AVG Email Server Edition

Podręcznik użytkownika

Wersja dokumentu 2015.11 (22.09.2015)

Spis treści

1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację systemu **AVG Email Server Edition**.

Gratulujemy zakupu systemu AVG Email Server Edition!

System **AVG Email Server Edition** należy do linii wielokrotnie nagradzanych produktów AVG, które zapewniają użytkownikom spokój ducha, a ich serwerom – pełne bezpieczeństwo. Podobnie jak pozostałe produkty, system **AVG Email Server Edition** zaprojektowano od podstaw pod kątem zapewnienia słynnego już poziomu ochrony w nowy, bardziej przyjazny dla użytkownika sposób.

System AVG zaprojektowano i zbudowano tak, by chronił użytkownika podczas pracy na komputerze i w sieci. Ciesz się pełną ochroną AVG.

Uwaga: *Ta dokumentacja zawiera opisy konkretnych funkcji AVG Email Server Edition. Aby uzyskać więcej informacji na temat innych funkcji systemu AVG, zajrzyj do podręcznika użytkownika AVG Internet Security, który zawiera wszystkie niezbędne szczegóły. Podręcznik ten może zostać pobrany ze strony http://www.avg.com.*

2. Wymagania instalacyjne AVG

2.1. Obsługiwane systemy operacyjne

AVG Email Server Edition służy do ochrony serwerów pocztowych działających pod następującymi systemami operacyjnymi:

- Windows 2012 Server R2 Edition
- Windows 2012 Server Edition (x86 i x64)
- Windows 2008 Server R2 Edition
- Windows 2008 Server Edition (x86 i x64)
- Windows 2003 Server (x86, x64) z dodatkiem SP1

2.2. Obsługiwane serwery poczty e-mail

Obsługiwane są następujące serwery pocztowe:

- MS Exchange 2003 Server
- MS Exchange 2007 Server
- MS Exchange 2010 Server
- MS Exchange 2013 Server
- Kerio MailServer – wersja 6.7.2 i wyższe

2.3. Minimalne wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG Email Server Edition**:

- Procesor Intel Pentium 1,5 GHz,
- 500 MB wolnego miejsca na dysku twardym (w celu instalacji),
- 512 MB pamięci RAM.

Zalecane wymagania sprzętowe dla systemu **AVG Email Server Edition**:

- Procesor Intel Pentium 1,8 GHz,
- 600 MB wolnego miejsca na dysku twardym (w celu instalacji),
- 512 MB pamięci RAM.

2.4. Deinstalacja poprzednich wersji

W przypadku korzystania ze starej wersji aplikacji AVG Email Server przed zainstalowaniem produktu **AVG Email Server Edition** konieczne będzie jej ręczne odinstalowanie. Deinstalacja poprzedniej wersji musi zostać wykonana ręcznie przy użyciu standardowych funkcji systemu Windows.

- Przejdź do menu ***Start/Ustawienia/Panel sterowania/Dodaj lub usuń programy*** i wybierz odpowiedni program z listy zainstalowanego oprogramowania (możesz to zrobić jeszcze prościej z poziomu menu ***Start/Wszystkie programy/AVG/Odinstaluj AVG***).

- Jeśli poprzednio używano systemu AVG w wersji 8.x lub starszej, nie należy zapomnieć o osobnym odinstalowaniu pluginów serwera.

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

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

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

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

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

2.5. Dodatki Service Pack dla MS Exchange

Dla serwera MS Exchange 2003 nie jest wymagany żaden dodatek Service Pack. Jednak w celu zapewnienia maksymalnego bezpieczeństwa zaleca się zaktualizowanie systemu oraz instalację najnowszych dodatków Service Pack i poprawek.

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

http://www.microsoft.com/en-us/download/details.aspx?id=9664

Na początku procesu instalacji zostaną sprawdzone wersje wszystkich bibliotek systemowych. Jeśli zajdzie potrzeba instalacji nowszych bibliotek, instalator zmieni rozszerzenie starszych plików na .delete. Biblioteki zostaną usunięte 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

Dodatek Service Pack dla serwera MS Exchange 2010 Server (opcjonalnie):

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

3. Proces instalacji systemu AVG

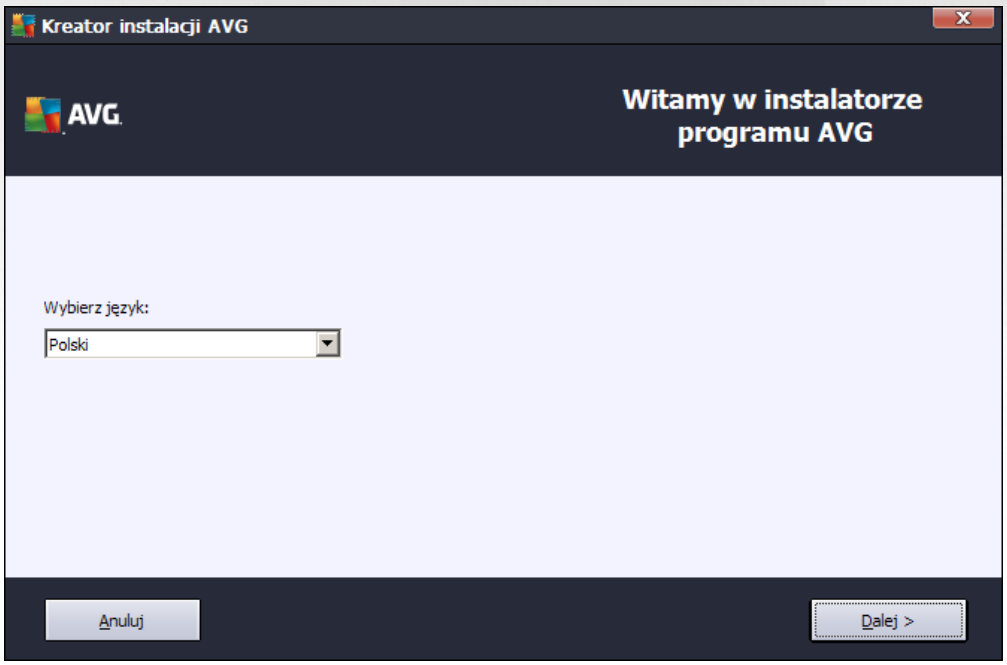
Aby zainstalować na komputerze program AVG, należy najpierw zdobyć najnowszy instalator. Można znaleźć go na dysku CD będącym częścią dystrybucyjnej edycji programu – istnieje jednak ryzyko, że będzie on nieaktualny. Dlatego zaleca się pobranie najnowszego pliku instalacyjnego z internetu. Plik można pobrać z witryny internetowej firmy AVG (pod adresem http://www.avg.com/download?prd=msw).

Dla tego produktu dostępne są dwa pakiety instalacyjne: dla 32-bitowych systemów operacyjnych (oznaczony jako x86) i dla systemów 64-bitowych (oznaczonych jako x64). Upewnij się, że używasz pakietu instalacyjnego odpowiedniego dla danego systemu operacyjnego.

Podczas procesu instalacji konieczne jest podanie numeru licencji. Należy więc przygotować go przed rozpoczęciem instalacji. Numer ten znajduje się na opakowaniu dysku CD. Przy zakupie systemu AVG przez internet numer licencji jest dostarczany pocztą e-mail.

Po pobraniu i zapisaniu pliku instalatora na dysku można uruchomić proces instalacji. Instalacja to sekwencja okien dialogowych zawierających krótkie opisy poszczególnych etapów. Poniżej znajdują się objaśnienia każdego z nich:

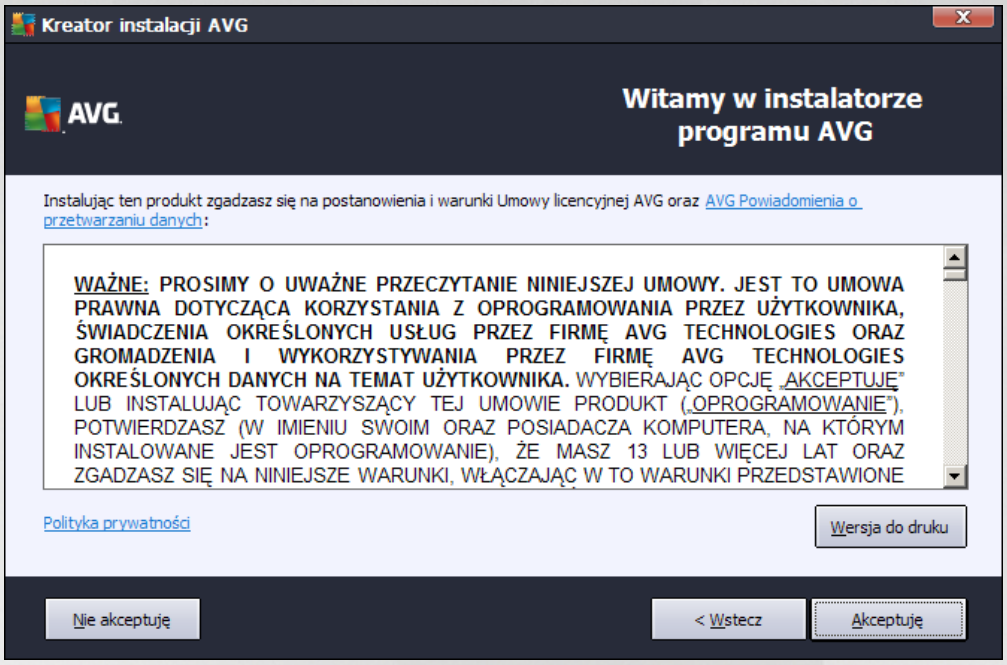
3.1. Uruchamianie instalacji



Proces instalacji rozpoczyna się od wyświetlenia ***okna powitalnego***. W tym miejscu należy wybrać język używany podczas procesu instalacji, a następnie kliknąć przycisk ***Dalej***.

Podczas procesu instalacji możliwe będzie również wybranie innych dodatkowych języków interfejsu aplikacji.

3.2. Umowa licencyjna

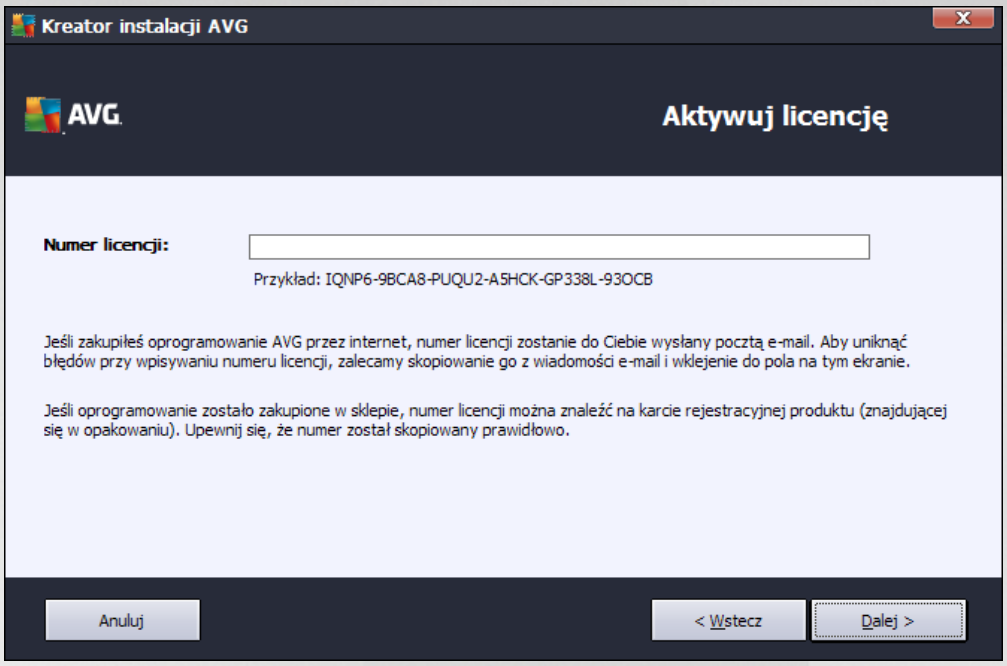


To okno pozwala Ci zapoznać się z warunkami licencji. Aby wyświetlić treść umowy licencyjnej w nowym oknie, kliknij przycisk ***Wersja do druku***. Kliknij przycisk ***Akceptuję***, aby potwierdzić wybór i przejść do kolejnego ekranu.

3.3. Aktywacja licencji

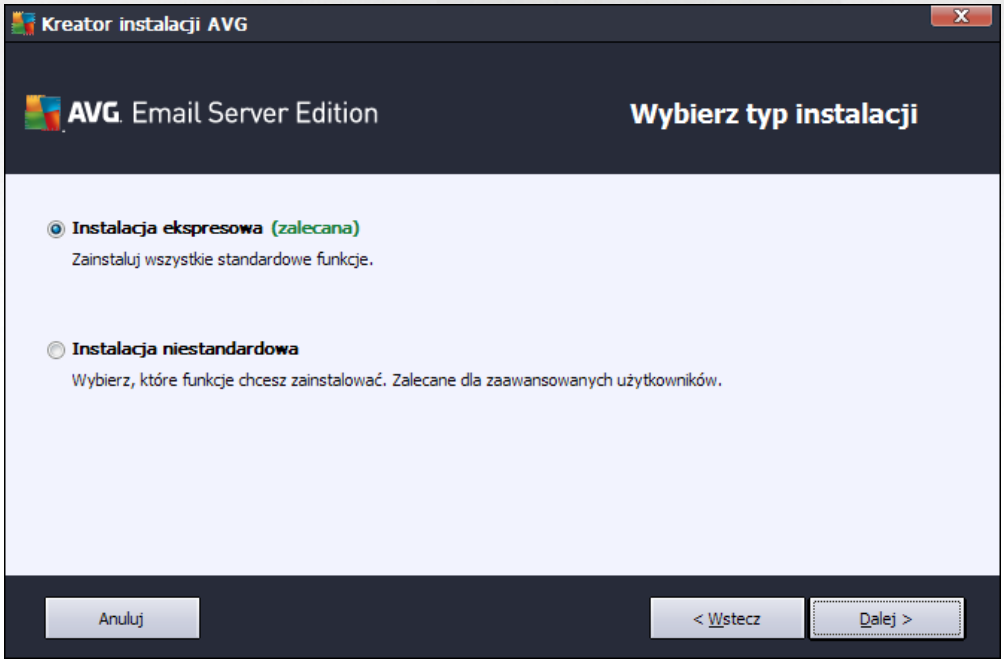
W oknie dialogowym ***Aktywacja licencji*** należy podać swój numer licencji.

Wprowadź numer licencji w polu tekstowym ***Numer licencji***. Numer licencji jest wysyłany pocztą e-mail po zakupieniu oprogramowania AVG online. Ważne jest dokładne wprowadzenie wspomnianego numeru. Jeśli numer jest dostępny w formie cyfrowej (w wiadomości e-mail), zaleca się skopiowanie i wklejenie go w odpowiednim polu.



Aby kontynuować instalację, kliknij przycisk ***Dalej***.

3.4. Wybór typu instalacji



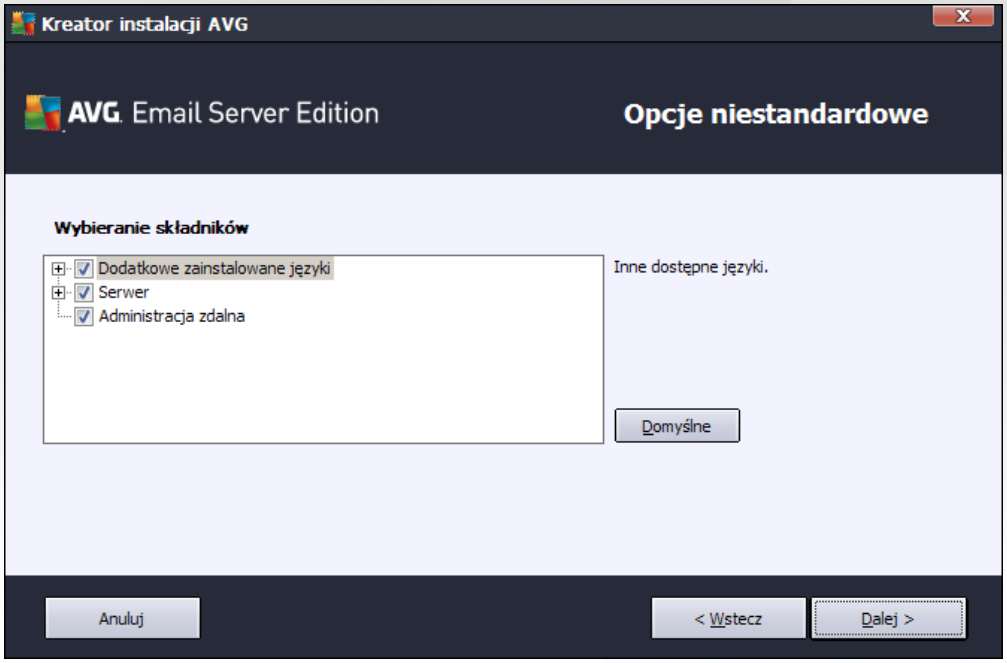
Okno dialogowe ***Wybierz typ instalacji*** umożliwia wybranie jednej z dwóch opcji: ***Instalacja ekspresowa*** lub ***Instalacja niestandardowa***.

Większość użytkowników zdecydowanie powinna wybrać opcję ***Instalacja ekspresowa***, która pozwala zainstalować system AVG w sposób całkowicie zautomatyzowany, z ustawieniami wstępnie zdefiniowanymi przez dostawcę oprogramowania. Taka konfiguracja zapewnia maksymalne bezpieczeństwo oraz optymalne wykorzystanie zasobów. Jeśli w przyszłości zajdzie potrzeba zmiany konfiguracji, można będzie to zrobić bezpośrednio z poziomu interfejsu AVG.

Opcję ***Instalacja niestandardowa*** powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować systemu AVG z ustawieniami domyślnymi (np. po to, aby dostosować go do specyficznych wymagań systemowych).

Po wybraniu Instalacji niestandardowej w dolnej części okna pojawi się pole ***Folder docelowy***. Pozwala ono określić lokalizację, w której ma zostać zainstalowany system AVG. Domyślnie pakiet AVG jest instalowany w folderze Program Files na dysku C:. Aby zmienić tę lokalizację, kliknij przycisk ***Przeglądaj*** i w wyświetlonym oknie wybierz odpowiedni folder.

3.5. Instalacja niestandardowa – opcje niestandardowe



Sekcja ***Wybór składników*** zawiera przegląd wszystkich składników systemu AVG, które można zainstalować. Jeśli ustawienia domyślne nie są dla Ciebie odpowiednie, możesz dodać lub usunąć żądane składniki.

Wybierać można jednak tylko składniki dostępne w zakupionej edycji systemu AVG. Tylko one będą widoczne w oknie dialogowym Wybór składników!

- ***Administracja zdalna*** – jeśli system AVG ma mieć możliwość łączenia się z bazą AVG DataCenter (wersje AVG Network Edition), konieczne jest wybranie tej opcji.

- ***Dodatkowe zainstalowane języki*** – ta opcja umożliwia określenie, jakie języki interfejsu AVG mają zostać zainstalowane. Należy w tym celu zaznaczyć opcję ***Dodatkowe zainstalowane języki*** i wybrać je z odpowiedniego menu.

Podstawowy przegląd poszczególnych składników dla serwerów (w gałęzi ***Serwer***):

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

  Sprawdza wszystkie przychodzące wiadomości e-mail i oznacza niepożądaną pocztę jako SPAM. Podczas przetwarzania każdej wiadomości wykorzystywanych jest kilka metod analizy oferujących najskuteczniejszą dostępną na rynku ochronę.

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

  Sprawdza wszystkie przychodzące, wychodzące i wewnętrzne wiadomości e-mail przechodzące przez serwer MS Exchange w roli HUB.

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

  Sprawdza wszystkie wiadomości przechodzące przez interfejs SMTP serwera MS Exchange (może być zainstalowany zarówno dla roli EDGE jak i HUB).

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

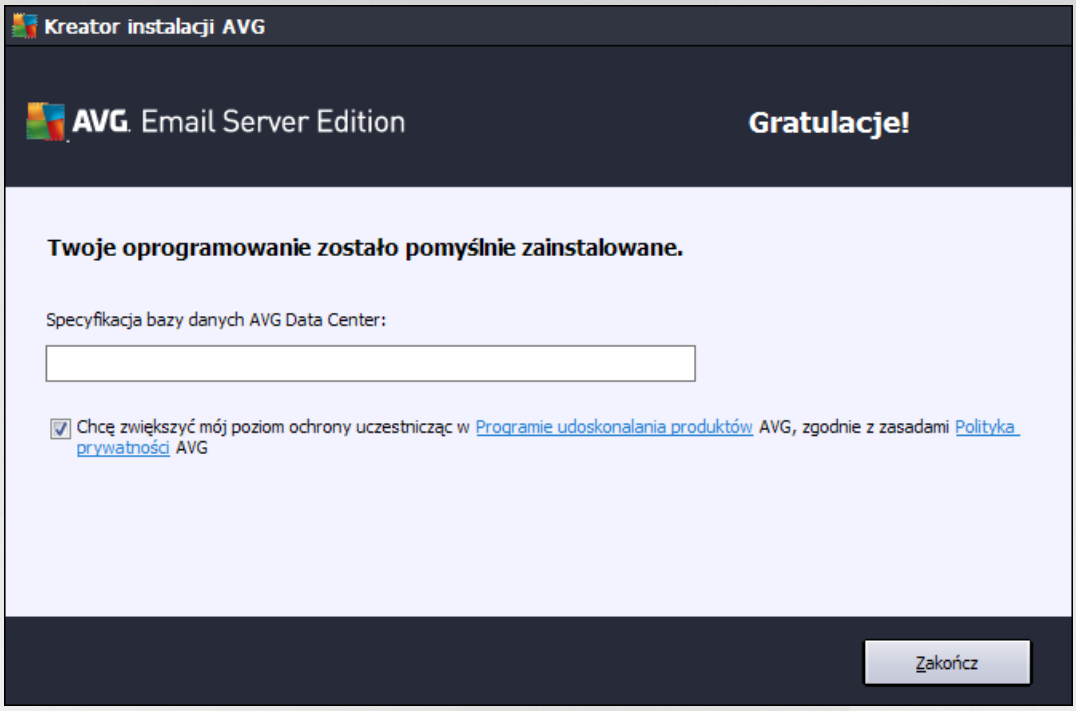
  Sprawdza wszystkie wiadomości e-mail przechowywane w skrzynkach pocztowych użytkownika. Wszystkie wykryte wirusy są przenoszone do Przechowalni wirusów lub usuwane.

Użytkownicy Exchange 2003 będą mogli skorzystać jedynie ze składników Anti-Spam i Email Scanner (VSAPI).

Aby kontynuować, kliknij przycisk ***Dalej***.

3.6. Ukończenie instalacji

Jeśli przy wyborze składników została wybrana ***Administracja zdalna***, na ostatnim ekranie możliwe będzie określenie parametrów połączenia z bazą AVG DataCenter.



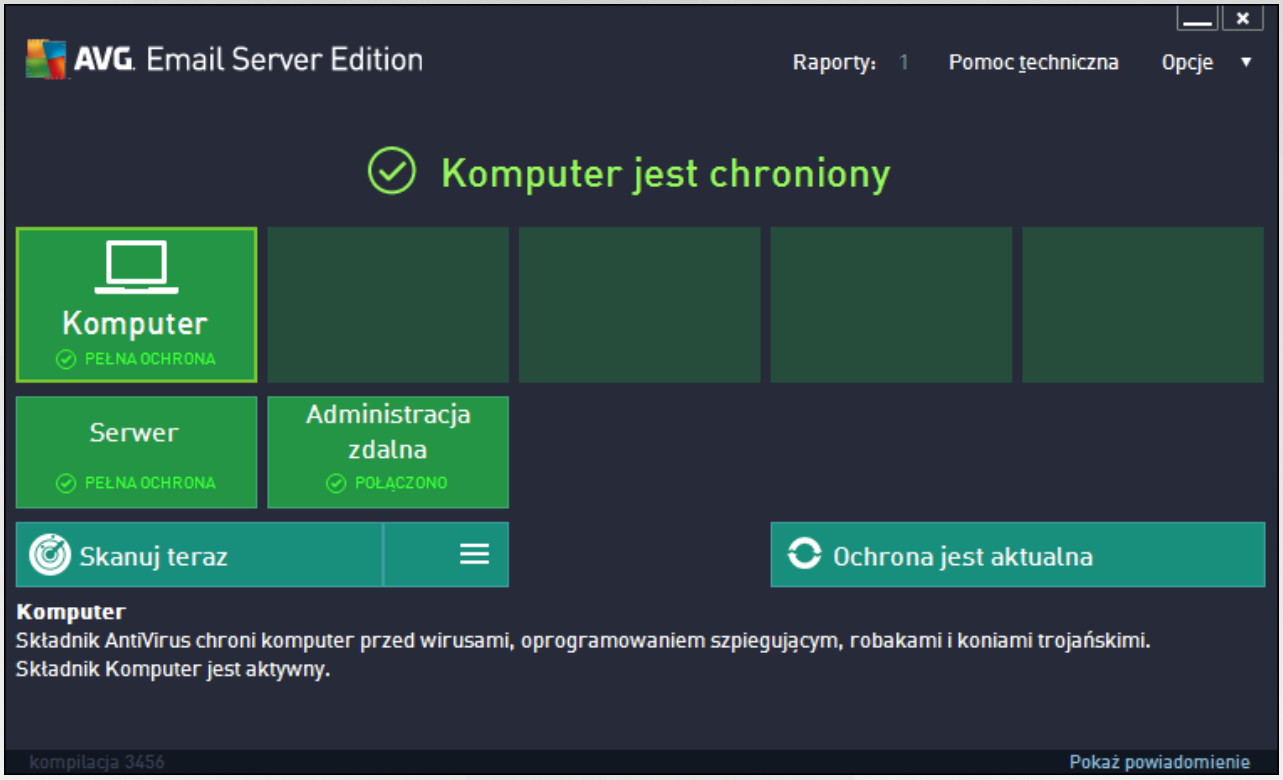
To samo okno pozwala Ci również zdecydować, czy chcesz brać udział w Programie udoskonalania produktów, który gromadzi anonimowe informacje o wykrytych zagrożeniach, aby podnieść ogólny poziom bezpieczeństwa w internecie. Jeśli się na to zgadzasz, pozostaw zaznaczone pole ***Chcę podnieść poziom mojej ochrony, uczestnicząc w Programie udoskonalania produktów AVG zgodnie z zasadami Polityki prywatności AVG*** *(opcja ta jest domyślnie zaznaczona)*.

Wybór należy zatwierdzić, klikając przycisk **Zakończ**.

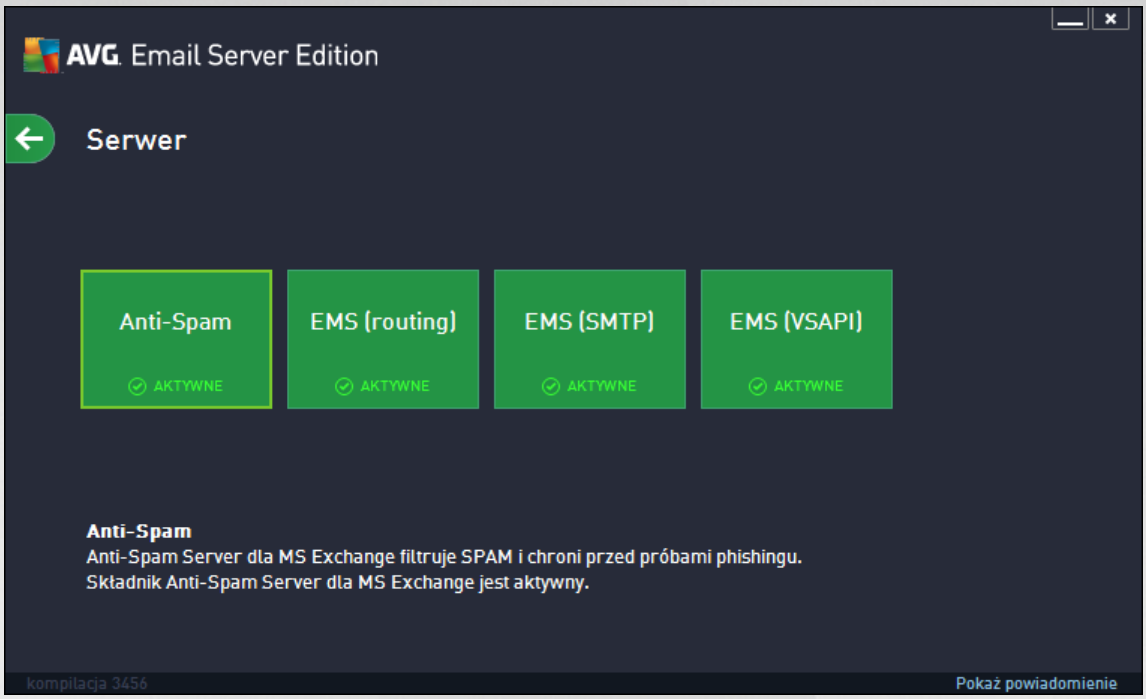
Program AVG jest zainstalowany na komputerze i w pełni funkcjonalny. System ten działa w tle, całkowicie automatycznie.

4. Po instalacji

Zaraz po zakończeniu instalacji pojawi się główny ekran ***AVG Email Server Edition***:



Niniejszy podręcznik dotyczy jedynie konkretnych funkcji ***AVG Email Server Edition***; wszystkie inne składniki i ustawienia opisane są w podręczniku AVG Desktop. Aby dostać się do głównego okna zawierającego składniki dla serwerów, kliknij przycisk ***Serwer***. Zobaczysz wówczas następujący ekran:



Przypominamy, że wszystkie składniki dla serwerów (chyba, że zdecydujesz się nie instalować niektórych z nich podczas procesu instalacji) będą dostępne jedynie w przypadku MS Exchange w wersji 2007 lub nowszej. MS Exchange 2003 obsługuje jedynie składniki Anti-Spam i Email Scanner (VSAPI).

Aby skonfigurować opcje ochrony serwera poczty e-mail, należy przejść do odpowiedniego rozdziału:

- ***Skanery poczty dla MS Exchange***
- ***Anti-Spam Server dla MS Exchange***
- ***AVG dla Kerio MailServer***

5. Skanery poczty dla MS Exchange

5.1. Przegląd

Podstawowy przegląd poszczególnych składników serwerowych edycji AVG Email Scanner:

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

  Sprawdza wszystkie przychodzące, wychodzące i wewnętrzne wiadomości e-mail przechodzące przez serwer MS Exchange w roli HUB.

  Składnik dostępny dla MS Exchange 2007/2010/2013 może zostać zainstalowany tylko na serwerze w roli HUB.

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

  Sprawdza wszystkie wiadomości e-mail przechodzące przez interfejs MS Exchange SMTP.

  Składnik dostępny tylko dla serwera MS Exchange 2007/2010/2013 w roli EDGE lub HUB.

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

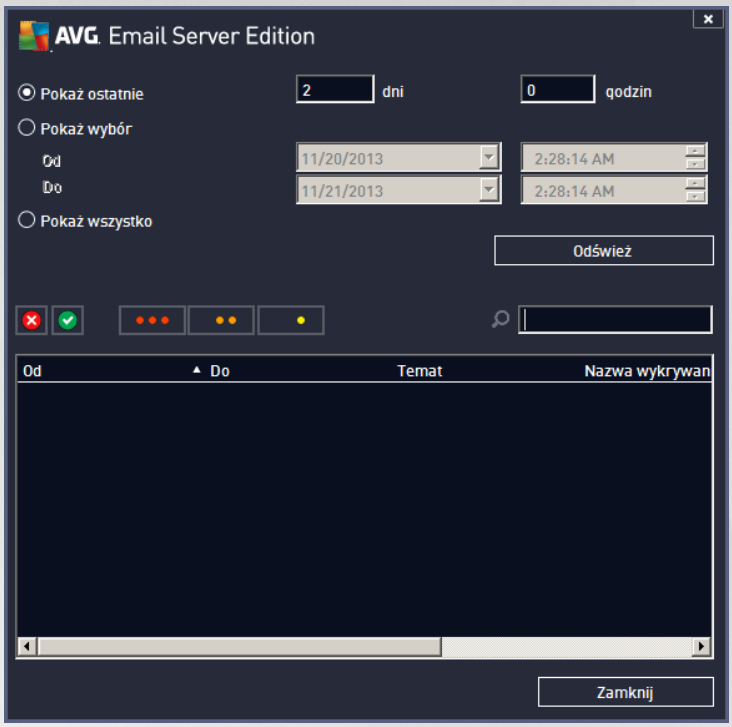
  Sprawdza wszystkie wiadomości e-mail przechowywane w skrzynkach pocztowych użytkownika. Wszystkie wykryte wirusy są przenoszone do Przechowalni wirusów lub usuwane.

Kliknij wybrany składnik, aby otworzyć jego interfejs. Wszystkie składniki posiadają następujące, wspólne przyciski i linki sterujące:

- ***WŁĄCZONY/WYŁĄCZONY*** – kliknięcie tego przycisku włącza/wyłącza wybrany składnik (jeśli jest on włączony, przycisk i tekst będą zielone, a jeśli wyłączony – czerwone).

- ***Wyniki skanowania***

  Otwiera nowe okno dialogowe, w którym dostępny jest przegląd wyników skanowania:



  W tym miejscu można sprawdzić wiadomości podzielone na kilka kart według poziomu zagrożenia. Poziomy zagrożenia i raportowania można dostosować w konfiguracji indywidualnych składników.

  Domyślnie wyświetlane są tylko wyniki z ostatnich dwóch dni. Okres, dla którego wyświetlane są wyniki, można dostosować za pomocą następujących opcji:

  o ***Pokaż ostatnie*** – wprowadź preferowaną liczbę dni i godzin.

  o ***Pokaż wybrane*** – wprowadź niestandardowy przedział czasu i daty.

  o ***Pokaż wszystko*** – wyświetla wszystkie dostępne wyniki.

  Przycisk ***Odśwież*** służy do ponownego załadowania wyników.

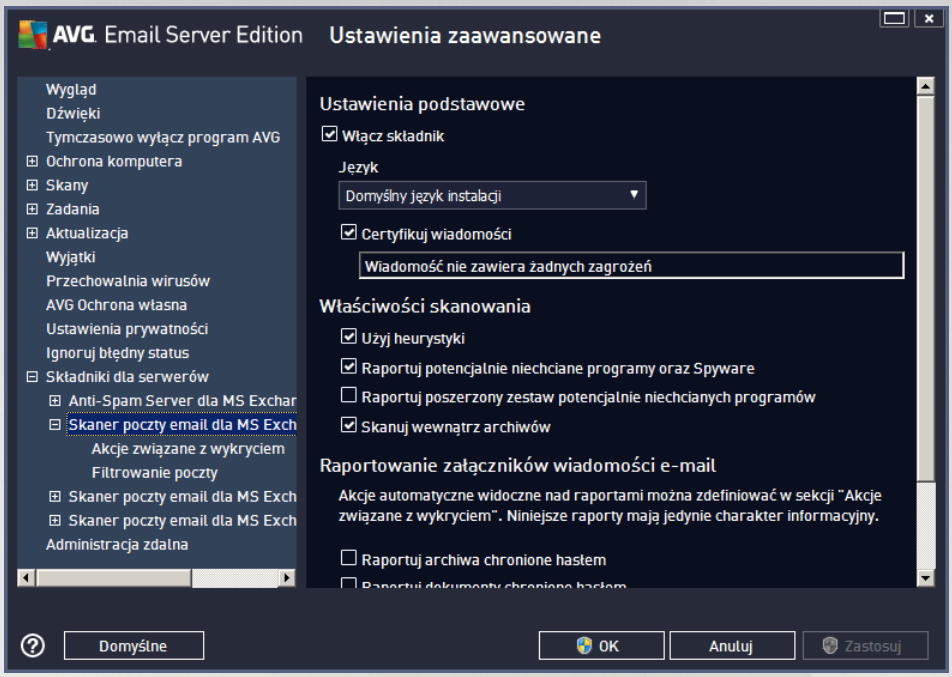
- ***Odśwież wartości statystyczne*** – aktualizuje powyższe statystyki.

Kliknięcie przycisku ***Ustawienia*** otworzy zaawansowane ustawienia wybranego składnika (więcej informacji na temat poszczególnych ustawień wszystkich składników znajdziesz w następnych rozdziałach).

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

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

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



Sekcja ***Ustawienia podstawowe*** zawiera następujące opcje:

- ***Włącz składnik*** – odznaczenie tej opcji spowoduje wyłączenie całego składnika.
- ***Język*** – wybierz preferowany język składnika.
- ***Certyfikuj wiadomości*** – zaznacz to pole, aby do wszystkich skanowanych wiadomości dołączać certyfikację. Jej treść można dostosować w kolejnym polu.

Sekcja ***Właściwości skanowania***:

- ***Użyj heurystyki*** – zaznacz to pole, aby włączyć analizę heurystyczną podczas skanowania.
- ***Raportowanie potencjalnie niechcianych programów i programów typu spyware*** – tę opcję należy zaznaczyć, aby raportowana była obecność potencjalnie niechcianych programów i programów typu spyware.
- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** – zaznaczenie tego pola umożliwi wykrycie większych ilości oprogramowania szpiegującego, tj. programów, które przy zakupie bezpośrednio od producenta są całkowicie nieszkodliwe, lecz później mogą zostać użyte niezgodnie z przeznaczeniem, w celu wyrządzenia szkody (np. różne paski narzędzi). To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera oraz podniesienie komfortu pracy. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona. Uwaga: Ta funkcja detekcji stanowi uzupełnienie poprzedniej opcji, dlatego w celu zapewnienia ochrony przed podstawowymi rodzajami oprogramowania szpiegującego poprzednie pole wyboru powinno być zawsze zaznaczone.
- ***Skanuj wewnątrz archiwów*** – opcję tę należy zaznaczyć, aby umożliwić skanerowi skanowanie również wewnątrz archiwów (zip, rar itp.).

W sekcji ***Raportowanie załączników wiadomości e-mail*** możliwe jest wybranie pozycji, które mają być

raportowane podczas skanowania. Jeśli to pole jest zaznaczone, każda wiadomość e-mail z taką pozycją będzie zawierać znacznik [INFORMATION]. Ta domyślna konfiguracja może zostać łatwo dostosowana w obszarze ***Informacje***, w sekcji ***Akcje związane z wykryciem*** (patrz niżej).

Dostępne są następujące opcje:

- ***Powiadamiaj o archiwach chronionych hasłem***
- ***Powiadamiaj o dokumentach chronionych hasłem***
- ***Powiadamiaj o plikach zawierających makra***
- ***Powiadamiaj o ukrytych rozszerzeniach***

W strukturze drzewa dostępne są następujące pozycje:

- ***Akcje związane z wykryciem***
- ***Filtrowanie poczty***

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

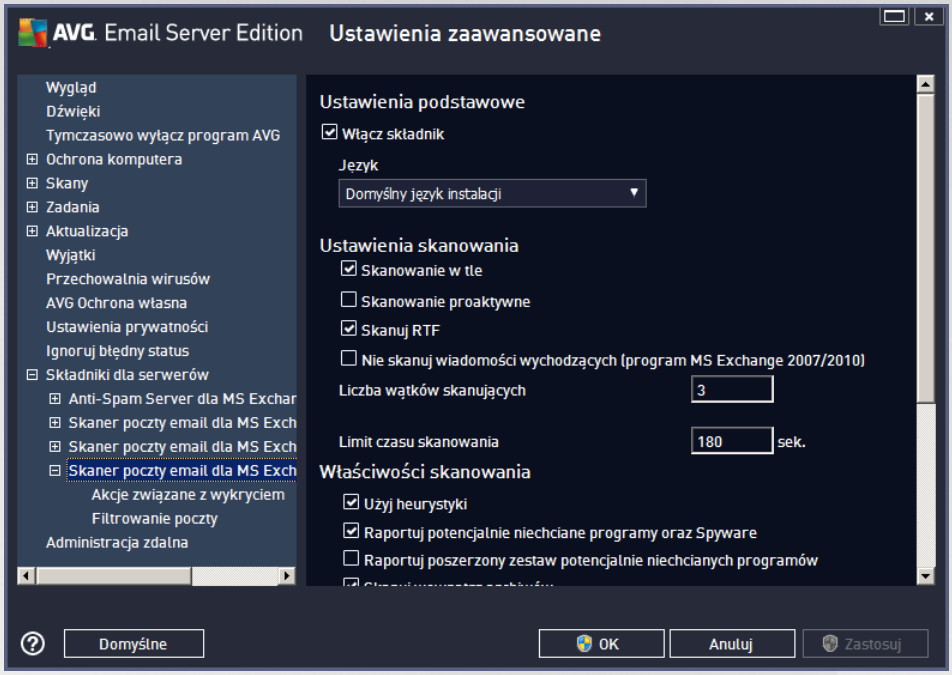
Konfiguracja ***Skanera poczty e-mail dla MS Exchange (agenta SMTP)*** jest dokładnie taka sama jak w przypadku agenta routingu. Więcej informacji na ten temat można znaleźć w rozdziale ***Skaner poczty e-mail dla MS Exchange (routing TA)*** powyżej.

W strukturze drzewa dostępne są następujące pozycje:

- ***Akcje związane z wykryciem***
- ***Filtrowanie poczty***

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

Ta pozycja zawiera ustawienia ***Skanera poczty e-mail dla MS Exchange (VSAPI)***.



Sekcja ***Ustawienia podstawowe*** zawiera następujące opcje:

- ***Włącz składnik*** – odznaczenie tej opcji spowoduje wyłączenie całego składnika.
- ***Język*** – wybierz preferowany język składnika.

Sekcja ***Ustawienia skanowania***:

- ***Skanowanie w tle*** – to pole wyboru umożliwia włączenie lub wyłączenie procesu skanowania w tle. Skanowanie w tle jest jedną z funkcji interfejsu aplikacji VSAPI 2.0/2.5. Zapewnia wielowątkowe skanowanie baz danych serwera Exchange. Zawsze gdy w folderach skrzynki pocztowej użytkownika pojawi się element, który nie był skanowany przy użyciu najnowszej wersji bazy danych, jest on przesyłany do programu AVG dla Exchange Server. Skanowanie i wyszukiwanie obiektów, które nie zostały jeszcze przeskanowane odbywa się równolegle.

  Dla każdej bazy danych stosowany jest określony wątek o niskim priorytecie, co gwarantuje, że inne zadania (np. magazynowanie wiadomości e-mail w bazie danych Microsoft Exchange) zawsze są realizowane jako pierwsze.

- ***Skanowanie proaktywne (wiadomości przychodzące)***

  W tym miejscu możliwe jest włączenie lub wyłączenie funkcji proaktywnego skanowania przy użyciu interfejsu VSAPI 2.0/2.5. Skanowanie to ma miejsce, gdy wiadomość została już zapisana w folderze, lecz klient nie zażądał jeszcze jej przeskanowania.

  Po przesłaniu do serwera Exchange, wiadomości zostają umieszczone w globalnej kolejce skanowania i otrzymują niski priorytet (maksymalnie 30 pozycji). Skanowanie opiera się w oparciu o schemat FIFO

(first in, first out). Jeśli użytkownik chce uzyskać dostęp do danej wiadomości podczas gdy jest ona umieszczona w kolejce, jej priorytet zostaje zmieniony na wysoki.

Wiadomości niemieszczące się w kolejce zostaną przekazane na serwer bez skanowania.

Nawet jeśli zostaną wyłączone obie opcje – ***Skanowanie w tle*** i ***Skanowanie proaktywne***, skaner dostępowy będzie wciąż aktywny przy próbie pobrania wiadomości za pomocą klienta MS Outlook.

- ***Skanowanie plików RTF*** − w tym miejscu możliwe jest określenie, czy mają być skanowane pliki RTF.
- ***Nie skanuj wiadomości wychodzących (MS Exchange 2007/2010/2013)*** – przy jednoczesnym wykorzystaniu interfejsu VSAPI i agenta routingu (routing TA) – nieważne, czy na jednym serwerze, czy na osobnych maszynach – może się zdarzyć, że poczta wychodząca będzie skanowana dwukrotnie. Pierwsze skanowanie jest przeprowadzane przez skaner dostępowy VSAPI, natomiast drugie – przez agenta transportu routingu. Może to spowodować pewne spowolnienie serwera oraz wydłużenie czasu oczekiwania na wysłanie wiadomości. Jeśli jesteś pewien, że posiadasz zainstalowane (i aktywne) oba składniki dla serwerów, możesz zaznaczyć to pole, by wyłączyć skaner dostępowy VSAPI i uniknąć dwukrotnego skanowania.
- ***Liczba wątków skanujących*** − proces skanowania jest domyślnie podzielony na określoną liczbę jednocześnie wykonywanych wątków (w celu zwiększenia ogólnej wydajności skanowania). W tym polu można zmienić liczbę wątków.

  Domyślna liczba wątków jest obliczana według wzoru: 2 * liczba procesorów + 1.

  Minimalna liczba wątków jest obliczana według wzoru: (liczba procesorów + 1) podzielona przez 2.

  Maksymalna liczba wątków jest obliczana według wzoru: (liczba procesorów pomnożona przez 5) + 1.

  W przypadku, gdy wartość jest równa minimalnej (lub od niej mniejsza) bądź równa maksymalnej (lub od niej większa), użyta zostanie wartość domyślna.

- ***Limit czasu skanowania*** – maksymalny czas (w sekundach) dostępu jednego wątku do skanowanej wiadomości (wartość domyślna to 180 sekund).

Sekcja ***Właściwości skanowania***:

- ***Użyj heurystyki*** – zaznacz to pole, aby włączyć analizę heurystyczną podczas skanowania.
- ***Raportowanie potencjalnie niechcianych programów i programów typu spyware*** – tę opcję należy zaznaczyć, aby raportowana była obecność potencjalnie niechcianych programów i programów typu spyware.
- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** – zaznaczenie tego pola umożliwi wykrycie większych ilości oprogramowania szpiegującego, tj. programów, które przy zakupie bezpośrednio od producenta są całkowicie nieszkodliwe, lecz później mogą zostać użyte niezgodnie z przeznaczeniem, w celu wyrządzenia szkody (np. różne paski narzędzi). To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera oraz podniesienie komfortu pracy. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona. Uwaga: Ta funkcja detekcji stanowi uzupełnienie poprzedniej opcji, dlatego w celu

zapewnienia ochrony przed podstawowymi rodzajami oprogramowania szpiegującego poprzednie pole wyboru powinno być zawsze zaznaczone.

- ***Skanuj wewnątrz archiwów*** – opcję tę należy zaznaczyć, aby umożliwić skanerowi skanowanie również wewnątrz archiwów (zip, rar itp.).

W sekcji ***Raportowanie załączników wiadomości e-mail*** możliwe jest wybranie pozycji, które mają być raportowane podczas skanowania. Domyślna konfiguracja może zostać łatwo dostosowana w obszarze ***Informacje***, w sekcji ***Akcje związane z wykryciem*** (patrz niżej).

Dostępne są następujące opcje:

- ***Powiadamiaj o archiwach chronionych hasłem***
- ***Powiadamiaj o dokumentach chronionych hasłem***
- ***Powiadamiaj o plikach zawierających makra***
- ***Powiadamiaj o ukrytych rozszerzeniach***

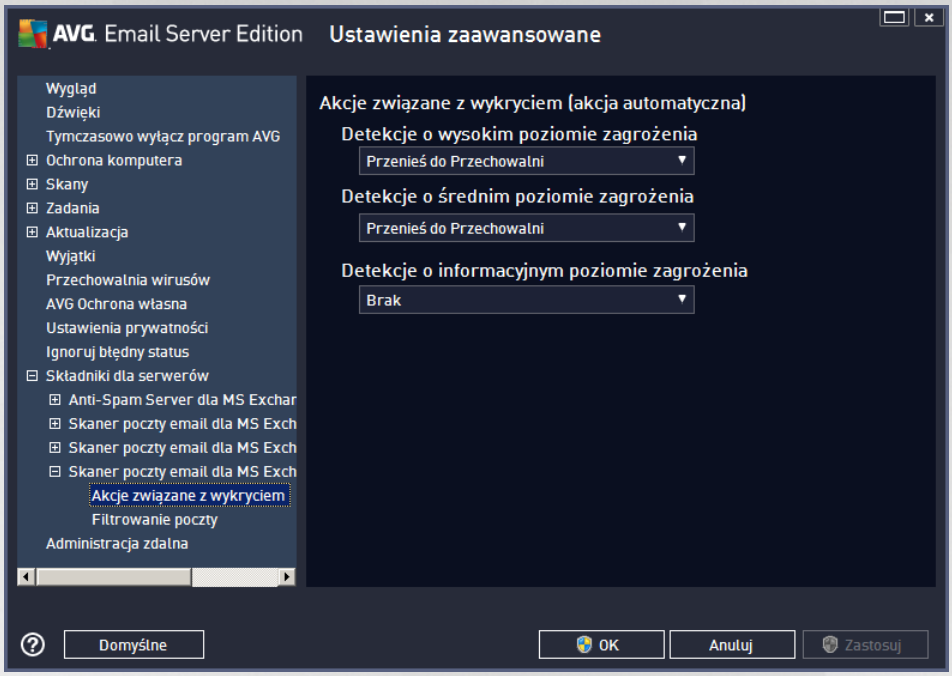
Generalnie niektóre spośród funkcji są rozszerzeniami usług interfejsu aplikacji Microsoft VSAPI 2.0/2.5. Szczegółowe informacje na temat interfejsu VSAPI 2.0/2.5 można znaleźć dzięki poniższym linkom:

- http://support.microsoft.com/default.aspx?scid=kb;pl-pl;328841&Product=exch2k – informacje na temat współpracy 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 dostępne są następujące pozycje:

- ***Akcje związane z wykryciem***
- ***Filtrowanie poczty***

5.5. Akcje związane z wykryciem



W sekcji ***Akcje związane z wykryciem*** można wybrać automatyczne akcje, które mają być wykonywane podczas procesu skanowania.

Akcje te są dostępne dla następujących pozycji:

- ***Detekcje o wysokim poziomie zagrożenia*** – szkodliwy kod, który sam się powiela, często pozostaje niezauważony do czasu, gdy wyrządzi szkody.
- ***Detekcje o średnim poziomie zagrożenia*** – takie programy mogą stanowić poważne zagrożenie komputera lub jedynie potencjalne ryzyko naruszenia prywatności.
- ***Detekcje o informacyjnym poziomie zagrożenia*** – wszystkie wykryte potencjalne zagrożenia, których nie można przypisać do kategorii wymienionych powyżej.

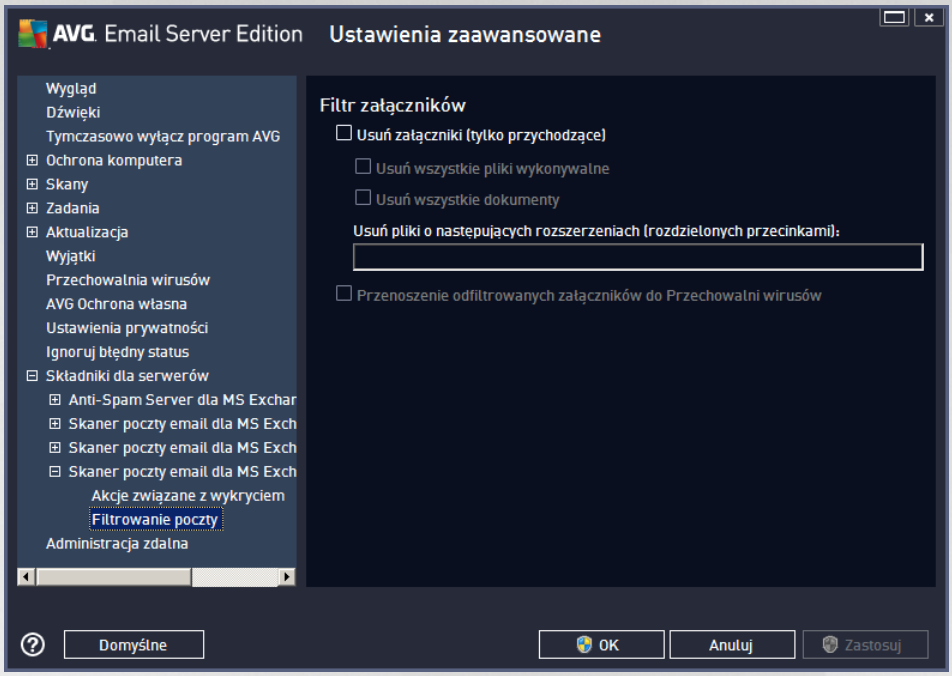
Z menu rozwijanego można wybrać akcję dla każdej pozycji:

- ***Brak*** – nie zostanie podjęta żadna akcja.
- ***Przenieś do Przechowalni*** – dane zagrożenie zostanie przeniesione do Przechowalni wirusów.
- ***Usuń*** – dane zagrożenie zostanie usunięte.

Aby wybrać niestandardowy temat dla wiadomości zawierających określoną pozycję lub zagrożenie, zaznacz pole ***Oznacz temat...*** i wprowadź odpowiednią wartość.

Ostatnia wymieniona funkcja nie jest dostępna dla Skanera poczty e-mail dla MS Exchange VSAPI.

5.6. Filtrowanie poczty



Pozycja ***Filtrowanie poczty*** umożliwia wybór załączników, które będą automatycznie usuwane. Dostępne są następujące opcje:

- ***Usuwaj załączniki*** – zaznacz to pole wyboru, aby włączyć tę funkcję.
- ***Usuń wszystkie pliki wykonywalne*** – usuwa wszystkie pliki wykonywalne.
- ***Usuń wszystkie dokumenty*** – usuwa wszystkie dokumenty.
- ***Usuń pliki o następujących rozszerzeniach (rozdzielonych przecinkami)*** – w tym polu należy wprowadzić rozszerzenia plików, które mają być automatycznie usuwane. Rozszerzenia należy rozdzielać przecinkami.
- ***Przenieś odfiltrowane załączniki do kwarantanny*** – to pole należy zaznaczyć, jeśli odfiltrowane załączniki nie mają być kompletnie usuwane. Po zaznaczeniu tego pola wszystkie załączniki wybrane w tym oknie dialogowym będą automatycznie przenoszone do Przechowalni wirusów. Jest to bezpieczne miejsce służące do przechowywania potencjalnie szkodliwych plików – możliwe jest tam ich przeglądanie i analizowanie bez narażania systemu na niebezpieczeństwo. Dostęp do kwarantanny można uzyskać z głównego menu interfejsu programu **AVG Email Server Edition**. Wystarczy kliknąć lewym przyciskiem myszy pozycję ***Opcje***, a następnie wybrać pozycję ***Przechowalnia wirusów***.

6. Anti-Spam Server dla MS Exchange

6.1. Zasady działania składnika Anti-Spam

Mianem „spam" określa się niechcianą pocztę e-mail, głównie reklamy produktów lub usług, które są hurtowo wysyłane do wielkiej liczby odbiorców jednocześnie, zapełniając ich skrzynki pocztowe. Spamem nie jest korespondencja seryjna rozsyłana do odbiorców po wyrażeniu przez nich zgody. Spam jest nie tylko irytujący, ale może być również źródłem oszustw, wirusów i obraźliwych treści.

Anti-Spam sprawdza wszystkie przychodzące wiadomości e-mail i oznacza niepożądaną pocztę jako SPAM. Podczas przetwarzania każdej wiadomości wykorzystywanych jest kilka metod analizy oferujących najskuteczniejszą dostępną na rynku ochronę.

6.2. Interfejs składnika Anti-Spam

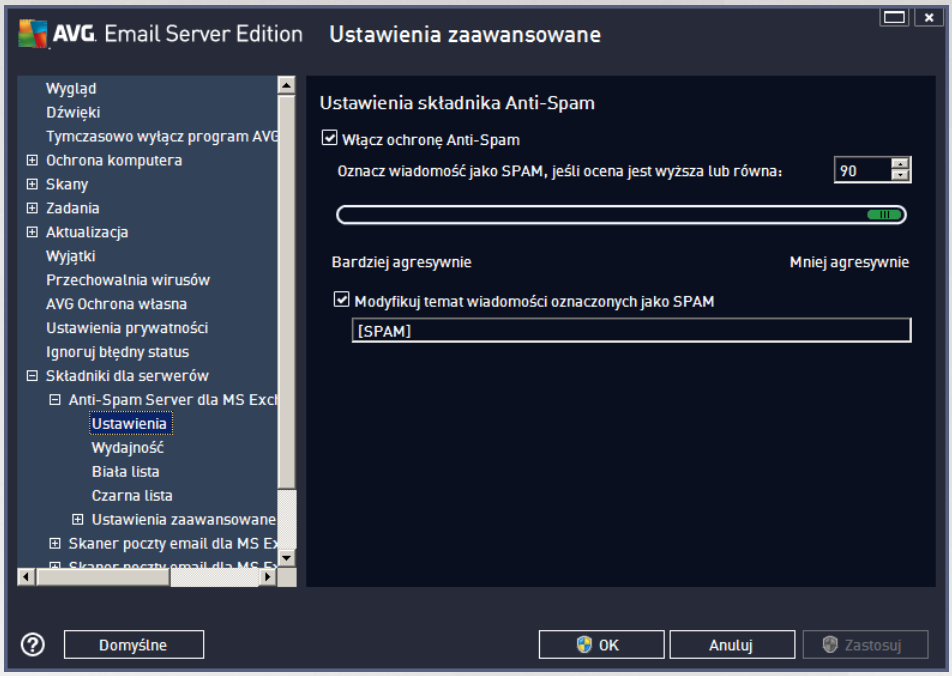
To okno zawiera krótki opis funkcji składnika przeznaczonego dla serwerów, informacje o jego stanie (*Włączony/Wyłączony*) oraz niektóre statystyki.

Dostępne przyciski i linki:

- ***WŁĄCZONY/WYŁĄCZONY*** – kliknięcie tego przycisku włącza/wyłącza wybrany składnik (jeśli jest on włączony, przycisk i tekst będą zielone, a jeśli wyłączony – czerwone).
- ***Odśwież wartości statystyczne*** – aktualizuje powyższe statystyki.
- ***Ustawienia*** – ten przycisk powoduje otwarcie zaawansowanych ustawień składnika Anti-Spam.

6.3. Ustawienia składnika Anti-Spam

6.3.1. Ustawienia



W tym oknie dialogowym można zaznaczyć pole ***Włącz ochronę antyspamową***, aby włączyć/wyłączyć skanowanie wiadomości e-mail w poszukiwaniu spamu.

W tym samym oknie można także wybrać mniej lub bardziej agresywne metody oceny. Filtr ***Anti-Spam*** przypisuje każdej wiadomości ocenę (*tj. wskaźnik informujący, jak bardzo jej treść przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. Ustawienie ***Oznacz wiadomość jako spam, jeśli ocena jest wyższa niż*** można dostosować, wpisując wartość (*od 50 do 90*) albo przesuwając suwak w lewo lub w prawo.

Poniżej przedstawiono opis progów oceny:

- ***Wartość 90*** – większość przychodzących wiadomości e-mail jest normalnie dostarczana (bez oznaczania ich jako spam). Spam, który łatwo zidentyfikować, jest odfiltrowywany, ale znaczna część spamu może nadal trafiać do Twojej skrzynki odbiorczej.

- ***Wartość 80–89*** – wiadomości e-mail, które stanowią potencjalny spam, są poprawnie odfiltrowywane. Niektóre z pożądanych wiadomości (niebędących spamem) mogą zostać błędnie zablokowane.

- ***Wartość 60–79*** – umiarkowanie agresywna konfiguracja. Spam będzie najprawdopodobniej odfiltrowany, lecz wiadomości nie będące spamem mogą również zostać uznane za spam.

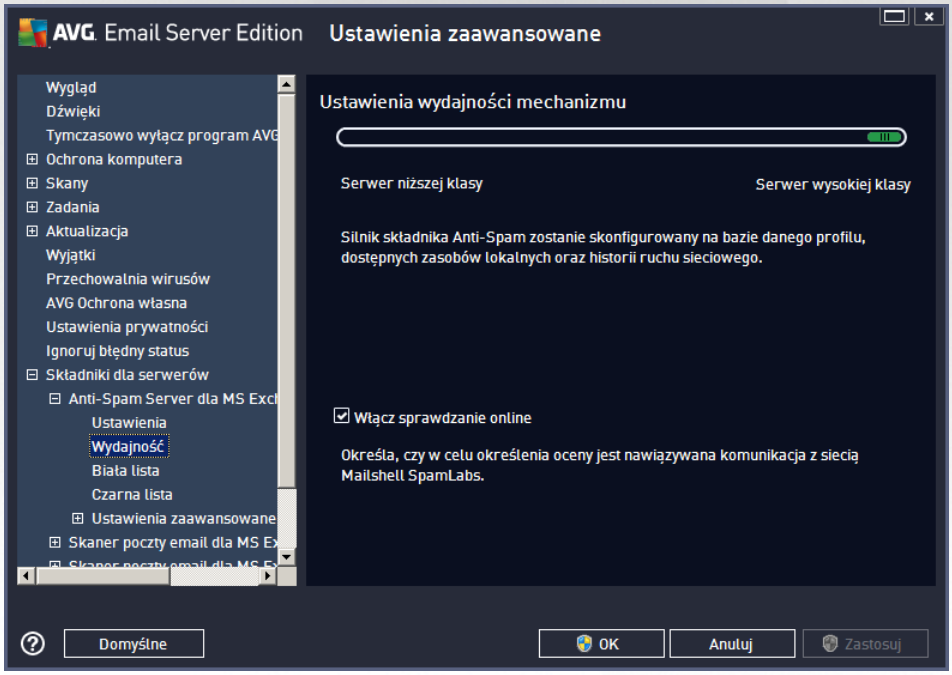
- ***Wartość 50–59*** – bardzo agresywna konfiguracja. Wiadomości e-mail niebędące spamem są odfiltrowywane w równym stopniu, jak wiadomości stanowiące spam. Nie zalecamy stosowania tego progu podczas normalnej pracy.

Następnie można zdefiniować, jakie akcje mają zostać podjęte wobec wiadomości e-mail wykrytych jako spam:

- ***Zmodyfikuj temat wiadomości oznaczonych jako spam*** – jeśli opcja ta jest zaznaczona, wszystkie wykryte wiadomości zawierające spam będą oznaczane (w temacie) wskazaną frazą lub znakiem; żądany tekst można wpisać w polu znajdującym się poniżej.

- ***Pytaj przed wysłaniem raportu o błędnym wykryciu*** – (opcja dostępna, jeśli podczas procesu instalacji wyrażono zgodę na udział w programie udoskonalania produktów) zaznaczenie tej opcji umożliwia nam zbieranie od uczestników programu na całym świecie aktualnych informacji dotyczących najnowszych zagrożeń; dzięki temu możemy udoskonalać zapewnianą im ochronę. Wybór tej opcji oznacza zgodę na raportowanie wykrytych zagrożeń firmie AVG. Raportowanie jest obsługiwane automatycznie. Można jednak zaznaczyć to pole wyboru, aby przed wysłaniem raportu o wykrytym spamie do firmy AVG wyświetlać pytanie, czy dana wiadomość faktycznie jest niepożądana.

6.3.2. Wydajność



Okno ***Ustawienia wydajności mechanizmu*** (*otwierane po kliknięciu pozycji* ***Wydajność*** *w lewym panelu nawigacyjnym*) daje dostęp do ustawień wydajności składnika ***Anti-Spam***. Przesuwając suwak w lewo lub w prawo, można zmienić wydajność skanowania na skali między trybami ***Brak pamięci*** i ***Wysoka wydajność***.

- ***Brak pamięci*** – w czasie skanowania w poszukiwaniu spamu nie będą stosowane żadne reguły. Do identyfikacji będą używane tylko dane szkoleniowe. Ten tryb nie jest zalecany do częstego stosowania, chyba że konfiguracja sprzętowa komputera jest bardzo słaba.

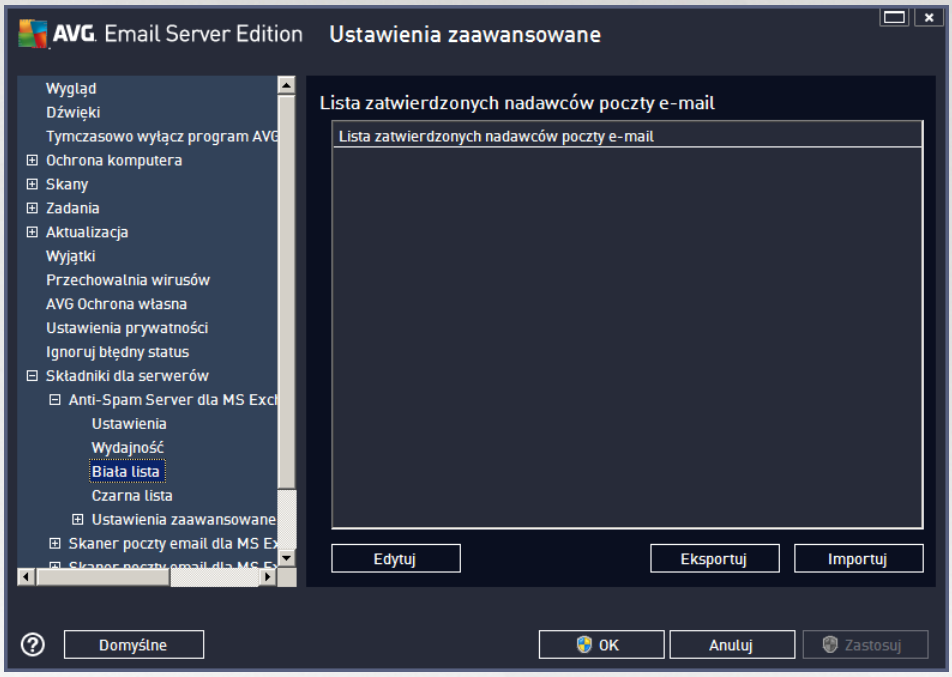
- ***Wysoka wydajność*** – wymaga dużej ilości pamięci. W czasie skanowania w poszukiwaniu spamu stosowane będą następujące funkcje: pamięć podręczna dla reguł i definicji spamu, reguły podstawowe i zaawansowane, adresy IP spamerów i inne bazy danych.

Opcja ***Włącz sprawdzanie online*** jest domyślnie włączona. Pozwala ona skuteczniej wykrywać spam dzięki współpracy z serwerami Mailshell. Skanowane dane są porównywane z bazami danych online firmy Mailshell.

Zwykle zaleca się zachowanie ustawień domyślnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny być wprowadzane wyłącznie przez zaawansowanych użytkowników, którzy doskonale wiedzą, co robią!

6.3.3. Biała lista

Kliknięcie elementu ***Biała lista*** pozwala otworzyć globalną listę akceptowanych adresów nadawców wiadomości e-mail i nazw domen, z których wysyłane wiadomości nigdy nie są oznaczane jako spam.



W interfejsie tym można utworzyć listę nadawców, którzy nigdy nie wysyłają niepożądanych wiadomości (spamu). Można także utworzyć listę nazw całych domen (np. *avg.com*), które nie wysyłają spamu.

Jeśli sporządziłeś już listę adresów i domen, możesz wprowadzić jej elementy pojedynczo lub importować wszystkie na raz. Dostępne są następujące przyciski kontrolne:

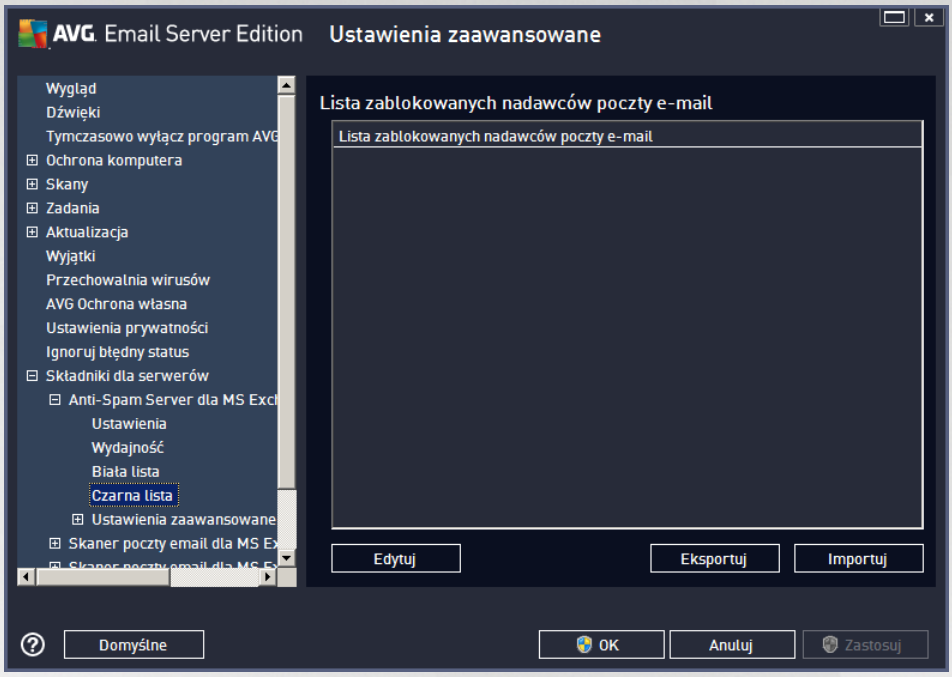
- ***Edytuj*** – *przycisk ten służy do otwarcia okna dialogowego, w którym można ręcznie wprowadzić listę adresów (również za pomocą metody kopiuj-wklej*). Każdą pozycję (nadawcę lub nazwę domeny) należy wprowadzić w osobnym wierszu.

- ***Importuj*** – po kliknięciu tego przycisku można zaimportować istniejącą listę adresów e-mail. Importowany plik musi być plikiem w formacie WAB lub zwykłym plikiem tekstowym zawierającym w każdym wierszu wyłącznie adres i nazwę domeny. Dane można zaimportować również z książki adresowej systemu Windows lub programu Microsoft Office Outlook.

- ***Eksportuj*** – jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zastaną zapisane w zwykłym pliku tekstowym.

6.3.4. Czarna lista

Kliknięcie elementu ***Czarna lista*** pozwala otworzyć globalną listę zablokowanych adresów nadawców wiadomości e-mail i nazw domen, z których wiadomości zawsze są oznaczane jako spam.



W interfejsie tym można utworzyć listę nadawców, którzy wysyłają lub prawdopodobnie będą wysyłali niepożądane wiadomości (spam). Można także utworzyć listę nazw domen (np. *spammingcompany.com*), z których użytkownik otrzymuje (lub spodziewa się otrzymywać) spam. Wszystkie wiadomości e-mail wysłane z tych adresów/domen będą identyfikowane jako spam.

Jeśli sporządziłeś już listę adresów i domen, możesz wprowadzić jej elementy pojedynczo lub importować wszystkie na raz. Dostępne są następujące przyciski kontrolne:

- ***Edytuj*** – *przycisk ten służy do otwarcia okna dialogowego, w którym można ręcznie wprowadzić listę adresów (również za pomocą metody kopiuj-wklej*). Każdą pozycję (nadawcę lub nazwę domeny) należy wprowadzić w osobnym wierszu.

- ***Importuj*** – po kliknięciu tego przycisku można zaimportować istniejącą listę adresów e-mail . Importowany plik musi być plikiem w formacie WAB lub zwykłym plikiem tekstowym zawierającym w każdym wierszu wyłącznie adres i nazwę domeny. Dane można zaimportować również z książki adresowej systemu Windows lub programu Microsoft Office Outlook.

- ***Eksportuj*** – jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zastaną zapisane w zwykłym pliku tekstowym.

6.3.5. Ustawienia zaawansowane

Ta gałąź zawiera zaawansowane ustawienia składnika Anti-Spam. Ustawienia te są przeznaczone wyłącznie dla doświadczonych użytkowników (zwykle administratorów sieci), którzy chcą szczegółowo skonfigurować filtry antyspamowe w celu uzyskania optymalnej ochrony serwerów poczty. Z tego względu nie istnieją tematy pomocy dla poszczególnych okien dialogowych, a jedynie krótkie opisy odpowiednich opcji, dostępne bezpośrednio w interfejsie użytkownika.

Stanowczo zalecamy pozostawienie tych ustawień bez zmian, jeśli nie posiadasz pełnej wiedzy na temat zaawansowanych ustawień silnika antyspamowego Spamcatcher (MailShell Inc.). Nieodpowiednie zmiany mogą skutkować obniżoną wydajnością lub nieprawidłowym działaniem składnika.

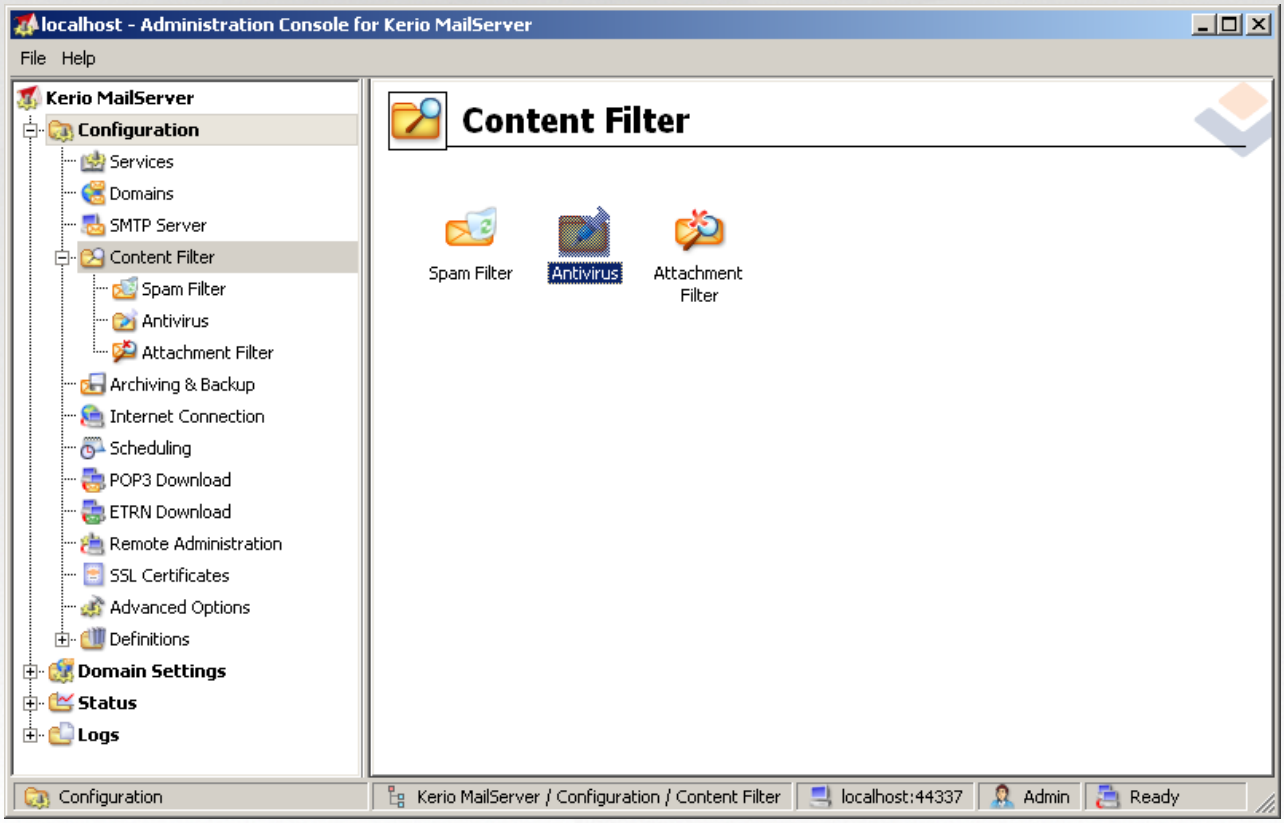
Aby mimo wszystko zmienić zaawansowaną konfigurację składnika Anti-Spam, należy postępować zgodnie z instrukcjami wyświetlanymi w interfejsie użytkownika. Poszczególne okna dialogowe najczęściej odpowiadają tylko jednej funkcji, której opis jest zawsze dostępny w tym samym miejscu:

- ***Filtry*** – lista języków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, fałszywi nadawcy
- ***RBL*** – serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba adresów IP
- ***Połączenie internetowe*** – limit czasu, serwer proxy, uwierzytelnianie na serwerze proxy

7. AVG dla Kerio MailServer

7.1. Konfiguracja

Mechanizm ochrony antywirusowej jest wbudowany w aplikację Kerio MailServer. W celu aktywowania ochrony poczty e-mail w programie Kerio MailServer za pomocą silnika skanującego AVG należy uruchomić aplikację Kerio Administration Console. W drzewie nawigacji po lewej stronie okna należy wybrać gałąź Filtr zawartości (znajdującą się w gałęzi Konfiguracja):

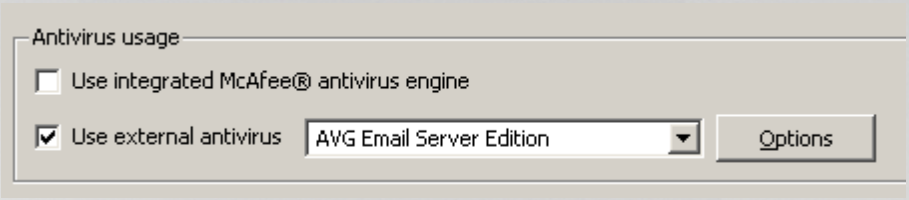


Kliknięcie pozycji Filtr zawartości wyświetli okno dialogowe zawierające trzy pozycje:

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

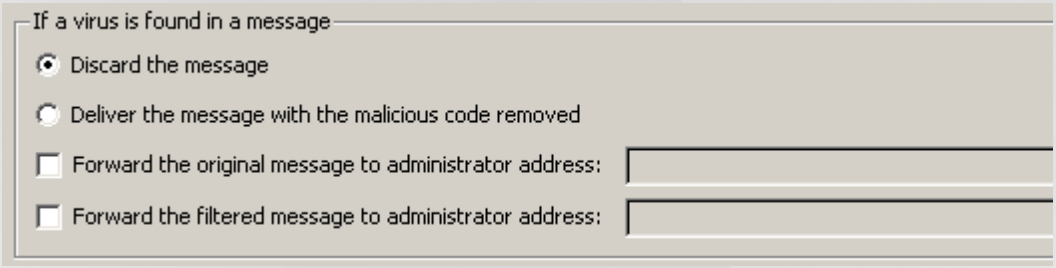
7.1.1. Ochrona antywirusowa

Aby aktywować program AVG dla Kerio MailServer, należy zaznaczyć pole wyboru Używaj zewnętrznego programu antywirusowego, a następnie z menu wybrać program AVG Email Server Edition w oknie konfiguracyjnym:



W następnej sekcji można określić, jakie akcje mają zostać podjęte w stosunku do wiadomości zainfekowanych lub spełniających kryteria filtrowania:

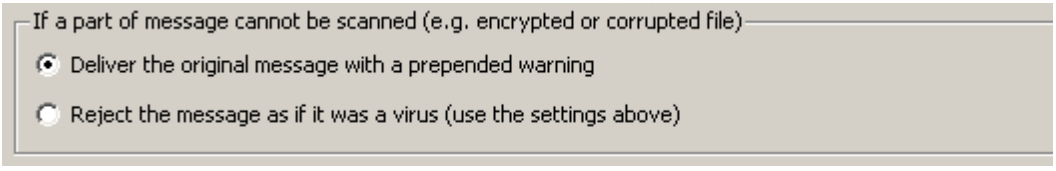
- ***W przypadku wykrycia wirusa w wiadomości e-mail***



W tej ramce można określić akcje, które mają zostać wykonane w przypadku wykrycia wirusa w wiadomości lub wyfiltrowania wiadomości z załącznikiem na podstawie ustawień filtru załączników:

  - ***Usuń wiadomość*** – po wybraniu tej opcji wiadomość zainfekowana lub spełniająca kryteria filtrowania będzie usuwana.
  - ***Dostarcz wiadomość z usuniętym szkodliwym kodem*** – po wybraniu tej opcji wiadomość zostanie dostarczona do odbiorcy bez potencjalnie szkodliwego załącznika.
  - ***Przekaż oryginalną wiadomość na adres administratora*** – po wybraniu tej opcji wiadomość zainfekowana wirusem będzie przekazywana na adres określony w polu tekstowym.
  - ***Przekaż wiadomość spełniającą kryteria filtrowania na adres administratora*** – po wybraniu tej opcji wiadomość spełniającą kryteria filtrowania będzie przekazywana na adres określony w polu tekstowym.

- ***W przypadku gdy nie można przeskanować części wiadomości (np. uszkodzony lub zaszyfrowany plik)***



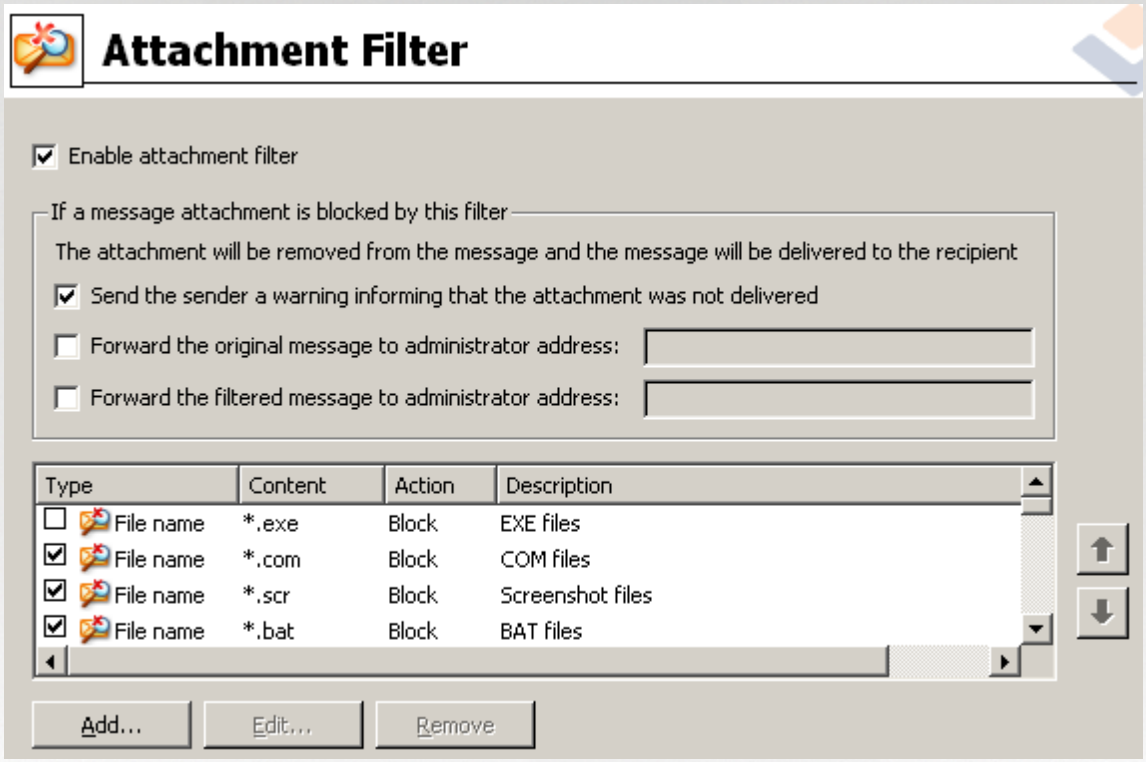
W tej ramce można określić akcje, które mają zostać wykonane w przypadku, gdy nie można przeskanować części wiadomości lub załącznika:

  - ***Dostarcz oryginalną wiadomość z przygotowanym ostrzeżeniem – wiadomość (lub załącznik) będzie dostarczany bez sprawdzania.*** Użytkownik zostanie ostrzeżony, że wiadomość może w dalszym ciągu zawierać wirusy.

- ***Odrzuć wiadomość tak, jak w przypadku wykrycia wirusa – system będzie działał w taki sam sposób, jak w przypadku wykrycia wirusa (np. wiadomość zostanie dostarczona bez załączników lub zostanie usunięta).*** Ta opcja jest bezpieczna, jednak przesyłanie zabezpieczonych hasłem archiwów nie będzie możliwe.

7.1.2. Filtr załączników

Menu Filtr załączników zawiera listę różnych definicji załączników:



Filtrowanie załączników wiadomości e-mail można włączyć lub wyłączyć za pomocą pola wyboru Włącz filtr załączników. Można także modyfikować następujące ustawienia:

- ***Wysyłaj do nadawcy ostrzeżenia, że załącznik nie został dostarczony***

  Nadawca otrzyma ostrzeżenie z serwera Kerio MailServer, o tym że wysłana wiadomość zawierała wirusa lub zablokowany załącznik.

- ***Przesyłaj oryginalną wiadomości na adres administratora***

  Wiadomość zostanie przekazana (w pierwotnej formie – z zainfekowanym lub niedozwolonym załącznikiem) na określony, zewnętrzny lub wewnętrzny adres e-mail.

- ***Przesyłaj wiadomości spełniającą kryteria filtrowania na adres administratora***

  Wiadomość bez zainfekowanego lub niedozwolonego załącznika zostanie (niezależnie od innych określonych poniżej akcji) przekazana na określony adres e-mail. Tę funkcję można wykorzystać do sprawdzenia poprawności działania mechanizmu antywirusowego lub filtru załączników.

Każda pozycja na liście załączników ma cztery pola:

- ***Typ*** – rodzaj załącznika określony na podstawie rozszerzenia podanego w polu Zawartość. Dostępne typy to Nazwa pliku lub Typ MIME. Aby uwzględnić lub wykluczyć tę pozycję w filtrowaniu załączników, można zaznaczyć odpowiednie pole.

- ***Zawartość*** – w tym polu można określić rozszerzenie, które ma być filtrowane. Dopuszczalne jest używanie znaków zastępczych (np. ciąg "*.doc" oznacza wszystkie pliki z rozszerzeniem DOC).

- ***Akcja*** – określa akcję, która ma zostać wykonana dla danego załącznika. Dostępne akcje to Akceptuj (akceptuje załącznik) i Blokuj (ta akcja zostanie wykonana zgodnie z ustawieniami znajdującymi się powyżej listy wykluczonych załączników).

- ***Opis*** – w tym polu należy wprowadzić opis załącznika.

Pozycję można usunąć z listy za pomocą przycisku Usuń, a dodać – za pomocą przycisku ***Dodaj...***. Można także zmienić istniejący wpis za pomocą przycisku ***Edytuj***. Zostanie wówczas wyświetlone poniższe okno:

- W polu Opis można wpisać krótki opis załącznika, który ma być filtrowany.

- W polu Jeśli wiadomość e-mail zawiera załącznik można wybrać typ załącznika (Nazwa pliku lub Typ MIME). Dodatkowo można wybrać konkretne rozszerzenie z dostępnej listy lub użyć symboli wieloznacznych.

W polu Wtedy można zdecydować, czy określony załącznik ma być blokowany, czy akceptowany.

8. FAQ i pomoc techniczna

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

Jeśli pomoc ta okaże się niewystarczająca, zalecamy kontakt z działem pomocy technicznej za pośrednictwem poczty e-mail. Zachęcamy do skorzystania z formularza kontaktowego, dostępnego po wybraniu polecenia menu systemowego ***Pomoc/Uzyskaj pomoc online***.