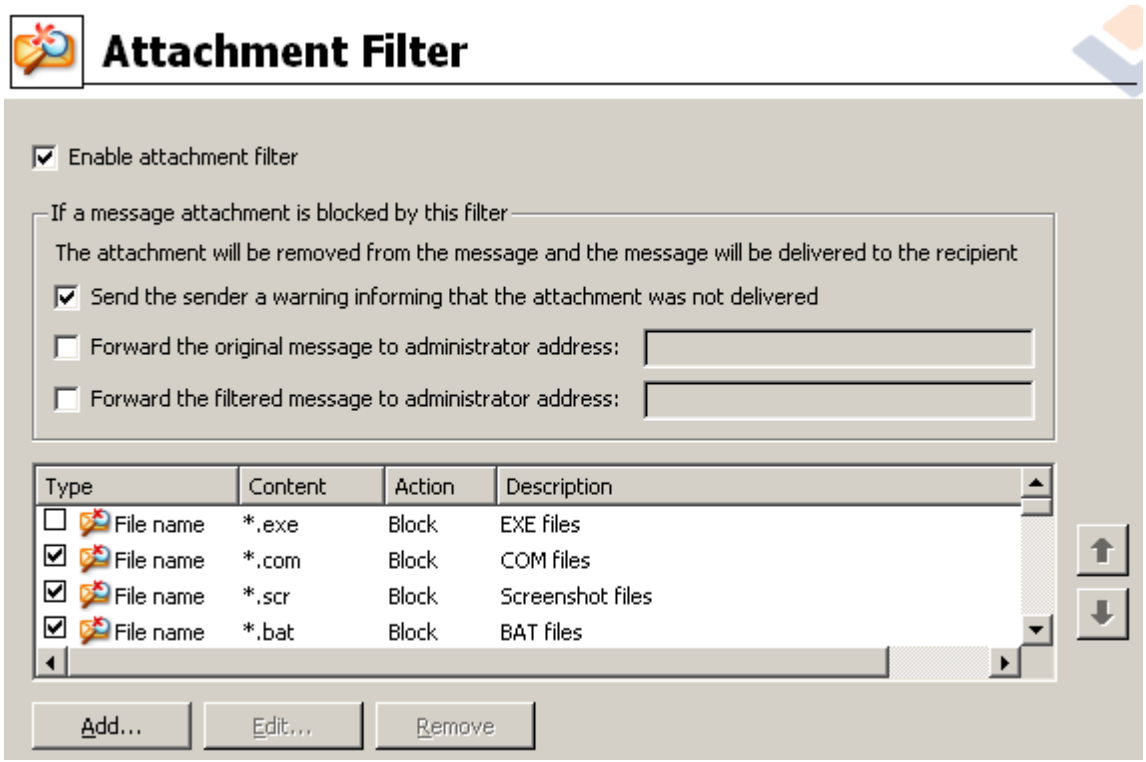
W tej ramce mozna okreslic akcje, które maja zostac wykonane w przypadku, gdy nie mozna przeskanowac czesci wiadomosci lub zalacznika:

- ***Dostarcz oryginalna wiadomosc z przygotowanym ostrzezeniem - wiadomosc (lub zalacznik) bedzie dostarczany bez sprawdzania.*** Uzytkownik zostanie ostrzezony, ze wiadomosc moze w dalszym ciagu zawierac wirusy.

- ***Odrzuc wiadomosc tak, jak w przypadku wykrycia wirusa - system bedzie dzialal w taki sam sposób, jak w przypadku wykrycia wirusa (np. wiadomosc zostanie dostarczona bez zalaczników lub zostanie usunieta).*** Ta opcja jest bezpieczna, jednak przesylanie zabezpieczonych haslem archiwów nie bedzie mozliwe.

6.1.2. Filtr zalaczników

Menu Filtr zalaczników zawiera liste róznych definicji zalaczników:



Filtrowanie zalaczników wiadomosci e-mail mozna wlaczyc lub wylaczyc za pomoca pola wyboru Wlacz filtr zalaczników. Mozna takze modyfikowac nastepujace ustawienia:

- ***Wysylaj do nadawcy ostrzezenia, ze zalacznik nie zostal dostarczony***

  Nadawca otrzyma ostrzezenie z serwera Kerio MailServer, o tym ze wyslana wiadomosc zawierala wirusa lub zablokowany zalacznik.

- ***Przesylaj oryginalna wiadomosci na adres administratora***

  Wiadomosc zostanie przekazana (w pierwotnej formie - z zainfekowanym lub

niedozwolonym zalacznikiem) na okreslony, zewnetrzny lub wewnetrzny adres e-mail.

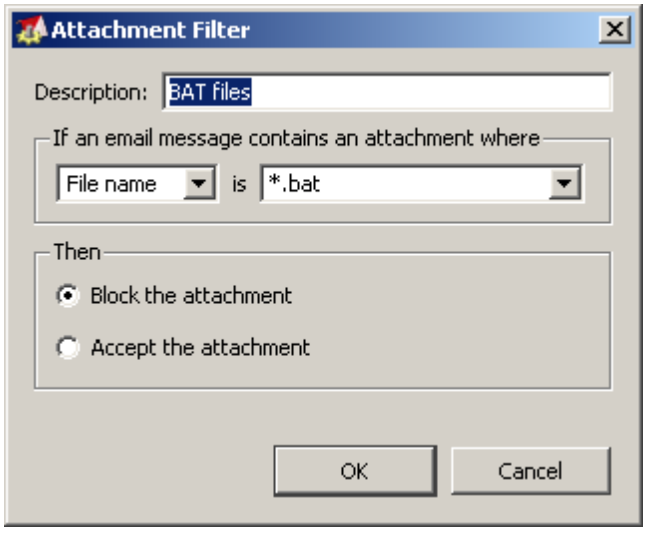
- ***Przesylaj wiadomosci spelniajaca kryteria filtrowania na adres administratora***

  Wiadomosc bez zainfekowanego lub niedozwolonego zalacznika zostanie (niezaleznie od innych podjetych akcji) przekazana na okreslony adres e-mail. Te funkcje mozna wykorzystac do sprawdzenia poprawnosci dzialania mechanizmu antywirusowego lub filtru zalaczników.

Kazda pozycja na liscie zalaczników ma cztery pola:

- ***Typ*** - rodzaj zalacznika okreslony na podstawie rozszerzenia podanego w polu Zawartosc. Dostepne typy to Nazwa pliku lub Typ MIME. Aby uwzglednic lub wykluczyc te pozycje w filtrowaniu zalaczników, mozna zaznaczyc odpowiednie pole.
- ***Zawartosc - w tym polu mozna okreslic rozszerzenie, które ma byc filtrowane.*** Dopuszczalne jest uzywanie znaków zastepczych (np. ciag "*.doc" oznacza wszystkie pliki z rozszerzeniem DOC).
- ***Akcja*** - okresla akcje, która ma zostac wykonana dla danego zalacznika. Dostepne akcje to Akceptuj (akceptuje zalacznik) i Blokuj (ta akcja zostanie wykonana zgodnie z ustawieniami znajdujacymi sie powyzej listy wykluczonych zalaczników).
- ***Opis*** - w tym polu nalezy wprowadzic opis zalacznika.

Pozycje mozna usunac z listy za pomoca przycisku Usun, a dodac - za pomoca przycisku ***Dodaj...***. Mozna takze zmienic istniejacy wpis za pomoca przycisku ***Edytuj.*** Zostanie wówczas wyswietlone ponizsze okno:



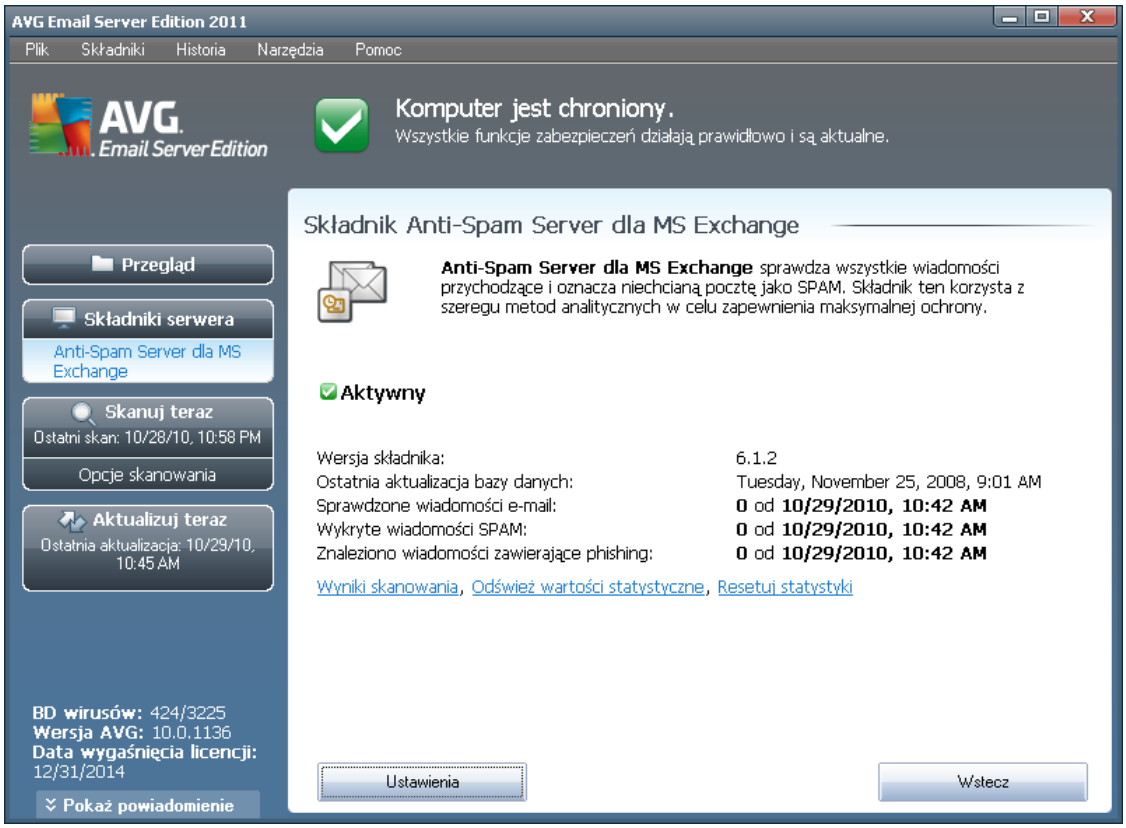
- W polu Opis mozna wpisac krótki opis zalacznika, który ma byc filtrowany.

- W polu Jesli wiadomosc e-mail zawiera zalacznik mozna wybrac typ zalacznika (Nazwa pliku lub Typ MIME). Dodatkowo mozna wybrac konkretne rozszerzenie z dostepnej listy lub uzyc symboli wieloznacznych.

W polu Wtedy mozna zdecydowac, czy okreslony zalacznik ma byc blokowany, czy akceptowany.

7. Konfiguracja skladnika Anti-Spam

7.1. Interfejs skladnika Anti-Spam

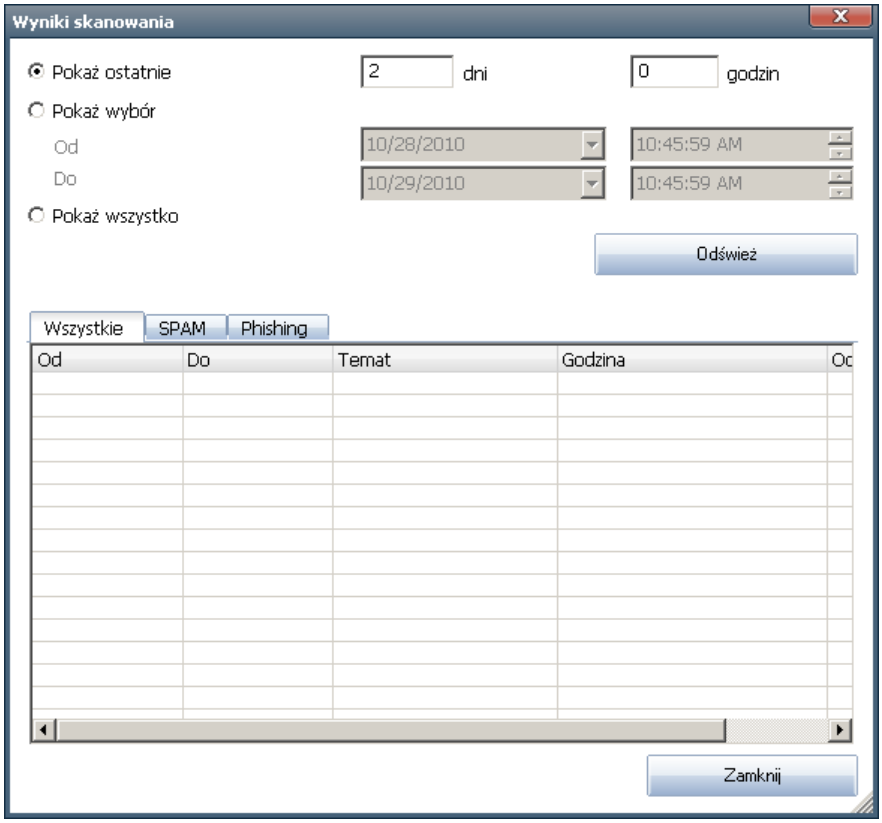


Okno dialogowe ***skladnika Anti-Spam*** Servermozna znalezc w sekcji ***Skladniki serwera*** (menu po lewej stronie). Zawiera ono krótka informacje o funkcjach skladnika oraz podsumowanie jego biezacego stanu (*Skladnik Anti-Spam Server for MS Exchange jest aktywny.*), a takze statystyki.

Dostepne linki:

- ***Wyniki skanowania***

  Otwiera nowe okno dialogowe, w którym dostepny jest przeglad wyników skanowania skladnika Anti-Spam:



W tym miejscu mozna sprawdzic wiadomosci wykryte jako SPAM (niepozadane) lub jako próba Phisingu (kradziezy danych osobowych, kont bankowych itp.). Domyslnie wyswietlane sa tylko wyniki z ostatnich dwóch dni. Okres, dla którego wyniki sa wyswietlane, mozna dostosowac za pomoca nastepujacych opcji:

- ***Pokaz ostatnie*** - wprowadz preferowana ilosc dni i godzin.
- ***Pokaz wybrane*** - wprowadz niestandardowy przedzial czasu i daty.
- ***Pokaz wszystko*** - wyswietla wszystkie dostepne wyniki.

Przycisk ***Odswiez*** sluzy do ponownego zaladowania wyników.

- ***Odswiez wartosci statystyczne*** - aktualizuje powyzsze statystyki.
- ***Resetuj wartosci statystyczne*** - zeruje wszystkie statystyki.

Dostepne przyciski:

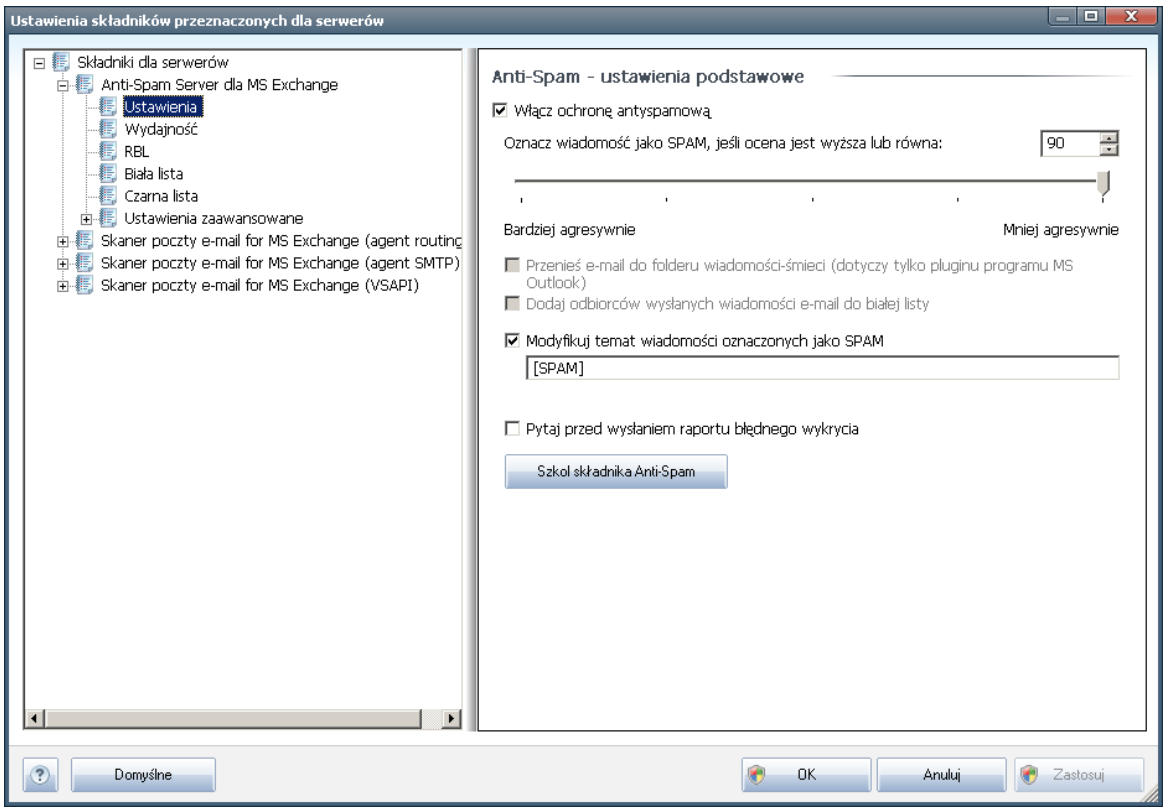
- ***Ustawienia*** - ten przycisk powoduje otwarcie okna Ustawienia skladnika Anti-Spam.
- ***Wstecz*** - ten przycisk umozliwia powrót do okna Przeglad skladników serwera.

7.2. Zasady dzialania skladnika Anti-Spam

Mianem spamu okresla sie niechciana poczte e-mail (głównie reklamy produktów lub uslug, które sa hurtowo rozsylane do wielkiej liczby odbiorców jednoczesnie, zapelniajac ich skrzynki pocztowe). Spamem nie jest korespondencja seryjna rozsylana do odbiorców po wyrazeniu przez nich zgody. Spam jest nie tylko irytujacy, ale moze byc równiez zródlem oszustw, wirusów i obrazliwych tresci.

Skladnik ***Anti-Spam*** sprawdza wszystkie przychodzace wiadomosci e-mail i oznacza te niepozadane jako SPAM. Podczas przetwarzania kazdej wiadomosci wykorzystywanych jest kilka metod analizy, oferujacych najskuteczniejsza dostepna na rynku ochrone.

7.3. Ustawienia skladnika Anti-Spam



W oknie dialogowym ***Podstawowe ustawienia skladnika Anti-Spam*** mozna zaznaczyc pole ***Wlacz ochrone antyspamowa***, aby wlaczyc/wylaczyc skanowanie wiadomosci e-mail w poszukiwaniu spamu.

W tym samym oknie mozna takze wybrac mniej lub bardziej agresywne metody oceny. Filtr ***Anti-Spam*** przypisuje kazdej wiadomosci ocene (*tj. wskaznik informujacy, jak bardzo jej tresc przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. Ustawienie ***Oznacz wiadomosc jako spam, jesli ocena jest wyzsza niz*** mozna dostosowac wpisujac wartosc (*od 50 do 90*) lub przesuwajac suwak w lewo lub w prawo.

Ponizej przedstawiono opis progów oceny:

- ***Wartosc 90*** - wiekszosc przychodzacych wiadomosci e-mail jest normalnie dostarczana (bez oznaczania ich jako spam). Spam, który latwo zidentyfikowac, jest odfiltrowywany, ale znaczna jego czesc ***moze nadal trafiac do Twojej skrzynki odbiorczej.

- ***Wartosc 80–89*** - wiadomosci e-mail, które stanowia potencjalny spam, sa poprawnie odfiltrowywane. Niektóre z pozadanych wiadomosci (niebedacych spamem) moga zostac blednie zablokowane.

- ***Wartosc 60–79*** - umiarkowanie agresywna konfiguracja. Wiadomosci e-mail, które moga stanowic spam, sa poprawnie odfiltrowywane. Pozadane wiadomosci (niebedace spamem) moga zostac blednie zablokowane.

- ***Wartosc 50–59*** - bardzo agresywna konfiguracja. Pozadane wiadomosci e-mail sa odfiltrowywane w równym stopniu, jak wiadomosci stanowiace spam. Nie zalecamy stosowania tego progu podczas normalnej pracy.

Nastepnie mozna zdefiniowac, jakie akcje maja zostac podjete wobec wiadomosci e-mail wykrytych jako spam:

- ***Zmodyfikuj temat wiadomosci oznaczonych jako spam*** - jesli opcja ta jest zaznaczona, wszystkie wykryte wiadomosci zawierajace spam beda oznaczane (w temacie) wskazana fraza lub znakiem; zadany tekst mozna wpisac w polu znajdujacym sie ponizej.

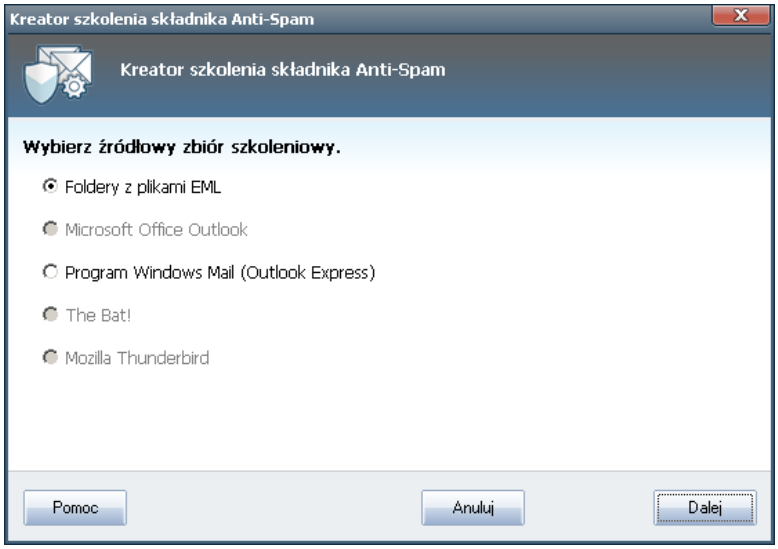
- ***Pytaj przed wyslaniem raportu blednego wykrycia*** - (opcja dostepna, jesli podczas procesu instalacji wyrazono zgode na udzial w programie udoskonalania produktów) zaznaczenie tej opcji umozliwia nam zbieranie od uczestników programu na calym swiecie aktualnych informacji dotyczacych najnowszych zagrozen; dzieki temu mozemy udoskonalac ochrone wszystkich uzytkowników. Wybór tej opcji oznacza zgode na raportowanie wykrytych zagrozen firmie AVG. Raportowanie jest obslugiwane automatycznie. Mozna jednak zaznaczyc to pole wyboru, aby przed wyslaniem raportu o wykrytym spamie do firmy AVG wyswietlac pytanie, czy dana wiadomosc faktycznie jest niepozadana.

  Uwaga: *Ta opcja nie jest dostepna w programie AVG Email Server Edition 2011.*

Przycisk ***Rozpocznij szkolenie skladnika Anti-Spam*** pozwala uruchomic ***Kreator szkolenia skladnika Anti-Spam*** opisany szczegółowo w nastepnym rozdziale.

7.3.1. Kreator szkolenia skladnika Anti-Spam

W pierwszym oknie dialogowym***kreatora szkolenia skladnika Anti-Spam*** nalezy wybrac zródlo wiadomosci e-mail, które zostana uzyte do szkolenia. Na ogól uzywa sie do tego celu niechcianych wiadomosci reklamowych, oraz e-maili blednie oznaczonych jako spam.



Dostepne sa nastepujace opcje:

- ***Konkretny klient poczty e-mail***- jesli uzywasz jednego z wymienionych klientów poczty e-mail (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), po prostu wskaz go na wyswietlonej liscie.

- ***Folder z plikami EML*** - jesli jest uzywany jakikolwiek inny program pocztowy, nalezy zgromadzic wszystkie wiadomosci w jednym folderze (w *formacie .eml*). Mozesz skorzystac z tego, ze wiele klientów poczty domyslnie przechowuje pliki .eml w okreslonym folderze na dysku. Nastepnie nalezy zaznaczyc opcje ***Folder z plikami EML***, oraz wskazac odpowiedni folder w nastepnym kroku.

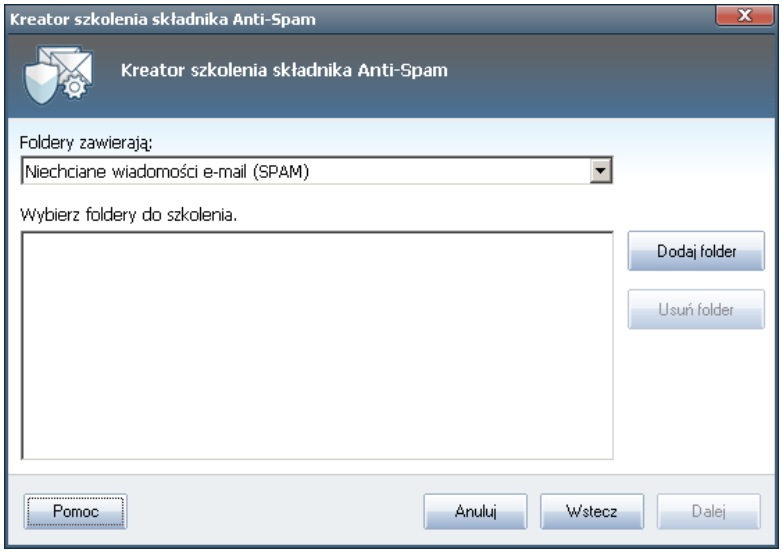
Aby proces szkolenia byl prostszy i przebiegal szybciej, warto juz wczesniej tak posortowac e-maile, aby folder uzywany w szkoleniu zawieral jedynie wiadomosci szkoleniowe (albo spam, albo ham). Nie jest to jednak konieczne, gdyz wiadomosci mozna przefiltrowac recznie w późniejszym czasie.

Aby kontynuowac, zaznacz odpowiednia opcje i kliknij przycisk ***Dalej*** .

7.3.2. Wybierz folder z wiadomosciami

Okno wyswietlane w tym kroku zalezy od poprzedniego wyboru.

Foldery z plikami EML



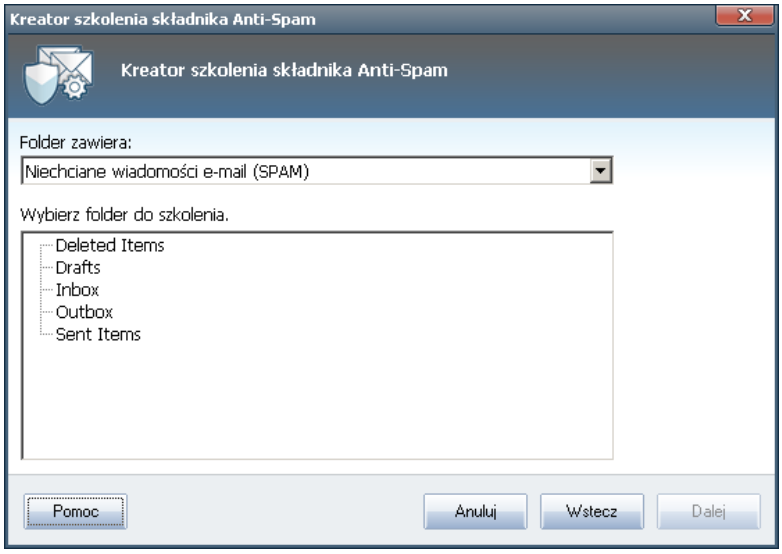
W oknie tym nalezy wybrac folder z wiadomosciami, które maja zostac uzyte do szkolenia. Kliknij przycisk ***Dodaj folder***, aby zlokalizowac folder z plikami .eml (*zapisanymi wiadomosciami e-mail*). Wybrany folder zostanie wyswietlony w biezacym oknie.

Z menu rozwijanego ***Foldery zawieraja*** wybierz jedna z dwóch opcji - czy folder zawiera pozadane wiadomosci (*HAM*), czy niechciane reklamy (*SPAM*). Nalezy pamietac, ze w nastepnym kroku bedzie mozliwa szczególowa selekcja plików, wiec folder nie musi zawierac tylko szkoleniowych wiadomosci e-mail. Mozna tez usunac z listy niechciane foldery, klikajac przycisk ***Usun folder***.

Po zakonczeniu ustawien nalezy kliknac przycisk ***Dalej*** i przejsc do ***Opcji filtrowania wiadomosci***.

Okreslony klient poczty e-mail

Po potwierdzeniu jednej z opcji pojawi sie nowe okno dialogowe.

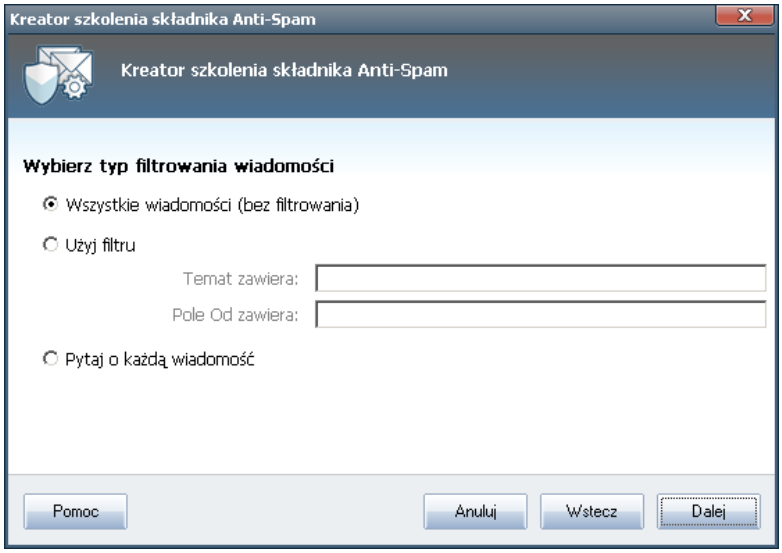


Uwaga: *W przypadku programu Microsoft Office Outlook pojawi sie najpierw monit o wybranie profilu programu MS Office Outlook.*

Z menu rozwijanego ***Foldery zawieraja*** wybierz jedna z dwóch opcji - czy folder zawiera pozadane wiadomosci (*HAM*), czy niechciane reklamy (*SPAM*). Nalezy pamietac, ze w nastepnym kroku bedzie mozliwa szczegółowa selekcja plików, wiec folder nie musi zawierac tylko szkoleniowych wiadomosci e-mail. W głównej czesci okna pojawi sie drzewo nawigacyjne wybranego klienta poczty e-mail. Zlokalizuj zadany folder i podswietl go za pomoca myszy.

Po zakonczeniu ustawien nalezy kliknac przycisk ***Dalej*** i przejsc do ***Opcji filtrowania wiadomosci***.

7.3.3. Opcje filtrowania wiadomosci



W tym oknie mozna ustawic filtrowanie wiadomosci e-mail.

Jesli wybrany folder na pewno zawiera tylko wiadomosci, które maja zostac uzyte do szkolenia, nalezy wybrac opcje ***Wszystkie wiadomosci (bez filtrowania)***.

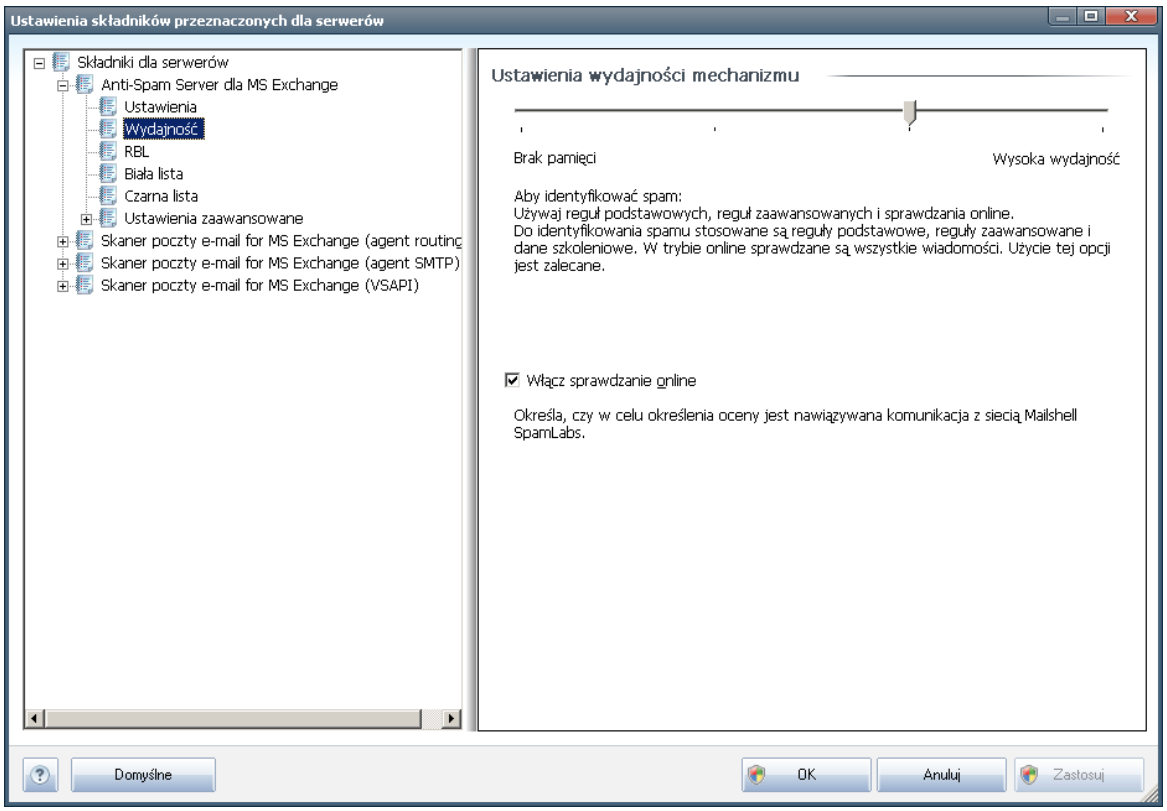
Jesli nie ma pewnosci co do wiadomosci znajdujacych sie w folderze, a Kreator ma pytac o kazda z nich oddzielnie (dajac mozliwosc okreslenia, czy ma ona zostac uzyta do szkolenia), nalezy wybrac opcje ***Pytaj o kazda wiadomosc***.

Aby zastosowac bardziej zaawansowane filtrowanie, nalezy wybrac opcje ***Uzyj filtru***. Mozna wpisac wyraz (nazwe), czesc wyrazu lub fraze, która ma byc wyszukiwana w tematach i/lub nazwach nadawców wiadomosci. Wszystkie wiadomosci dokladnie spelniajace kryteria wyszukiwania zostana uzyte do szkolenia, bez dalszych monitów.

Uwaga: *W przypadku wypelnienia obu pól tekstowych zostana uzyte takze adresy spelniajace tylko jeden z dwóch warunków!*

Gdy juz zdecydujesz sie na jedna z opcji, kliknij przycisk ***Dalej***. Kolejne okno dialogowe ma charakter informacyjny i sygnalizuje, ze kreator jest gotowy do przetwarzania wiadomosci. Aby rozpoczac szkolenie, nalezy ponownie kliknac przycisk ***Dalej*** Szkolenie rozpocznie sie zgodnie z wybranymi wczesniej parametrami.

7.4. Wydajnosc



Okno ***Ustawienia wydajnosci mechanizmu*** (*otwierane po kliknieciu pozycji*

Wydajnosc *w lewym panelu nawigacyjnym*) daje dostep do ustawien wydajnosci skladnika ***Anti-Spam***. Przesuwajac suwak w lewo lub w prawo, mozna zmienic wydajnosc skanowania na skali miedzy trybami ***Brak pamieci*** i ***Wysoka wydajnosc***.

- ***Brak pamieci*** - w czasie skanowania w poszukiwaniu spamu nie beda stosowane zadne reguly. Do identyfikacji beda uzywane tylko dane szkoleniowe. Ten tryb nie jest zalecany do czestego stosowania, chyba ze konfiguracja sprzetowa komputera jest bardzo slaba.

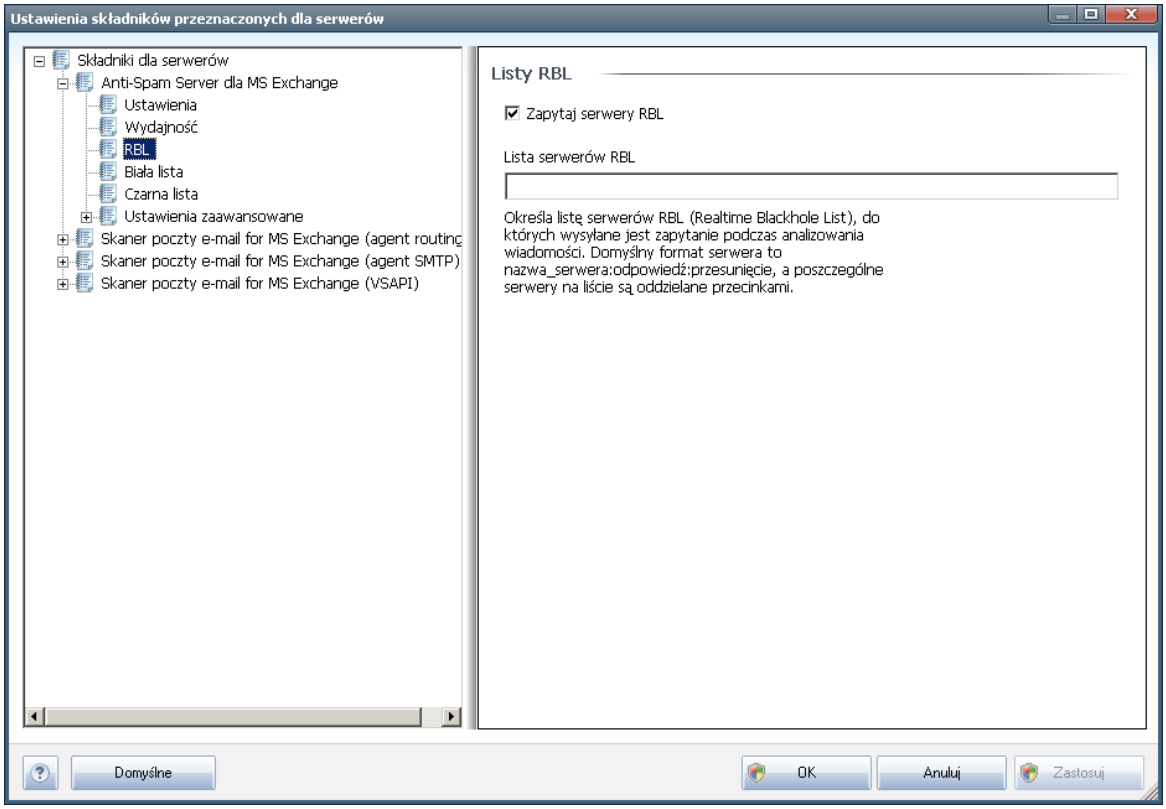
- ***Wysoka wydajnosc*** - wymaga duzej ilosci pamieci. W czasie skanowania w poszukiwaniu spamu stosowane beda nastepujace funkcje: pamiec podreczna dla regul i definicji spamu, reguly podstawowe i zaawansowane, adresy IP spamerów i inne bazy danych.

Opcja ***Wlacz sprawdzanie online*** jest domyslnie wlaczona. Pozwala ona skuteczniej wykrywac spamdzieki komunikacji z serwerami Mailshell: skanowane dane sa porównywane z bazami danych online firmy Mailshell.

Zwykle zaleca sie zachowanie ustawien domyslnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny byc wprowadzane wylacznie przez zaawansowanych uzytkowników, którzy doskonale wiedza, co robia!

7.5. RBL

Kliknięcie pozycji ***RBL*** otwiera okno o nazwie ***Listy RBL***:



W oknie tym mozna wlaczyc/wylaczyc funkcje ***Zapytaj serwery RBL***.

Serwer RBL (*Realtime Blackhole List*) to specjalny serwer DNS z obszerna baza danych znanych nadawców spamu. Jezeli funkcja ta jest wlaczona, wszystkie wiadomosci e-mail zostana sprawdzone przy uzyciu bazy serwera RBL i oznaczone jako spam, w przypadku gdy okaza sie identyczne z którymkolwiek wzorem w bazie danych.

Bazy danych serwerów RBL zawieraja zawsze aktualne sygnatury spamu, co zapewnia najskuteczniejsze i najdokladniejsze wykrywanie niechcianych wiadomosci. Funkcja ta jest szczególnie przydatna dla uzytkowników otrzymujacych duze ilosci spamu, który zazwyczaj nie jest wykrywany przez silnik AVG Anti-Spam.

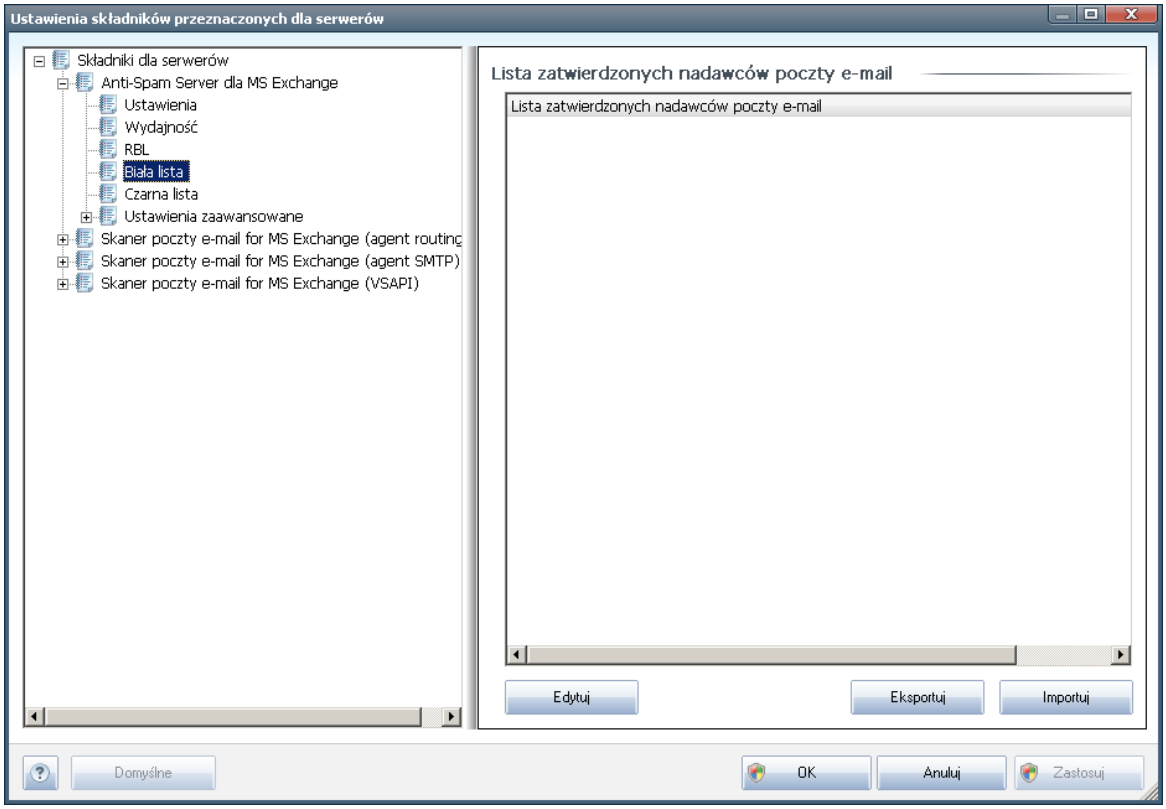
Lista serwerów RBL pozwala okreslic lokalizacje wybranych serwerów RBL. Domyslnie zdefiniowane sa tam dwa serwery RBL. Zmiany ustawien domyslnych powinny byc dokonywane tylko przez doswiadczonych uzytkowników i wylacznie w przypadkach, gdy jest to absolutnie niezbedne!

Uwaga: *Wlaczenie tej funkcji moze w niektórych systemach i konfiguracjach spowolnic proces odbierania poczty e-mail, poniewaz kazda wiadomosc musi byc zweryfikowana przy uzyciu bazy danych serwera RBL.*

Do serwera nie sa wysylane zadne dane osobiste!

7.6. Biala lista

Kliknięcie pozycji ***Biala lista*** pozwala otworzyc globalna liste zablokowanych adresów indywidualnych nadawców i domen, z których wiadomosci nigdy nie sa oznaczane jako spam.



W interfejsie tym mozna utworzyc liste nadawców, którzy nigdy nie wysylaja niepozadanych wiadomosci (spamu). Mozna takze utworzyc liste nazw calych domen (np. *avg.com*), które nie wysylaja spamu.

Po przygotowaniu listy adresów i domen, jej elementy mozna wprowadzic pojedynczo lub zaimportowac wszystkie na raz. Dostepne sa nastepujace przyciski kontrolne:

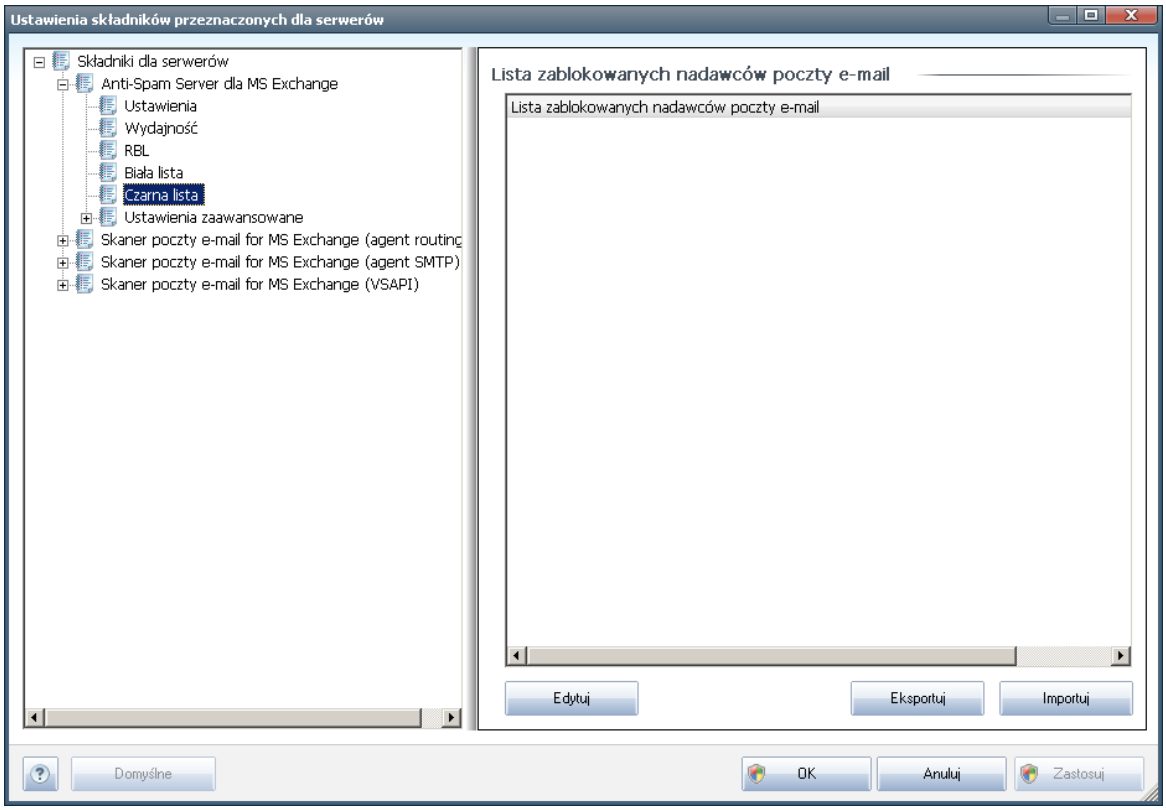
- ***Edytuj*** - *przycisk ten sluzy do otwarcia okna dialogowego, w którym mozna recznie wprowadzic liste adresów (równiez za pomoca metody kopiuj-wklej*). Kazda pozycje (nadawce lub nazwe domeny) nalezy wprowadzic w osobnym wierszu.

- ***Importuj*** - istniejaca liste adresów e-mail mozna zaimportowac po kliknieciu tego przycisku. Importowany plik musi byc zwyklym plikiem tekstowym i w kazdym wierszu zawierac wylacznie adres i nazwe domeny lub plikiem WAB. Ewentualnie mozna przeprowadzic import danych z ksiazki adresowej systemu Windows lub programu Microsoft Office Outlook.

- ***Eksportuj*** - jezeli z jakiegos powodu chcesz wyeksportowac wpisy, mozna uzyc przycisku Eksportuj. Wszystkie wpisy zastana zapisane w zwyklym pliku tekstowym.

7.7. Czarna lista

Kliknięcie pozycji ***Czarna lista*** pozwala otworzyc globalna liste zablokowanych adresów indywidualnych nadawców i domen, z których wiadomosci zawsze sa oznaczane jako spam.



W interfejsie tym mozna utworzyc liste nadawców, którzy wysylaja lub prawdopodobnie beda wysylali niepozadane wiadomosci (spam). Mozna takze utworzyc liste nazw domen (np. *spammingcompany.com*), z których uzytkownik otrzymuje (lub spodziewa sie otrzymywac) spam. Wszystkie wiadomosci e-mail wyslane z tych adresów/domen beda identyfikowane jako spam.

Po przygotowaniu listy adresów i domen, jej elementy mozna wprowadzic pojedynczo lub zaimportowac wszystkie na raz. Dostepne sa nastepujace przyciski kontrolne:

- ***Edytuj*** - *przycisk ten sluzy do otwarcia okna dialogowego, w którym mozna recznie wprowadzic liste adresów (równiez za pomoca metody kopiuj-wklej)*. Kazda pozycje (nadawce lub nazwe domeny) nalezy wprowadzic w osobnym wierszu.

- ***Importuj*** - istniejaca liste adresów e-mail mozna zaimportowac po kliknieciu

tego przycisku. Importowany plik musi byc zwyklym plikiem tekstowym i w kazdym wierszu zawierac wylacznie adres i nazwe domeny lub plikiem WAB. Ewentualnie mozna przeprowadzic import danych z ksiazki adresowej systemu Windows lub programu Microsoft Office Outlook.

- ***Eksportuj*** - jezeli z jakiegos powodu chcesz wyeksportowac wpisy, mozna uzyc przycisku Eksportuj. Wszystkie wpisy zastana zapisane w zwyklym pliku tekstowym.

7.8. Ustawienia zaawansowane

Zwykle zaleca sie zachowanie ustawien domyslnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny byc wprowadzane wylacznie przez zaawansowanych uzytkowników!

Aby mimo wszystko zmienic konfiguracje skladnika Anti-Spam na bardzo zaawansowanym poziomie, nalezy postepowac zgodnie z instrukcjami wyswietlanymi w interfejsie uzytkownika. Poszczególne okna dialogowe najczesciej odpowiadaja tylko jednej funkcji, której opis jest zawsze dostepny w tym samym miejscu:

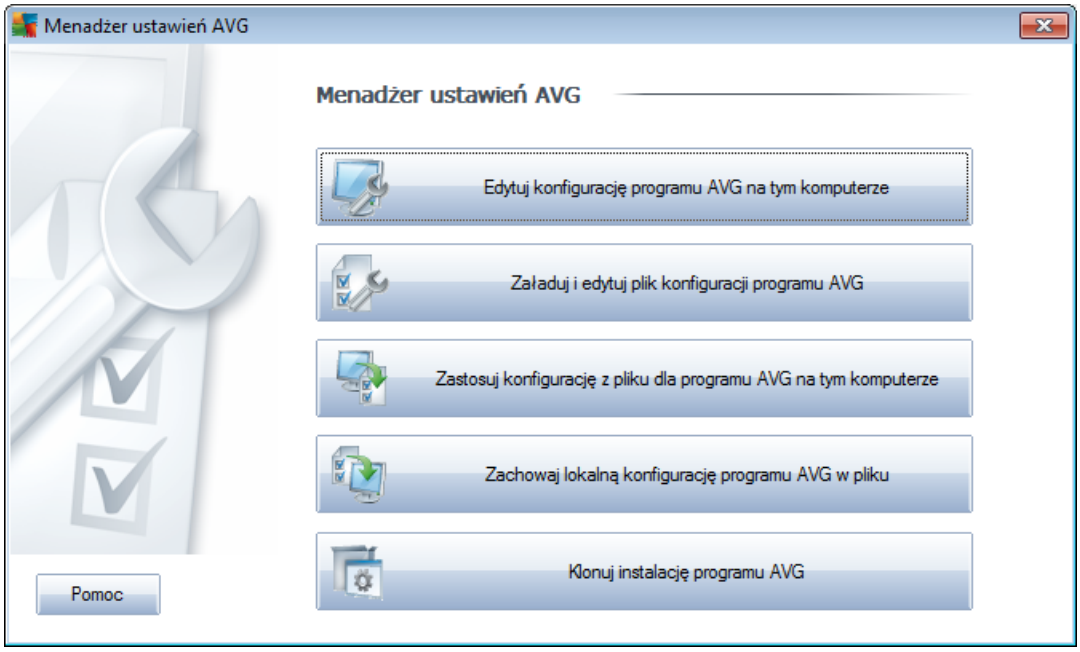
- ***Pamiec podreczna*** - sygnatury, reputacja domen, LegitRepute
- ***Szkolenie*** - maksymalna liczba wpisów slów, próg automatycznego szkolenia, waga
- ***Filtry*** - lista jezyków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, falszywi nadawcy
- ***RBL*** - serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba adresów IP
- ***Polaczenie internetowe*** - limit czasu, serwer proxy, uwierzytelnianie na serwerze proxy

8. Menedzer ustawien systemu AVG

Menedzer ustawien systemu AVG to narzedzie odpowiednie przede wszystkim dla mniejszych sieci, pozwalajace na kopiowanie, edycje i dystrybucje konfiguracji systemu AVG. Konfiguracja moze zostac zapisana na urzadzeniu przenosnym (dysk USB itp.), a nastepnie recznie zastosowana na wybranej stacji roboczej.

Narzedzie to jest elementem instalacji systemu AVG i mozna uzyskac do niego dostep z menu Start:

Wszystkie programy/AVG 2011/Menedzer ustawien systemu AVG



- ***Edytuj konfiguracje systemu AVG zainstalowanego na tym komputerze***

  Ten przycisk pozwala na otwarcie okna dialogowego z zaawansowanymi ustawieniami lokalnej instalacji systemu AVG. Wszystkie zmiany dokonane w tym miejscu zostana uwzglednione w lokalnej instalacji systemu AVG.

- ***Zaladuj i edytuj plik konfiguracyjny systemu AVG***

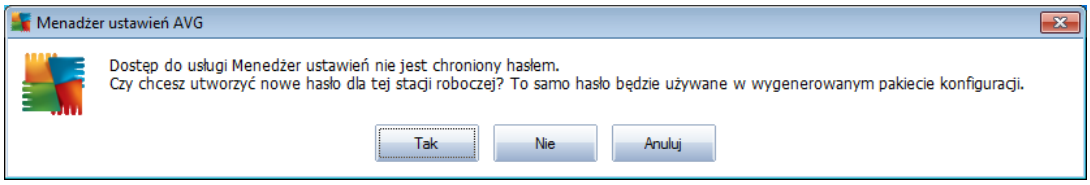
  Jesli plik konfiguracyjny systemu AVG (.pck) juz istnieje, mozna go otworzyc do edycji za pomoca tego przycisku. Po zatwierdzeniu zmian przyciskiem ***OK*** lub ***Zastosuj*** plik zostanie zastapiony nowymi ustawieniami!

- ***Zastosuj plik konfiguracyjny dla systemu AVG zainstalowanego na tym komputerze***

  Ten przycisk otwiera plik konfiguracyjny systemu AVG (.pck) i powoduje jego zastosowanie dla lokalnej instalacji systemu AVG.

- ***Zapisz konfiguracje lokalnej instalacji systemu AVG w pliku***

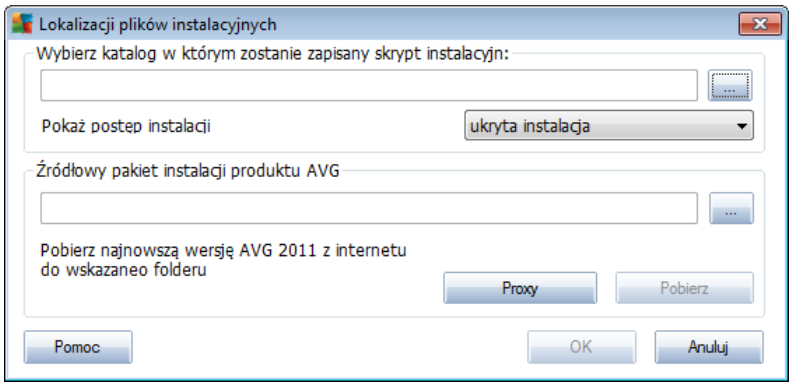
  Ten przycisk pozwala zapisac plik konfiguracyjny (.pck) lokalnej instalacji systemu AVG. Jesli dla dozwolonych akcji nie zostalo ustawione haslo, moze zostac wyswietlone nastepujace okno dialogowe:



  Kliknij odpowiedz ***Tak***, jesli dostep do dozwolonych pozycji ma byc chroniony haslem, a nastepnie wprowadz wymagane informacje i zatwierdz swój wybór. Kliknij ***Nie***, aby pominac tworzenie hasla i kontynuowac zapisywanie konfiguracji lokalnej instalacji systemu AVG.

- ***Klonuj instalacje systemu AVG***

  Ta opcja pozwala wykonac dokladna kopie lokalnej instalacji systemu AVG dzieki utworzeniu pakietu instalacyjnego o niestandardowych parametrach. Aby kontynuowac, nalezy wybrac folder, w którym ma zostac zapisany skrypt.



  Nastepnie z menu rozwijanego nalezy wybrac jedna z nastepujacych opcji:

  - ***Instalacja ukryta*** - podczas procesu instalacji nie beda wyswietlane zadne informacje.
  - ***Wyswietlaj tylko postep instalacji*** - instalacja nie bedzie wymagala zadnej interakcji ze strony uzytkownika, ale jej postep bedzie w pelni widoczny.
  - ***Pokaz Kreatora instalacji*** - instalacja bedzie widoczna, a uzytkownik bedzie musial recznie potwierdzac wszystkie kroki.

  Aby pobrac najnowszy pakiet instalacyjny systemu AVG bezposrednio ze strony AVG do wybranego folderu, nalezy kliknac przycisk ***Pobierz***. Mozliwe jest tez reczne umieszczenie pakietu instalacyjnego systemu AVG w tym folderze.

Za pomoca przycisku ***Proxy*** mozna zdefiniowac ustawienia serwera proxy, jesli siec wymaga tego do pomyslnego nawiazania polaczenia.

Po kliknieciu przycisku ***OK*** rozpoczety zostanie krótkotrwaly proces klonowania. Moze sie zdarzyc, ze zostanie wyswietlone okno dialogowe z prosba o ustawienie hasla dla dozwolonych pozycji (patrz wyzej). Po zakonczeniu procesu, w wybranym folderze powinien zostac utworzony plik ***AvgSetup.bat***. Po uruchomieniu pliku ***AvgSetup.bat***, system AVG zostanie zainstalowany zgodnie z parametrami wybranymi powyzej.

9. FAQ i pomoc techniczna

W przypadku jakichkolwiek problemów z oprogramowaniem AVG (w kwestiach handlowych lub technicznych) nalezy skorzystac z sekcji ***FAQ*** w witrynie firmy AVG pod adresem http://www.avg.com.

Jesli pomoc ta okaze sie niewystarczajaca, zalecamy kontakt z dzialem pomocy technicznej za posrednictwem poczty e-mail. Zachecamy do skorzystania z formularza kontaktowego, dostepnego po wybraniu polecenia menu systemowego ***Pomoc/ Uzyskaj pomoc online***.