



AVG 9.0 Email Server Edition

Podrecznik uzytkownika

Wersja dokumentu 90.4 (31. 3. 2010)

Copyright AVG Technologies CZ, s.r.o. Wszelkie prawa zastrzezone.
Wszystkie pozostale znaki towarowe sa wlasnoscia ich wlasncieli.

W produkcie zastosowano algorytm MD5 Message-Digest Algorithm firmy RSA Data Security, Inc. utworzony w roku 1991, Copyright (C) 1991-2, RSA Data Security, Inc.

W produkcie wykorzystywany jest kod z biblioteki C-SaCzech. Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

W produkcie zastosowano biblioteki do kompresji zlib, Copyright (c) 1995-2002 Jean-loup Gailly i Mark Adler.

Spis treści

1. Wprowadzenie	4
2. Wymagania instalacyjne AVG	5
2.1 Obsługiwane systemy operacyjne	5
2.2 Obsługiwane serwery poczty e-mail	5
2.3 Minimalne wymagania sprzętowe	5
2.4 Odinstaluj poprzednie wersje	6
2.5 Dodatki Service Pack dla MS Exchange	7
3. Proces instalacji systemu AVG	8
3.1 Uruchamianie instalacji	8
3.2 Umowa licencyjna	9
3.3 Sprawdzanie stanu systemu	9
3.4 Wybór typu instalacji	10
3.5 Aktywacja programu AVG	10
3.6 Instalacja niestandardowa - Folder docelowy	12
3.7 Instalacja niestandardowa - Wybór składników	13
3.8 Instalacja niestandardowa - Baza DataCenter	15
3.9 Instalowanie	15
3.10 Ukończenie instalacji	16
4. Skaner poczty e-mail dla serwera MS Exchange Server 2007/2010	19
4.1 Przegląd	19
4.2 Skaner poczty e-mail dla MS Exchange (routing TA)	23
4.3 Skaner poczty e-mail dla MS Exchange (SMTP TA)	25
4.4 Skaner poczty e-mail dla MS Exchange (VSAPI)	26
4.5 Akcje związane z wykryciem	29
4.6 Filtrowanie poczty	31
5. Skaner poczty e-mail dla serwera MS Exchange Server 2000/2003	32
5.1 Przegląd	32
5.2 VSAPI 2.0	35
5.3 Skaner poczty e-mail dla MS Exchange (VSAPI)	36
5.4 Akcje związane z wykryciem	39
5.5 Filtrowanie poczty	41

6. AVG dla Kerio MailServer	42
6.1 Konfiguracja	42
6.1.1 Ochrona antywirusowa	42
6.1.2 Filtr załączników	42
7. Konfiguracja Anti-Spam	48
7.1 Interfejs składowca Anti-Spam	48
7.2 Zasady działania składowca Anti-Spam	50
7.3 Anti-Spam - Ustawienia	51
7.3.1 Kreator szkolenia składowca Anti-Spam	51
7.3.2 Wybierz folder z wiadomościami	51
7.3.3 Opcje filtrowania wiadomości	51
7.4 Wydajność	57
7.5 RBL	58
7.6 Biała lista	59
7.7 Czarna lista	61
7.8 Ustawienia zaawansowane	62
8. Menedżer ustawień systemu AVG	63
9. FAQ i pomoc techniczna	66



1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację systemu **AVG 9.0 Email Server Edition**.

Gratulujemy zakupu systemu AVG 9.0 Email Server Edition!

System **AVG 9.0 Email Server Edition** należy do linii uznanych i nagradzanych produktów AVG, które zapewniają użytkownikom spokój ducha, a ich komputerom - pełne bezpieczeństwo. Podobnie jak pozostałe produkty, system **AVG 9.0 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 opis funkcji charakterystycznych dla wersji E-mail 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 9.0 Email Server Edition służy do ochrony serwerów pocztowych działających pod następującymi systemami operacyjnymi:

- Windows 2008 Server Edition (x86 i x64)
- Windows 2003 Server (x86, x64) z dodatkiem SP1
- Windows 2000 Server z dodatkiem SP4 + zbiorczy pakiet aktualizacji 1

2.2. Obsługiwane serwery poczty e-mail

Obsługiwane są następujące serwery poczty e-mail:

- **MS Exchange 2000 Server (z dodatkiem Service Pack 1 lub nowszym)**

Uwaga: Zanim możliwe będzie korzystanie z silnika skanującego AVG na serwerze MS Exchange 2000, konieczne jest zainstalowanie dodatku Service Pack 1. Program **AVG dla MS Exchange 2000/2003 Server** korzysta z interfejsu aplikacji VSAPI 2.0 (lub 2.5 w przypadku Exchange 2003), który obecny jest dopiero we wspomnianym dodatku Service Pack.

- **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 sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG 9.0 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 9.0 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. Odinstaluj poprzednie wersje

W przypadku korzystania ze starej wersji aplikacji AVG Email Server przed zainstalowaniem produktu **AVG 9.0 Email Server Edition** konieczne będzie jej ręczne odinstalowanie. Deinstalacja poprzedniej wersji musi zostać wykonana ręcznie przy użyciu standardowych funkcji systemu Windows.

- Z menu Start należy kolejno wybrać opcje **Ustawienia/Panel sterowania/Dodaj lub Usun programy**, a następnie z listy zainstalowanego oprogramowania wybrać odpowiedni program. Należy się upewnić, czy do deinstalacji został wybrany właściwy program AVG. Przed deinstalacją aplikacji AVG File Server Edition należy również odinstalować program Email Server Edition.
- Po odinstalowaniu aplikacji Email Server Edition, można kontynuować deinstalację poprzedniej wersji programu AVG File Server Edition. Można to zrobić, kolejno wybierając z menu Start opcje **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 `setupln.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

Ponieważ program **AVG dla MS Exchange 2000/2003 Server** korzysta z interfejsu VSAPI 2.0/2.5, należy zainstalować dodatek Service Pack 1 (lub nowszy) dla serwera MS Exchange 2000. Najnowszy dodatek Service Pack dla serwera MS Exchange 2000 można pobrać, korzystając z linku:

Dodatek Service Pack dla serwera MS Exchange 2000 Server:

<http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.msp>

W przypadku serwera MS Exchange 2003 żaden dodatek Service Pack nie jest wymagany, zaleca się jednak zaktualizowanie systemu i instalację najnowszych dodatków Service Pack i poprawek w celu zapewnienia maksymalnego bezpieczeństwa.

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

<http://www.microsoft.com/exchange/evaluation/sp2/overview.msp>

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>

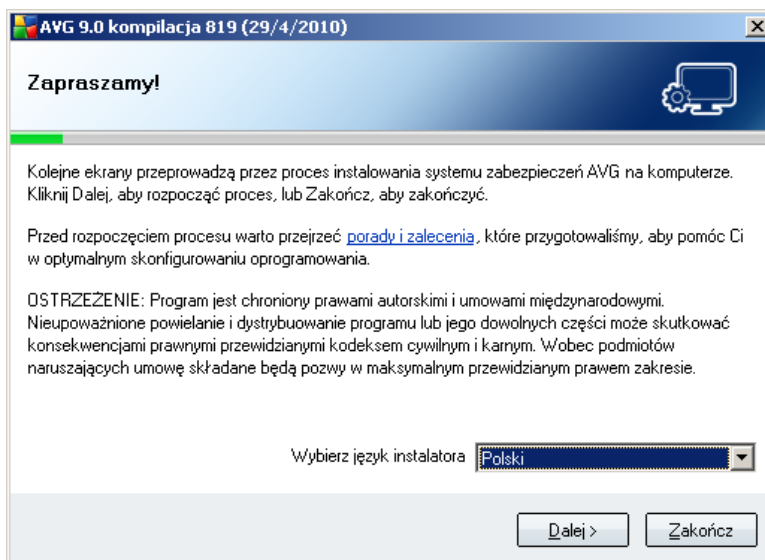
3. Proces instalacji systemu AVG

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

Podczas procesu instalacji konieczne jest podanie numeru licencji. Należy więc przygotować go przed rozpoczęciem instalacji. Numer sprzedaży 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 wyjaśnienia każdego z nich:

3.1. Uruchamianie instalacji



Proces instalacji rozpoczyna się od wyświetlenia **okna powitalnego**. Można w nim wskazać język, który ma być używany podczas instalacji. W dolnej części okna znajdziesz menu **Wybierz język instalatora**. Kliknij przycisk **Dalej**, aby potwierdzić wybór i przejść do kolejnego ekranu.

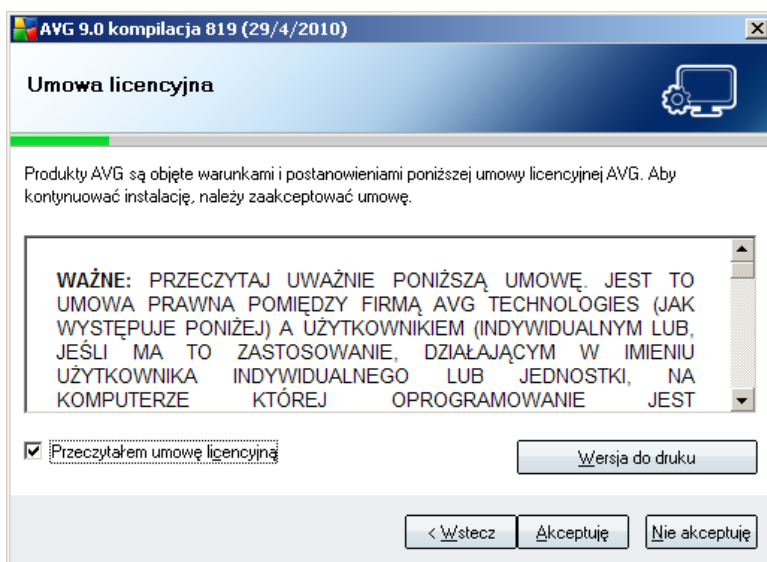
Uwaga: Podczas procesu instalacji możliwe będzie również wybranie innych

dodatkowych języków interfejsu aplikacji.

3.2. Umowa licencyjna

Okno dialogowe **Umowa licencyjna** zawiera pełną treść umowy licencyjnej AVG. Przeczytaj ją uważnie i potwierdź jej akceptację, zaznaczając pole **Przeczytałem warunki umowy licencyjnej** i wciskając przycisk **Akceptuję**. Jeśli nie zgadzasz się z postanowieniami umowy, kliknij przycisk **Nie akceptuję**; instalacja zostanie natychmiast przerwana.

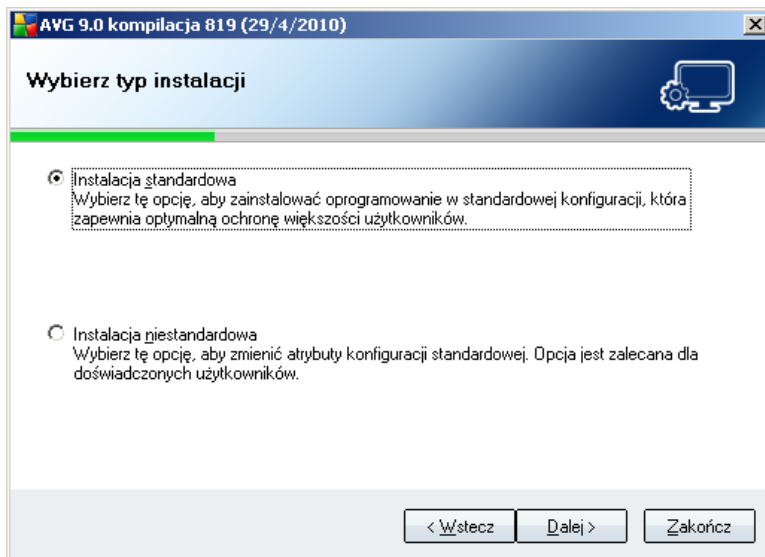
Aby wyświetlić umowę licencyjną w nowym oknie umożliwiającym jej wydrukowanie, kliknij przycisk **Wersja do druku**.



3.3. Sprawdzanie stanu systemu

Po potwierdzeniu umowy licencyjnej zostaniesz przeniesiony do okna **Sprawdzanie stanu systemu**. W oknie tym nie trzeba wykonywać żadnych czynności; system jest sprawdzany przed rozpoczęciem instalacji AVG. Należy poczekać na ukończenie procesu; przejście do kolejnego okna nastąpi automatycznie.

3.4. Wybór typu instalacji



Okno dialogowe **Wybierz typ instalacji** daje możliwość wybrania jednej z dwóch opcji: **Instalacji standardowej** lub **Instalacji niestandardowej**.

Większość użytkowników zdecydowanie powinna wybrać opcję **Instalacja standardowa**, która pozwala zainstalować system AVG w całkowicie zautomatyzowany sposób, z ustawieniami zdefiniowanymi przez dostawcę oprogramowania AVG. 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.

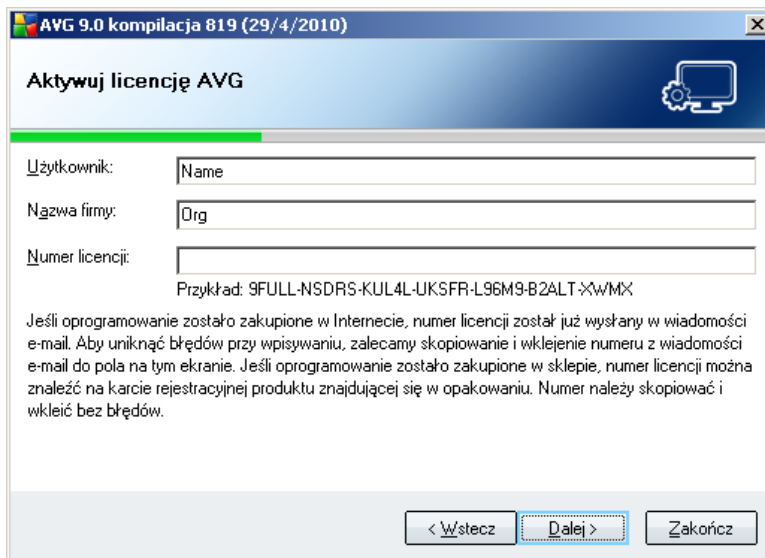
Instalacje niestandardowa powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować systemu AVG z domyślnymi ustawieniami (np. chcą dostosować go do specyficznych wymagań systemowych).

3.5. Aktywacja programu AVG

W oknie dialogowym **Aktywacja licencji AVG** należy wprowadzić swoje dane rejestracyjne. W polu **Nazwa użytkownika** wprowadź swoje imię i nazwisko, a w polu **Nazwa firmy** - nazwę organizacji.

Następnie 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 go i wklejenie w odpowiednim

polu.

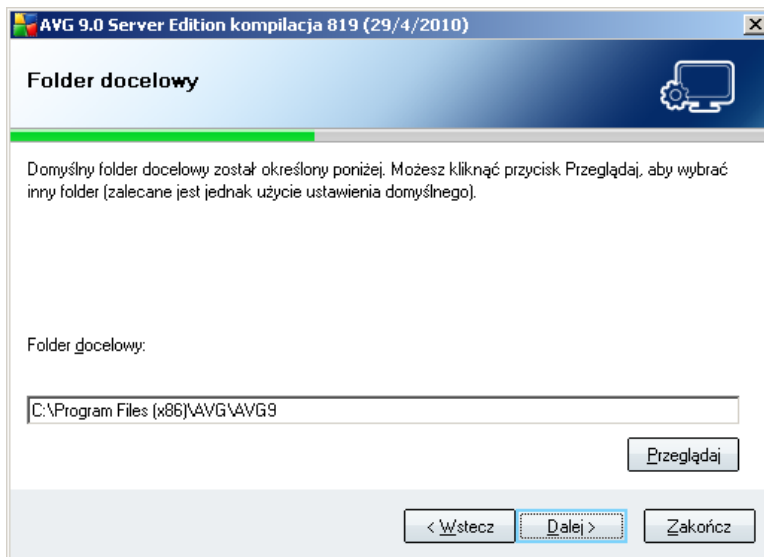


The screenshot shows a window titled "AVG 9.0 kompilacja 819 (29/4/2010)" with a sub-header "Aktywuj licencję AVG". It contains three input fields: "Użytkownik:" with "Name", "Nazwa firmy:" with "Org", and "Numer licencji:" which is empty. Below the fields is a text block with instructions and an example license key: "Przykład: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XXWMXX". At the bottom are three buttons: "< Wstecz", "Dalej >", and "Zakończ".

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

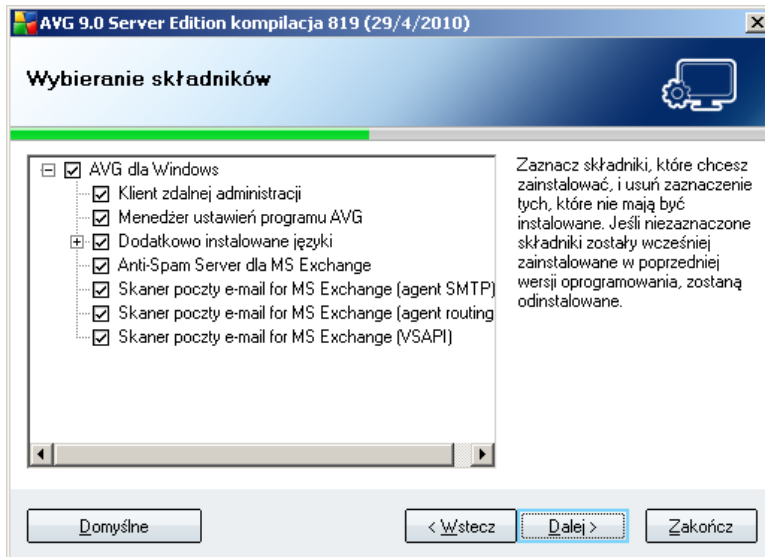
Jeśli w poprzednim kroku została wybrana instalacja standardowa, nastąpi przekierowanie bezpośrednio do okna dialogowego **Podsumowanie instalacji**. Jeśli została wybrana instalacja niestandardowa, zostanie wyświetlone okno **Folder docelowy**.

3.6. Instalacja niestandardowa - Folder docelowy



Okno **Folder docelowy** pozwala określić lokalizację dla plików systemu 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. Kliknij przycisk **Dalej**, aby potwierdzić wybór.

3.7. Instalacja niestandardowa - Wybór składników



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

Wybierac można jednak tylko składniki należące do zakupionej edycji systemu AVG. Tylko one będą widoczne w oknie dialogowym Wybór składników!

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

Uwaga: Tylko składniki serwera dostępne na liście mogą być zarządzane zdalnie!

- **Menedżer ustawień systemu AVG** - narzędzie przeznaczone przede wszystkim dla administratorów sieci, pozwalające na kopiowanie, edycje i dystrybucje konfiguracji systemu AVG. Konfiguracja może zostać zapisana na urządzeniu przenośnym (dysk USB itp.), a następnie zastosowana ręcznie (lub w dowolny inny sposób) na wybranych stacjach roboczych.
- **Instalacja dodatkowych języków** - ta opcja umożliwi 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 serwera:

- **Anti-Spam Server for 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.

- **Skanner 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 może zostać zainstalowany tylko dla serwera w roli HUB.

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

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

Składnik dostępny dla MS Exchange 2007 może zostać zainstalowany dla serwera w roli EDGE lub HUB.

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

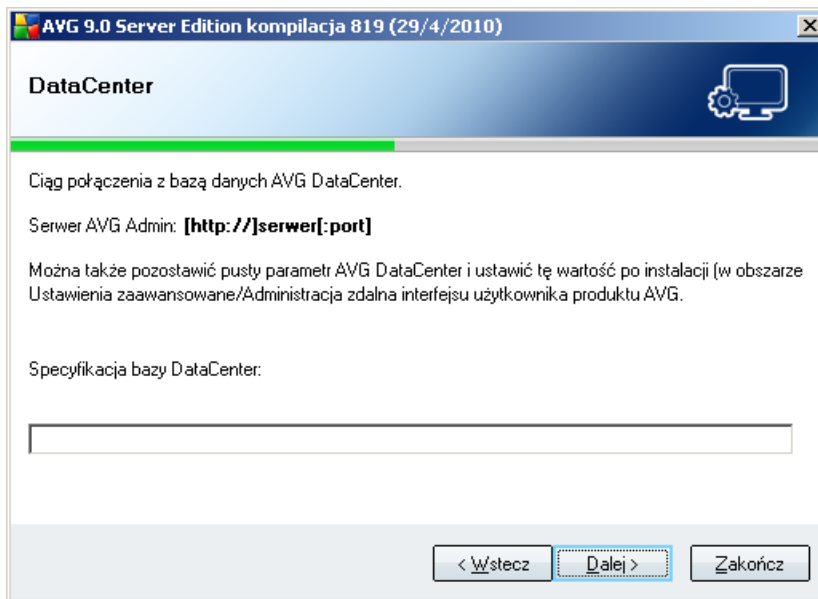
Sprawdza wszystkie wiadomości e-mail przechowywane w skrzynkach pocztowych użytkownika. Wszystkie wykryte wirusy są przenoszone do Przechowalni lub usuwane.

Uwaga: Opcje dostępne dla serwerów MS Exchange 2007 i MS Exchange 2003 różnią się.

Aby kontynuować, kliknij przycisk **Dalej**.

3.8. Instalacja niestandardowa - Baza DataCenter

Jesli przy wyborze skladników zostala wybrana **Administracja zdalna**, na tym ekranie mozliwe bedzie okreslenie parametrów polaczenia z baza AVG DataCenter.

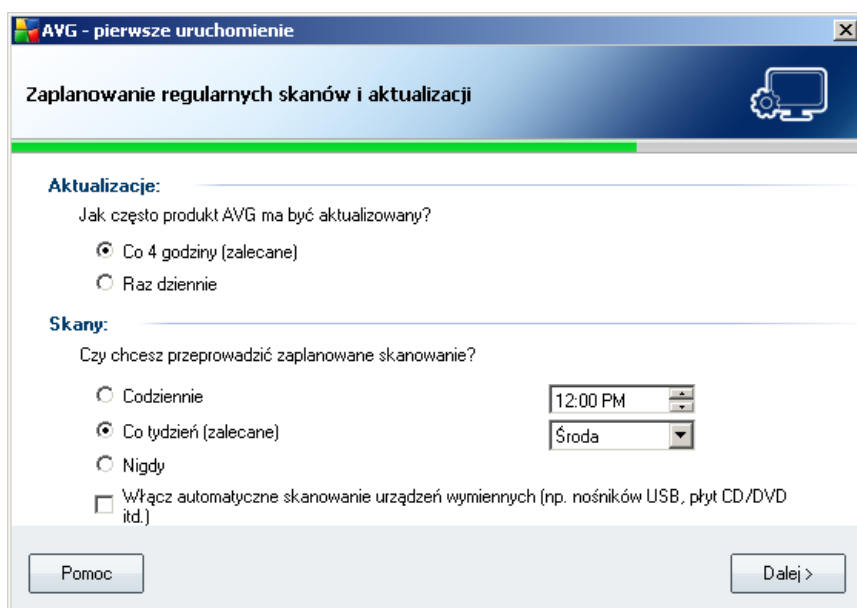


3.9. Instalowanie

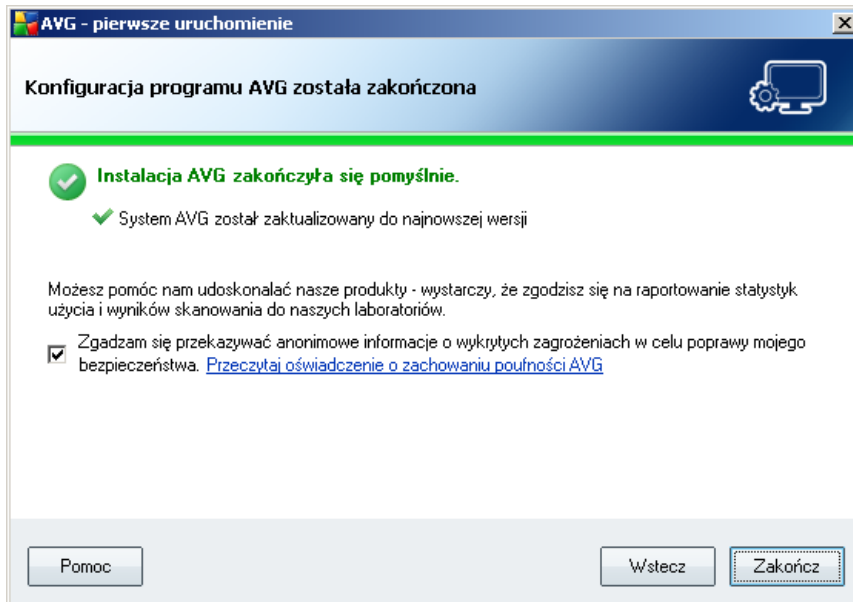
Okno **Instalowanie** zawiera jedynie informacje o postępie instalacji i nie wymaga żadnych działań ze strony użytkownika. Należy poczekać na ukończenie instalacji, po której nastąpi przekierowanie do okna **Instalacja zakończona**.

3.10. Ukończenie instalacji

Kreator pierwszego uruchomienia jest automatycznie uruchamiany podczas instalacji. Konieczne jest ukończenie wszystkich jego kroków:

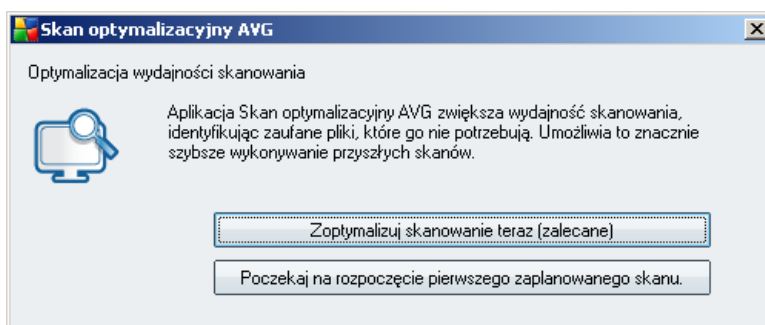


W oknie dialogowym **Zaplanowanie regularnych skanów i aktualizacji** można częstotliwość uruchamiania skanów zaplanowanych oraz sprawdzania dostępności nowych plików aktualizacyjnych. Zaleca się zachowanie wartości domyślnych. Aby kontynuować, kliknij przycisk **Dalej**.



W tym oknie dialogowym należy wskazać, czy informacje o znalezionych zagrożeniach i szkodliwych witrynach mają być anonimowo przesyłane do laboratorium wirusów AVG. Jeśli tak, należy zaznaczyć opcję **Zgadzam się dostarczać ANONIMOWE informacje o wykrytych zagrożeniach, aby podnieść swój poziom ochrony**. Aby kontynuować, kliknij przycisk **Zakończ**.

Zostanie wyświetlone okno dialogowe **Skan optymalizacyjny AVG**. Funkcja optymalizacji skanowania przeszukuje foldery *Windows* i *Program Files* w poszukiwaniu odpowiednich plików (*obecnie są to pliki *.exe, *.dll i *.sys*) i zapisuje informacje o nich. Przy kolejnych próbach uzyskania dostępu do nich, nie będą one więcej skanowane, dzięki czemu czas przyszłych testów ulegnie znacznemu skróceniu.



Zalecamy skorzystanie z tej opcji i uruchomienie procesu optymalizacji. W tym celu należy kliknąć przycisk **Optymalizuj skanowanie teraz**.



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

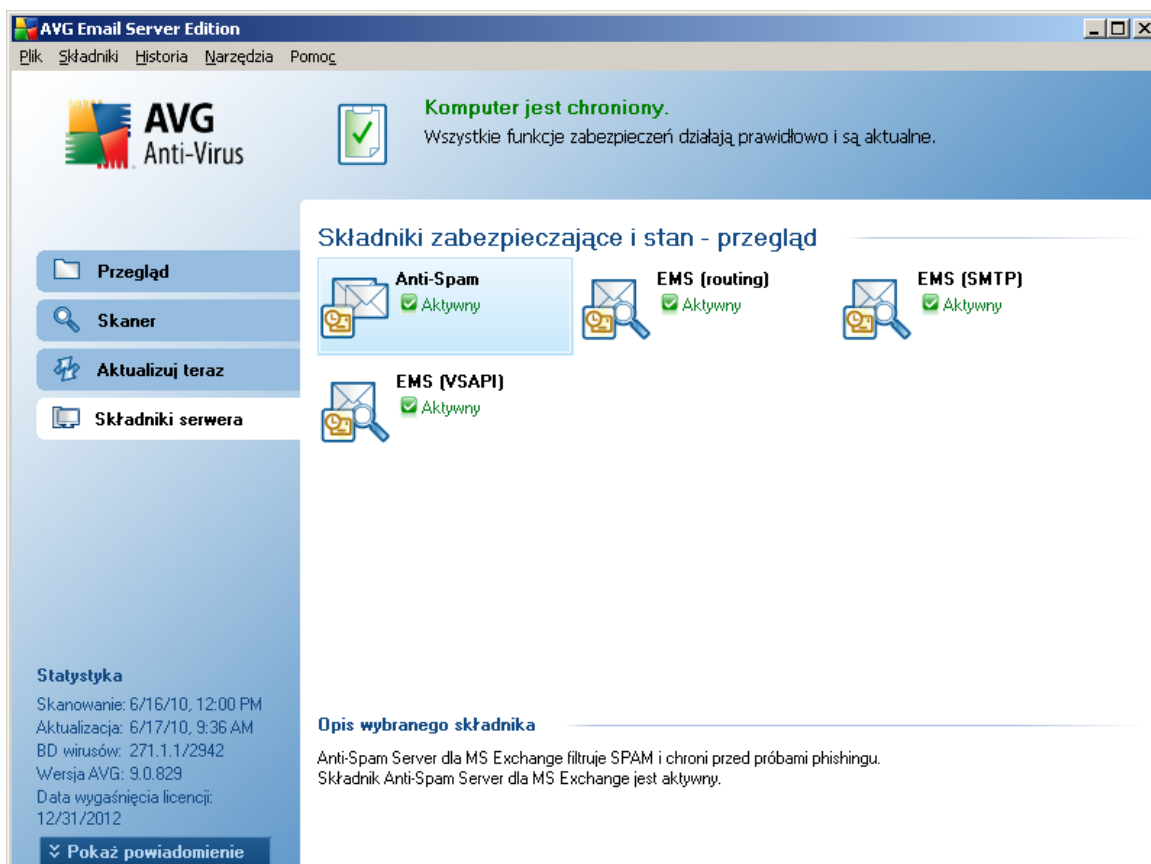
Aby skonfigurować opcje ochrony serwera poczty e-mail, należy przejść do odpowiedniego rozdziału:

- [***Skaner poczty e-mail dla serwera MS Exchange Server 2007/2010***](#)
- [***Skaner poczty e-mail dla serwera MS Exchange Server 2000/2003***](#)
- [***AVG dla Kerio MailServer***](#)

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

4.1. Przegląd

Opcje konfiguracji produktu AVG dla MS Exchange Server 2007 są w pełni zintegrowane z produktem AVG 9.0 Email Server Edition jako składniki serwera.



Podstawowy przegląd poszczególnych składników serwera:

- **[Anti-Spam - 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.

- **[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 MS Exchange 2007 moze zostac zainstalowany tylko dla serwera w roli HUB.

- **[EMS \(SMTP\) - Skaner poczty e-mail dla MS Exchange \(agent SMTP\)](#)**

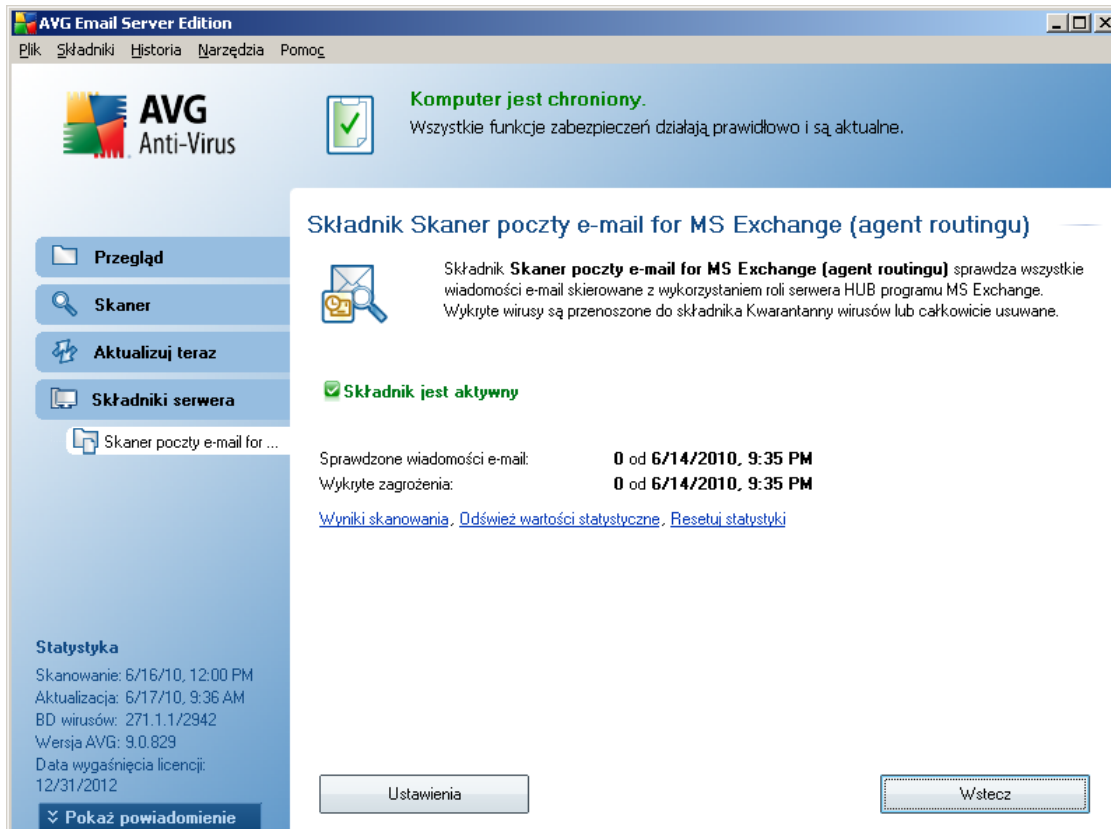
Sprawdza wszystkie wiadomosci e-mail przechodzace przez interfejs MS Exchange SMTP.

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

- **[EMS \(VSAPI\) - Skaner poczty e-mail dla MS Exchange \(VSAPI\)](#)**

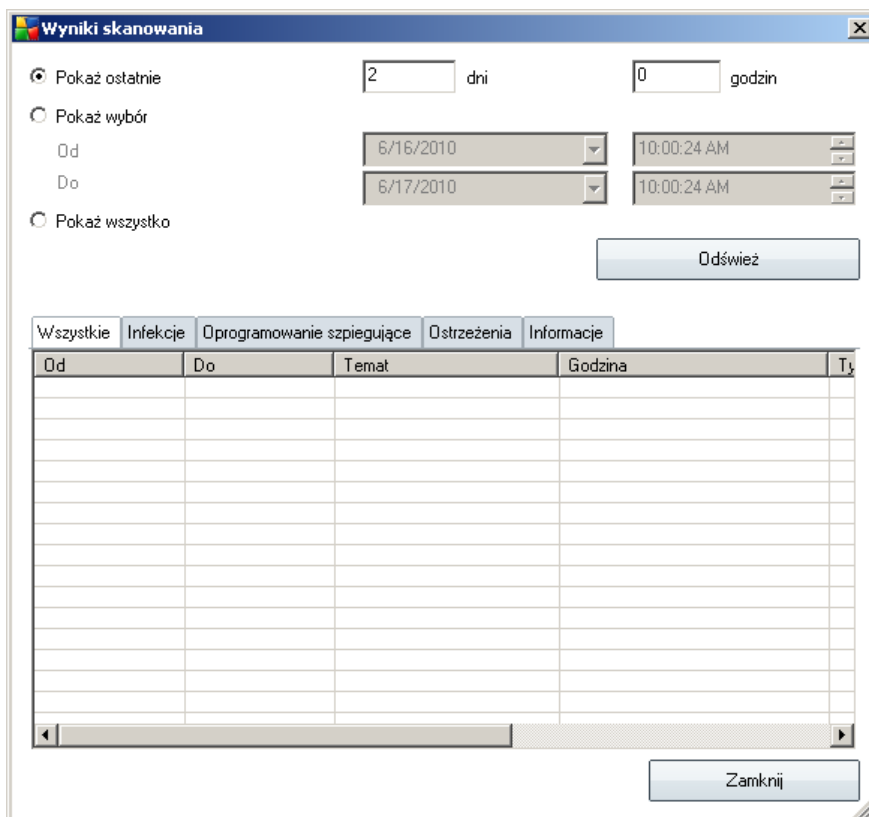
Sprawdza wszystkie wiadomosci e-mail przechowywane w skrzynkach pocztowych uzytkownika. Wszystkie wykryte wirusy sa przenoszone do Przechowalni lub usuwane.

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



- **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.

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

- **Pokaż ostatnie** - wprowadź preferowaną ilość dni i godzin.
- **Pokaż wybrane** - wprowadź niestandardowy przedział czasu i daty.
- **Pokaż wszystko** - wyświetla wszystkie dostępne wyniki.

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

- **Odśwież wartości statystyczne** - aktualizuje powyższe statystyki.
- **Resetuj wartości statystyczne** - zeruje wszystkie statystyki.

Dostępne przyciski:

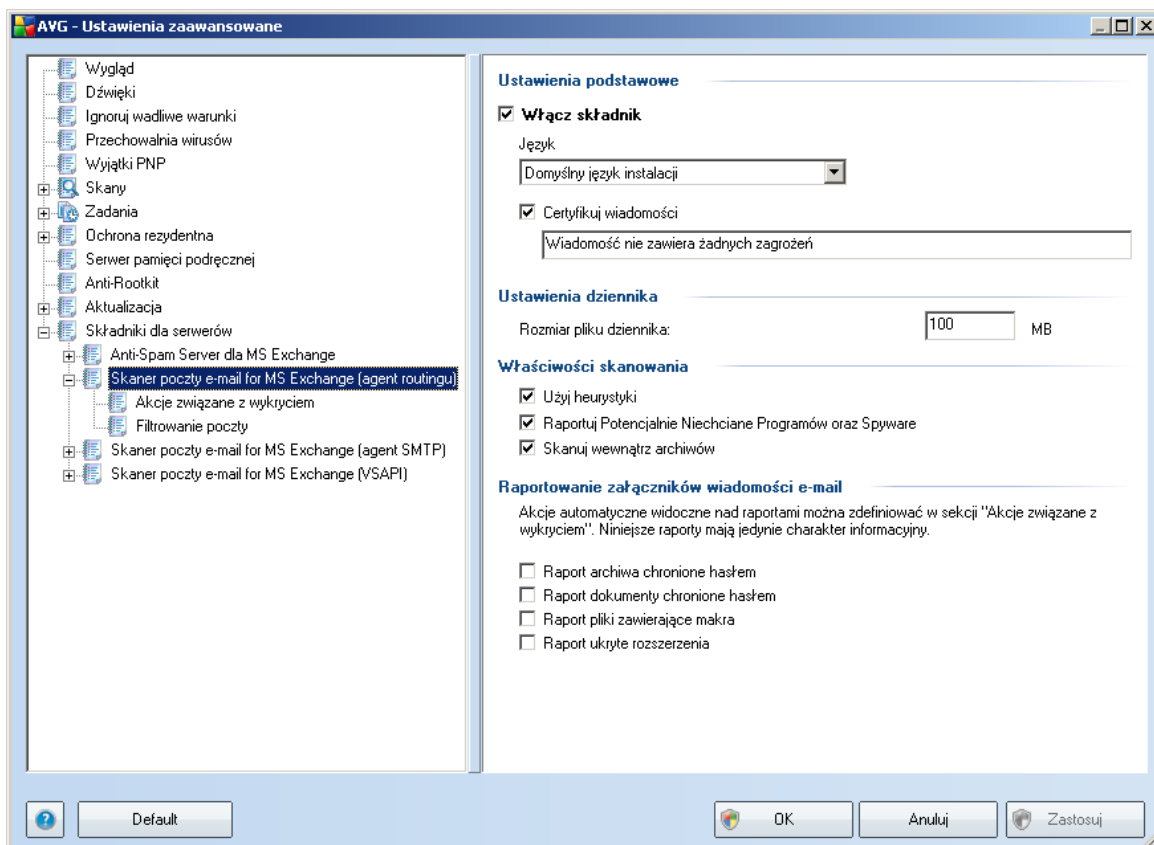
- **Ustawienia** - ten przycisk pozwala otworzyć ustawienia składowca.
- **Wstecz** - ten przycisk umożliwia powrót do okna Przegląd składowców serwera.

Wiecej informacji na temat indywidualnych ustawień wszystkich składowców można znaleźć w rozdziałach poniżej.

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

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

Z listy **Składowki 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.
- **Jezyk** - wybierz preferowany jezyk składnika.
- **Certyfikuj wiadomosci** - zaznacz to pole, aby do wszystkich skanowanych wiadomosci dołączac certyfikacje. Jej tresc mozna dostosowac w kolejny polu.

Sekcja **Ustawienia dziennika**:

- **Rozmiar pliku dziennika** - wybierz preferowany rozmiar pliku dziennika. Wartość domyślna: 100 MB.

Sekcja **Wlasciwosci skanowania**:

- **Uzyj heurystyki** - zaznacz to pole, aby włączyc analize heurystyczna podczas skanowania.
- **Raportowanie potencjalnie niechcianych programów i programów typu spyware** - opcje te nalezy zaznaczyc, aby raportowana byla obecność potencjalnie niechcianych programów i programów typu spyware.
- **Skanuj wewnatrz archiwów** - opcje te nalezy zaznaczyc, aby umożliwic skanerowi skanowanie również wewnatrz archiwów (zip, rar itp.)

W sekcji **Raportowanie załączników wiadomosci 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** 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](#)

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

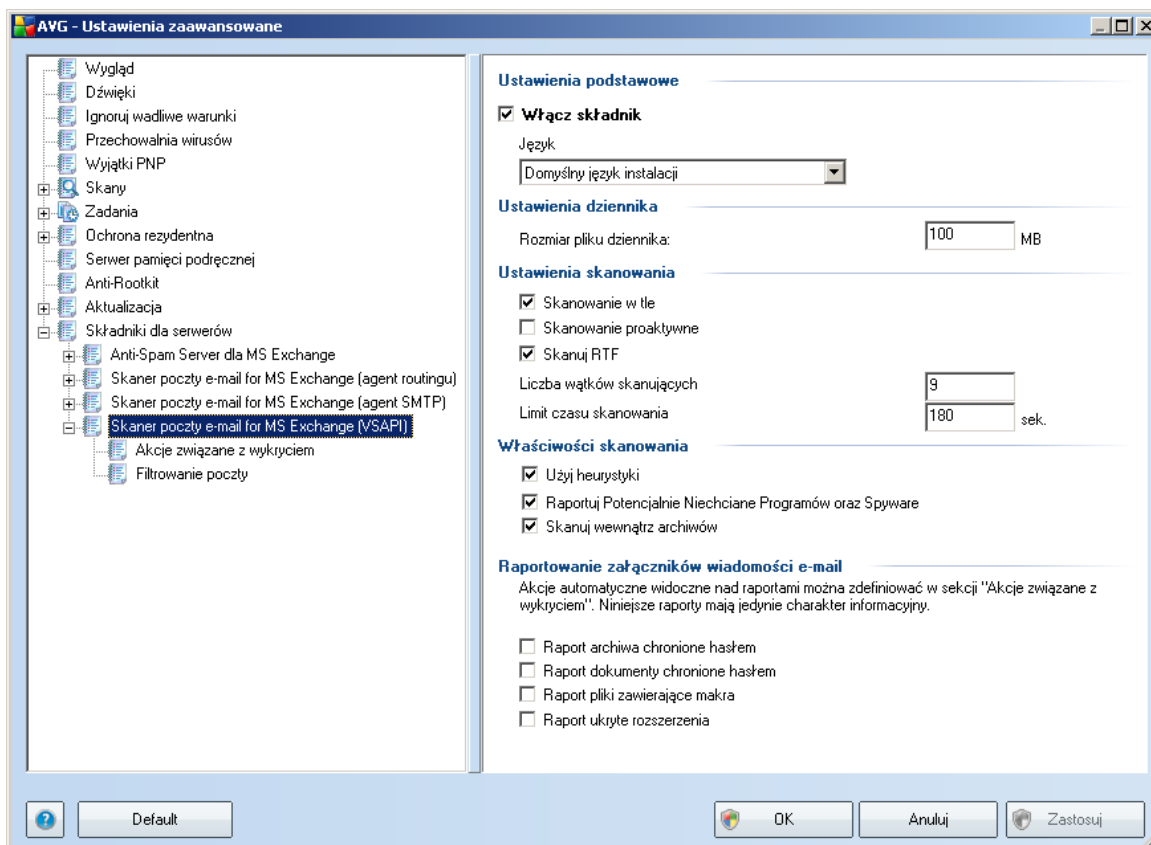
Konfiguracja ***Skanera poczty e-mail dla MS Exchange (agenta SMTP)*** jest dokładnie taka sama jak w przypadku agenta routingu. Więcej informacji na ten temat można znaleźć w rozdziale [***Skaner poczty e-mail dla MS Exchange \(routing TA\)***](#) powyżej.

W strukturze drzewa dostępne są następujące podpozycje:

- [***Akcje związane z wykryciem***](#)
- [***Filtrowanie poczty***](#)

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

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



Sekcja **Ustawienia podstawowe** zawiera następujące opcje:

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

Sekcja **Ustawienia dziennika**:

- **Rozmiar pliku dziennika** - wybierz preferowany rozmiar pliku dziennika. Wartość domyślna: 100 MB.

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 2007 Server. Skanowanie i wyszukiwanie obiektów, które nie zostały jeszcze przeskanowane odbywa się równoległe.

Dla każdej bazy danych stosowany jest określony watek 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 zaządał 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.

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

Uwaga: 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.
- **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: $2 * \text{liczba procesorów} + 1$.

Minimalna liczba wątków jest obliczana według wzoru: $(\text{liczba procesorów} + 1) / 2$.

Maksymalna liczba wątków jest obliczana według wzoru: $(\text{liczba procesorów})$

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** - te opcje należy zaznaczyć, aby raportowana była obecność potencjalnie niechcianych programów i programów typu spyware.
- **Skanuj wewnątrz archiwów** - opcje te należy zaznaczyć, aby umożliwić 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**

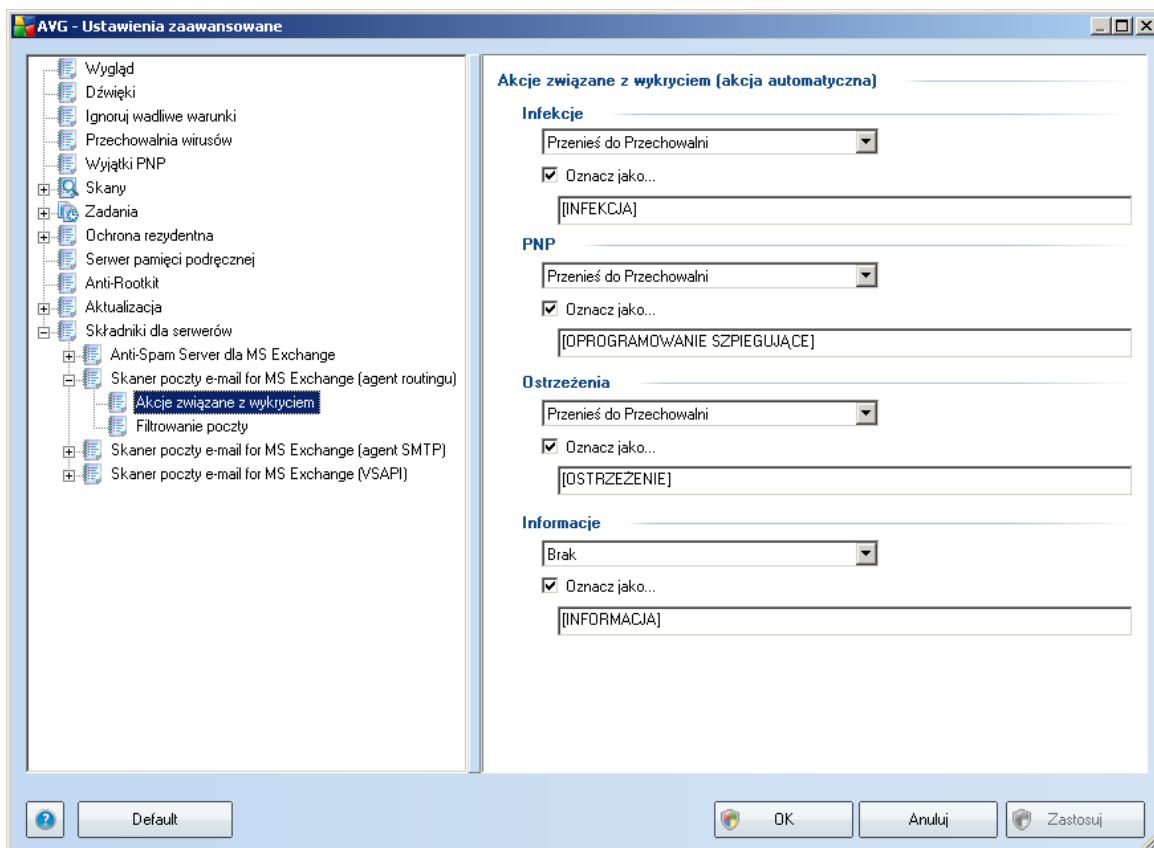
Generalnie, funkcje te są rozszerzeniami usług interfejsu Microsoft VSAPI 2.0/2.5. Szczegółowe informacje na temat interfejsu VSAPI 2.0/2.5 można znaleźć, odwiedzając poniższe linki (oraz linki znajdujące na tych stronach):

- <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](#)

4.5. Akcje związane z wykryciem



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

Akcje te są dostępne dla następujących pozycji:

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

- **Ostrzeżenia**
- **Informacje**

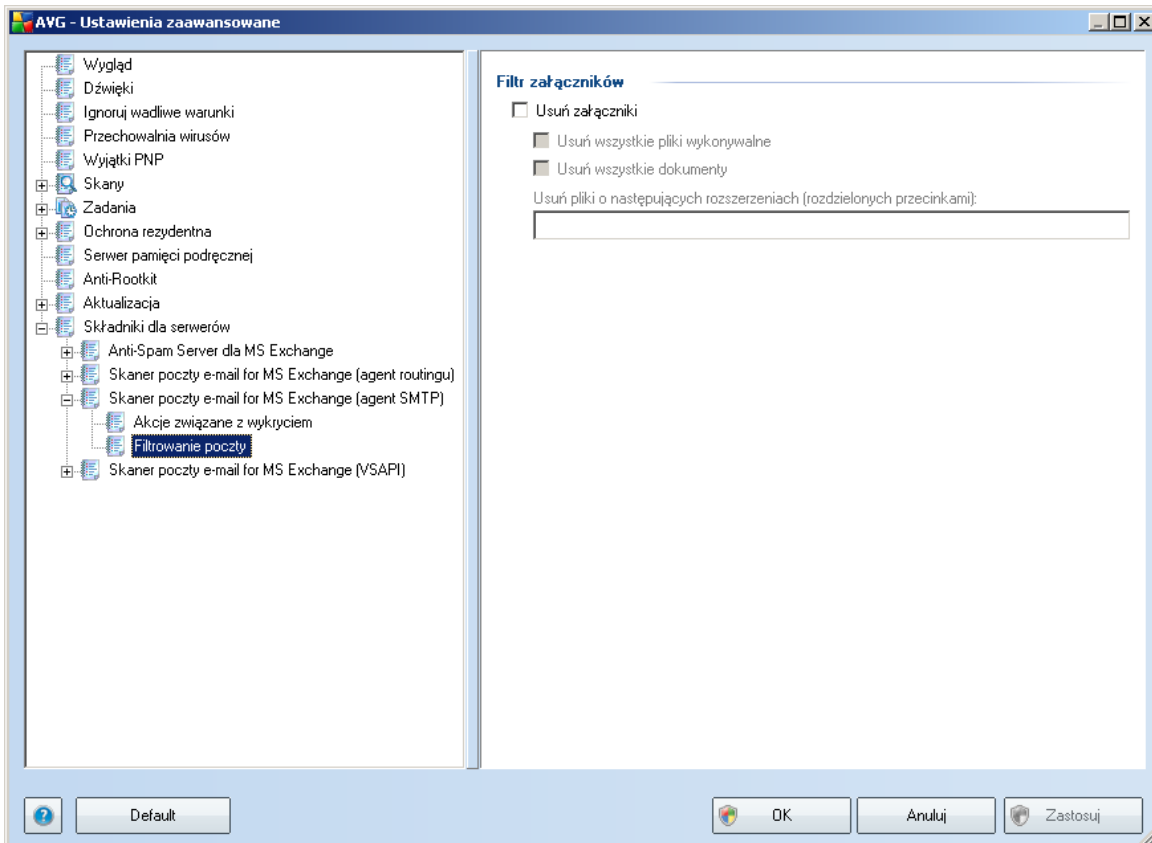
Z menu rozwijanego mozna wybrac akcje dla kazdej pozycji:

- **Brak** - nie zostanie podjeta zadna akcja.
- **Przenies do Przechowalni** - dane zagrozenie zostanie przeniesione do Przechowalni wirusow.
- **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.

4.6. Filtrowanie poczty



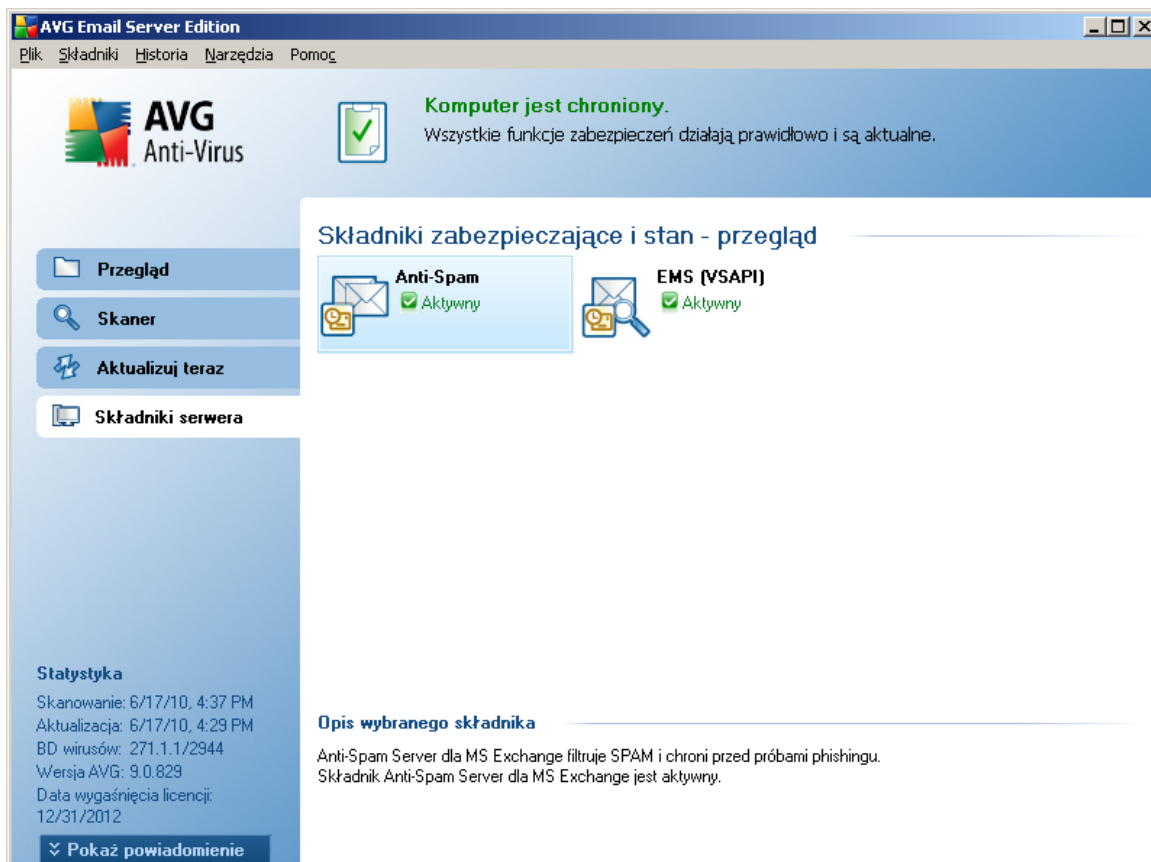
Pozycja **Filtrowanie poczty** umożliwia wybór załączników, które będą automatycznie usuwane. Dostępne są następujące opcje:

- **Usuwać załączniki** - zaznacz to pole wyboru, aby włączyć te funkcje.
- **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.

5. Skaner poczty e-mail dla serwera MS Exchange Server 2000/2003

5.1. Przegląd

Opcje konfiguracji Skanera poczty-email dla MS Exchange Server 2003 są w pełni zintegrowane z produktem AVG 9.0 Email Server Edition (jako składnik serwera).



Dostępne są następujące składniki serwera:

Podstawowy przegląd poszczególnych składników serwera:

- **[Anti-Spam - Anti-Spam Server dla MS Exchange](#)**

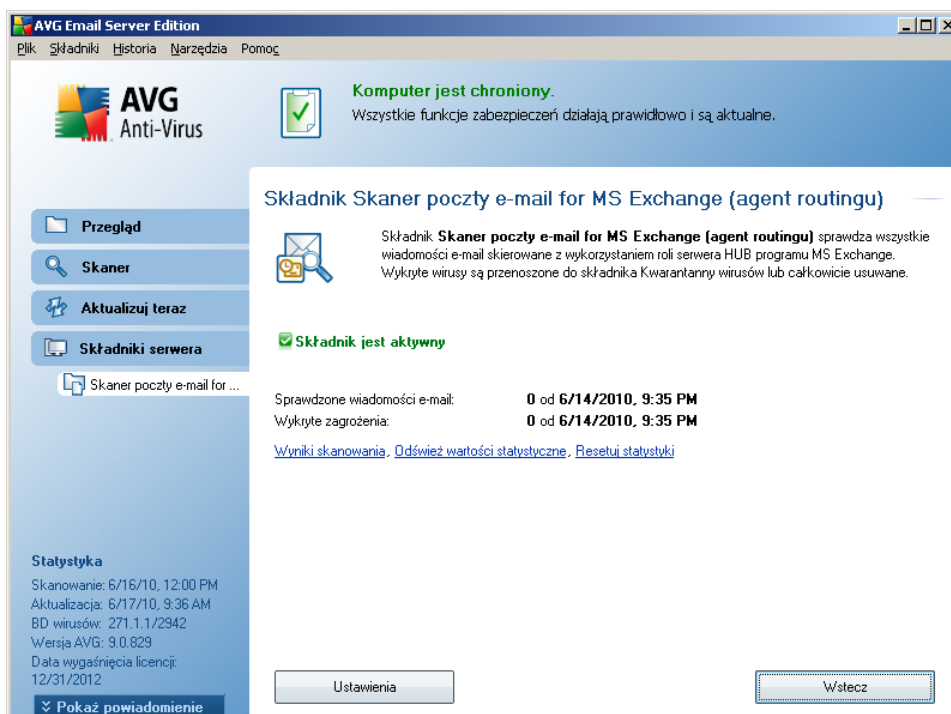
Sprawdza wszystkie przychodzące wiadomości e-mail i oznacza niepożądaną pocztę jako SPAM. Podczas przetwarzania każdej wiadomości wykorzystywanych

jest kilka metod analizy, oferujących najskuteczniejszą dostępną na rynku ochronę.

- **[EMS \(VSAPI\) - Skaner poczty e-mail dla MS Exchange \(VSAPI\)](#)**

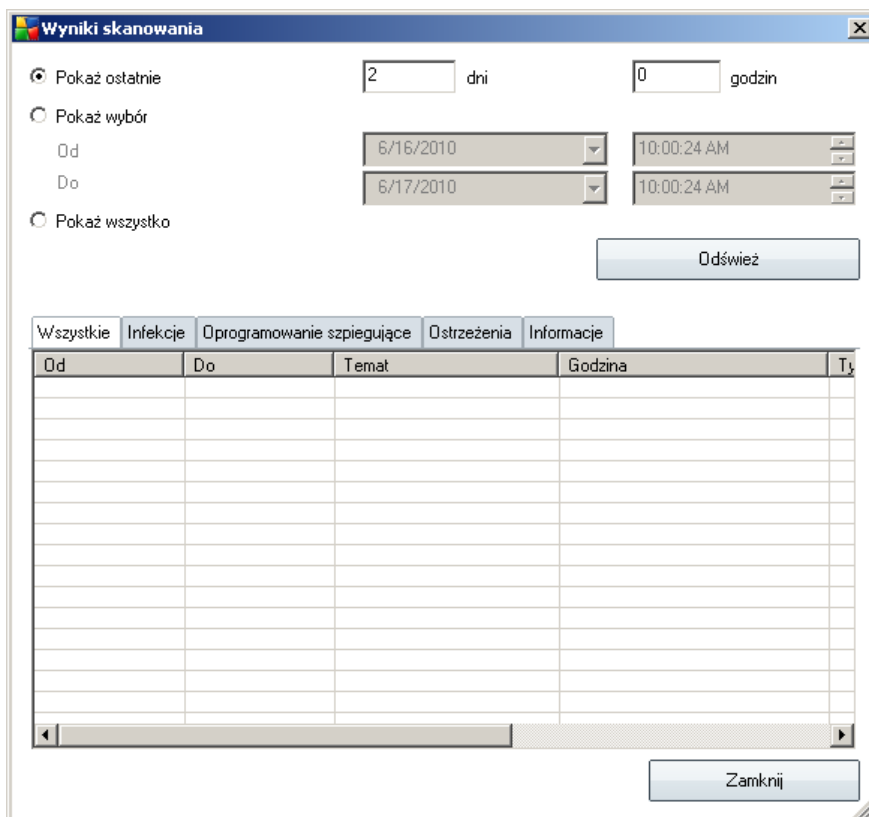
Sprawdza wszystkie wiadomości e-mail przechowywane w skrzynkach pocztowych użytkownika. Wszystkie wykryte wirusy są przenoszone do Przechowalni lub usuwane.

Dwukrotnie kliknij wybrany kładnik, aby otworzyć jego interfejs. Z wyjątkiem składnika Anti-Spam wszystkie składniki posiadają wspólne przyciski i linki:



- ***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.

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

- **Pokaż ostatnie** - wprowadź preferowaną ilość dni i godzin.
- **Pokaż wybrane** - wprowadź niestandardowy przedział czasu i daty.
- **Pokaż wszystko** - wyświetla wszystkie dostępne wyniki.

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

- **Odśwież wartości statystyczne** - aktualizuje powyższe statystyki.
- **Resetuj wartości statystyczne** - zeruje wszystkie statystyki.



Dostępne przyciski:

- **Ustawienia** - ten przycisk pozwala otworzyć ustawienia składnika.
- **Wstecz** - ten przycisk umożliwia powrót do okna Przegląd składników serwera.

Wiecej informacji na temat indywidualnych ustawień wszystkich składników można znaleźć w rozdziałach poniżej.

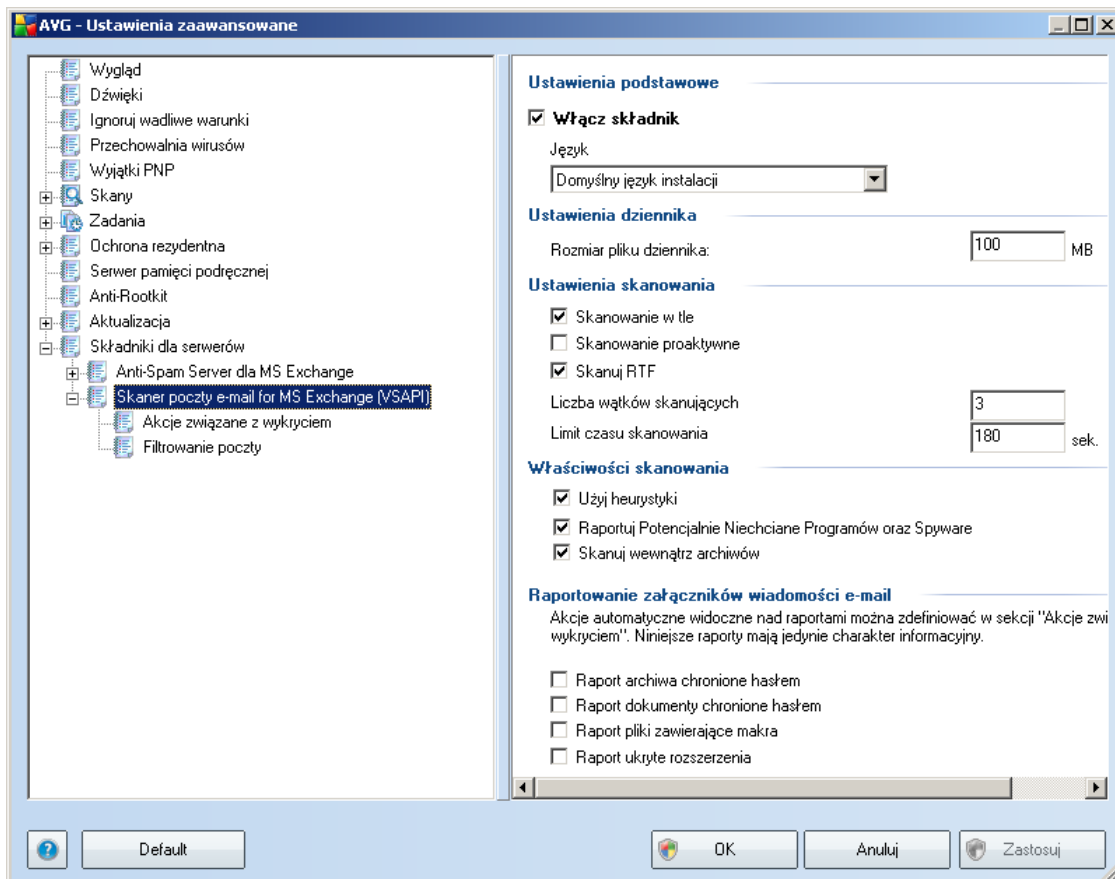
5.2. VSAPI 2.0

Interfejs wyszukiwania wirusów **VSAPI 2.0** (w serwerze Exchange 2000 Server) nie pozwala na usunięcie zainfekowanych plików wiadomości e-mail. Ponieważ zainfekowany załącznik wiadomości e-mail nie może zostać usunięty, jego nazwa zostaje zmieniona: program AVG dla Exchange 2000/2003 Server dodaje do oryginalnej nazwy pliku rozszerzenie .virusinfo.txt. Treść pliku jest zastępowana komunikatem o wykrytym wirusie. Jeśli wirus został wykryty bezpośrednio w treści wiadomości, cała treść wiadomości jest zastępowana komunikatem o wykryciu wirusa.

Interfejs wyszukiwania wirusów **VSAPI 2.5** (w serwerze Exchange 2003) pozwala już na usuwanie zainfekowanych wiadomości. Te funkcje można ustawić w oknie konfiguracji programu AVG dla MS Exchange 2000/2003 Server.

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

Ta pozycja zawiera ustawienia **Skanera dokumentów 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 logowania:**

- **Rozmiar pliku dziennika** - wybierz preferowany rozmiar pliku dziennika. Wartość domyślna: 100 MB.

Sekcja **Ustawienia skanowania:**

- **Skanowanie w tle** - to pole wyboru umożliwia włączenie lub wyłączenie możliwości 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 2007 Server. Skanowanie i wyszukiwanie obiektów, które nie zostały jeszcze przeskanowane odbywa się równoległe.

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 zaządał 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.

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

Uwaga: 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.
- **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: $2 * \text{liczba procesorów} + 1$.

Minimalna liczba wątków jest obliczana według wzoru: $(\text{liczba procesorów} + 1) / 2$.

Maksymalna liczba wątków jest obliczana według wzoru: $(\text{liczba procesorów})$

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** - opcje te należy zaznaczyć, aby raportowana była obecność potencjalnie niechcianych programów i programów typu spyware.
- **Skanuj wewnątrz archiwów** - opcje te należy zaznaczyć, aby umożliwić skanerowi skanowanie również wewnątrz plików zarchiwizowanych (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, wszystkie te funkcje są rozszerzeniami usług interfejsu Microsoft VSAPI 2.0/2.5. Szczegółowe informacje na temat interfejsu VSAPI 2.0/2.5 można znaleźć, odwiedzając poniższe łącza (oraz łącza znajdujące na powiązanych stronach sieci Web):

- <http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP> - ogólne informacje o interfejsie VSAPI 2.0 w dodatku Service Pack 1 dla serwera Exchange 2000.
- <http://support.microsoft.com/default.aspx?scid=kb;pl-pl;328841&Product=exch2k>

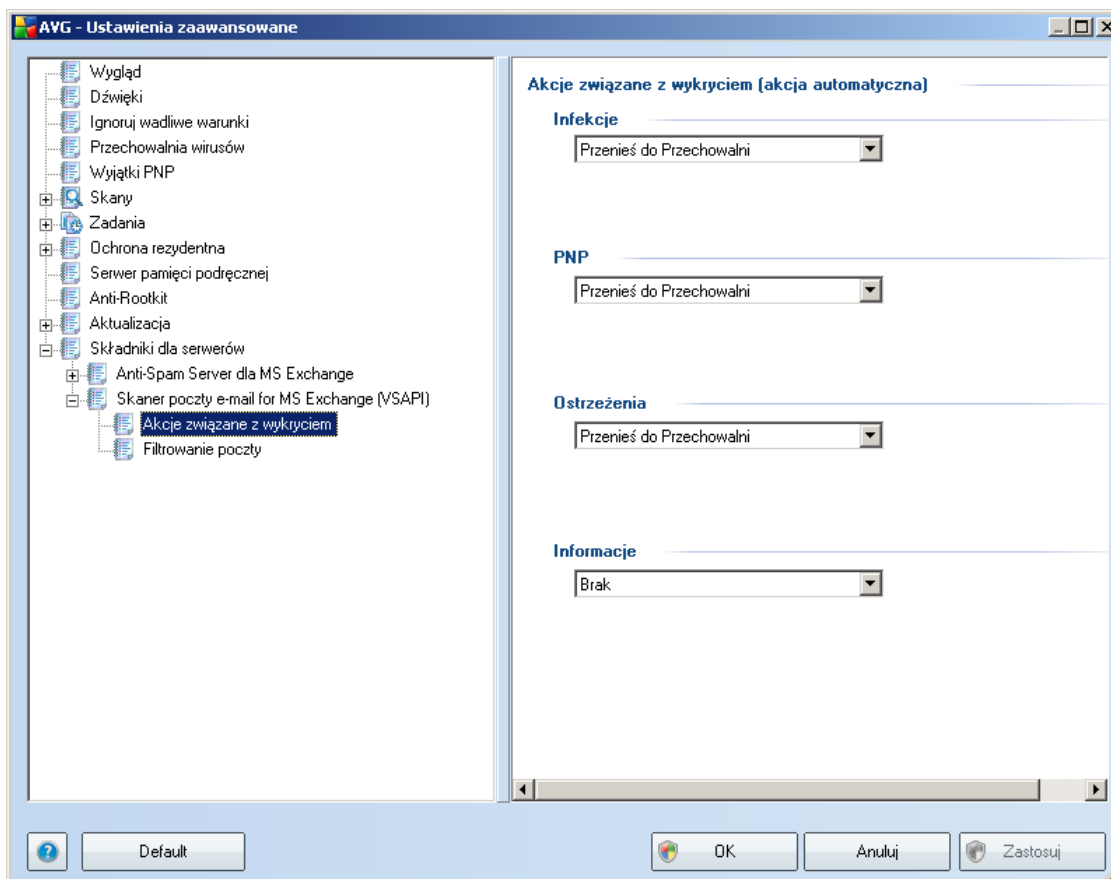
- informacje na temat współpracy serwera Exchange i oprogramowania antywirusowego.

- <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**](#)

5.4. Akcje związane z wykryciem



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

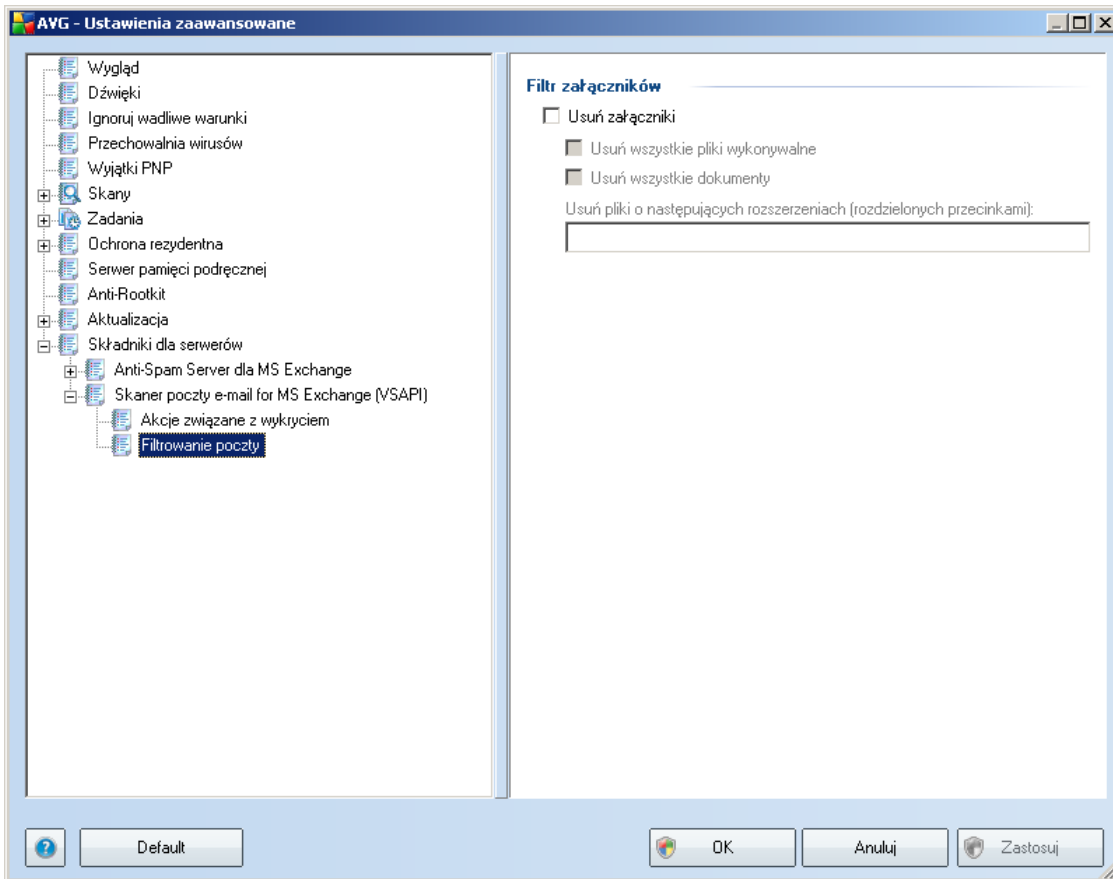
Akcje te są dostępne dla następujących pozycji:

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

Z menu rozwijanego można wybrać akcje dla każdej pozycji:

- **Brak** - nie zostanie podjęta żadna akcja.
- **Przenies do Przechowalni** - dane zagrożenie zostanie przeniesione do Przechowalni wirusów.
- **Usun** - dane zagrożenie zostanie usunięte.

5.5. Filtrowanie poczty



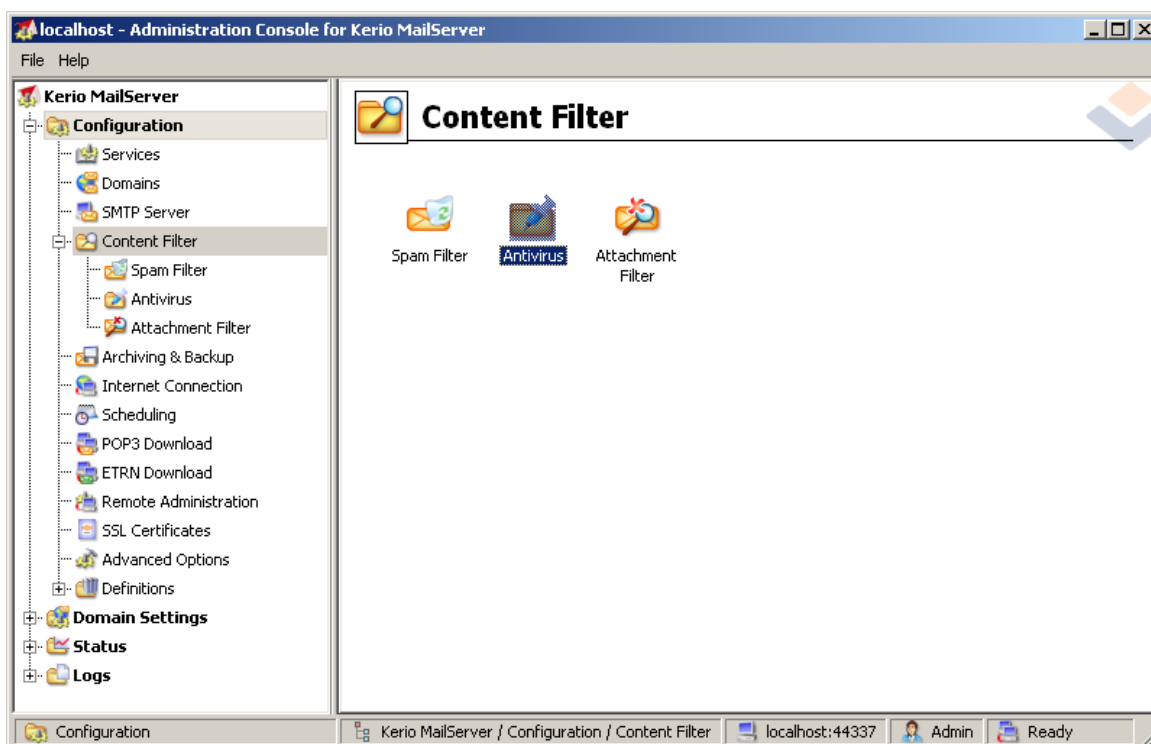
Pozycja **Filtrowanie poczty** umożliwia wybór załączników, które będą automatycznie usuwane (o ile ta funkcja ma być używana). Dostępne są następujące opcje:

- **Usuwać załączniki** - zaznacz to pole wyboru, aby włączyć te funkcje.
- **Usuń wszystkie pliki wykonywalne** - usuwa wszystkie pliki wykonywalne.
- **Usuń wszystkie dokumenty** - usuwa wszystkie pliki dokumentów.
- **Usuń pliki o następujących rozszerzeniach (rozdzielonych przecinkami)** - w tym polu należy wprowadzić rozszerzenia plików, które mają być automatycznie usuwane. Rozszerzenia należy rozdzielać 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 pomocą silnika skanującego AVG, należy uruchomić aplikację Kerio Administration Console. W drzewie nawigacji po lewej stronie okna należy wybrać gałąź Filtr zawartości (znajdująca się w gałęzi Konfiguracja):

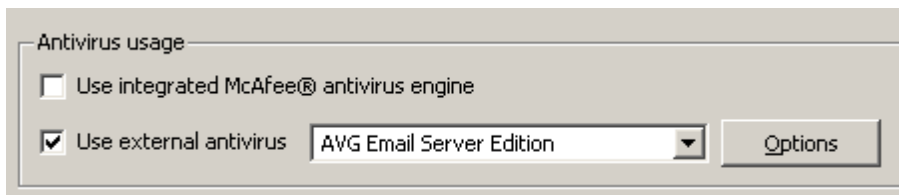


Kliknięcie pozycji Filtr zawartości wyświetli okno dialogowe zawierające trzy pozycje:

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

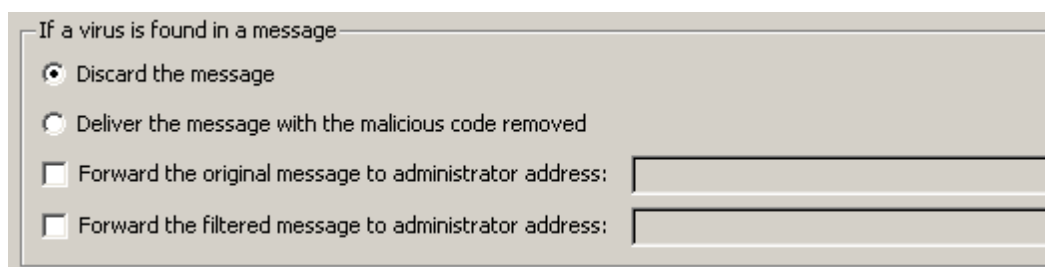
6.1.1. Ochrona antywirusowa

Aby aktywować program AVG dla Kerio MailServer, należy zaznaczyć pole wyboru Użyj 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**

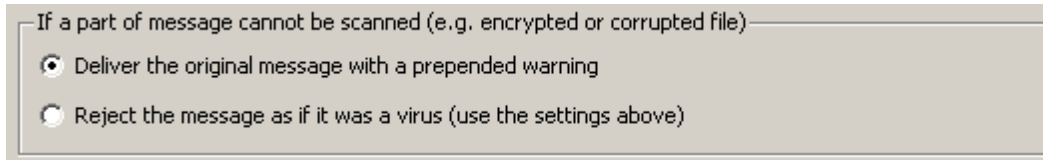


W tej ramce można określić akcje, które mają zostać wykonane w przypadku wykrycia wirusa w wiadomości lub wyfiltrowania wiadomości z załącznikiem na podstawie ustawień filtra załączników:

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

filtrowania będzie przekazywana na adres określony w polu tekstowym.

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



If a part of message cannot be scanned (e.g. encrypted or corrupted file)

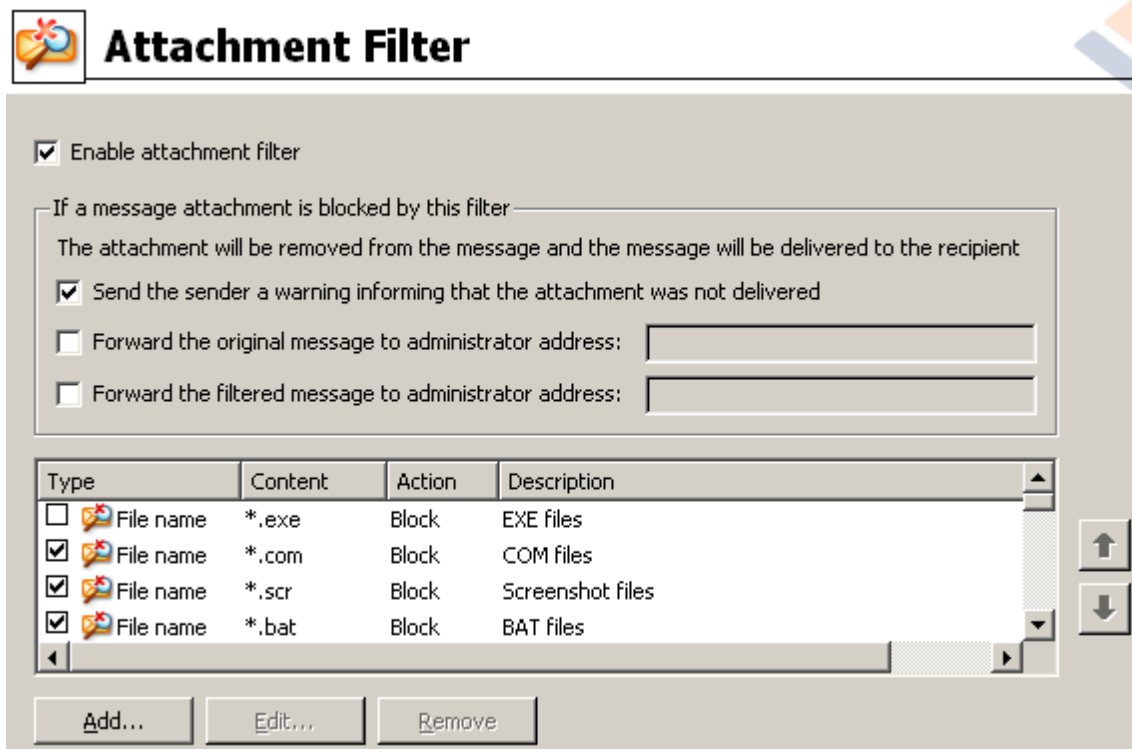
- Deliver the original message with a prepended warning
- Reject the message as if it was a virus (use the settings above)

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.
- ***Odrzuc 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.

6.1.2. 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 spełniająca kryteria filtrowania na adres**

administratora

Wiadomość bez zainfekowanego lub niedozwolonego załącznika zostanie (niezależnie od innych podjętych akcji) przekazana na określony adres e-mail. Te funkcje można wykorzystać do sprawdzenia poprawności działania mechanizmu antywirusowego lub filtra 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 te pozycje 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 Blokuje (ta akcja zostanie wykonana zgodnie z ustawieniami znajdującymi się powyżej listy wykluczonych załączników).
- **Opis** - w tym polu należy wprowadzić opis załącznika.

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

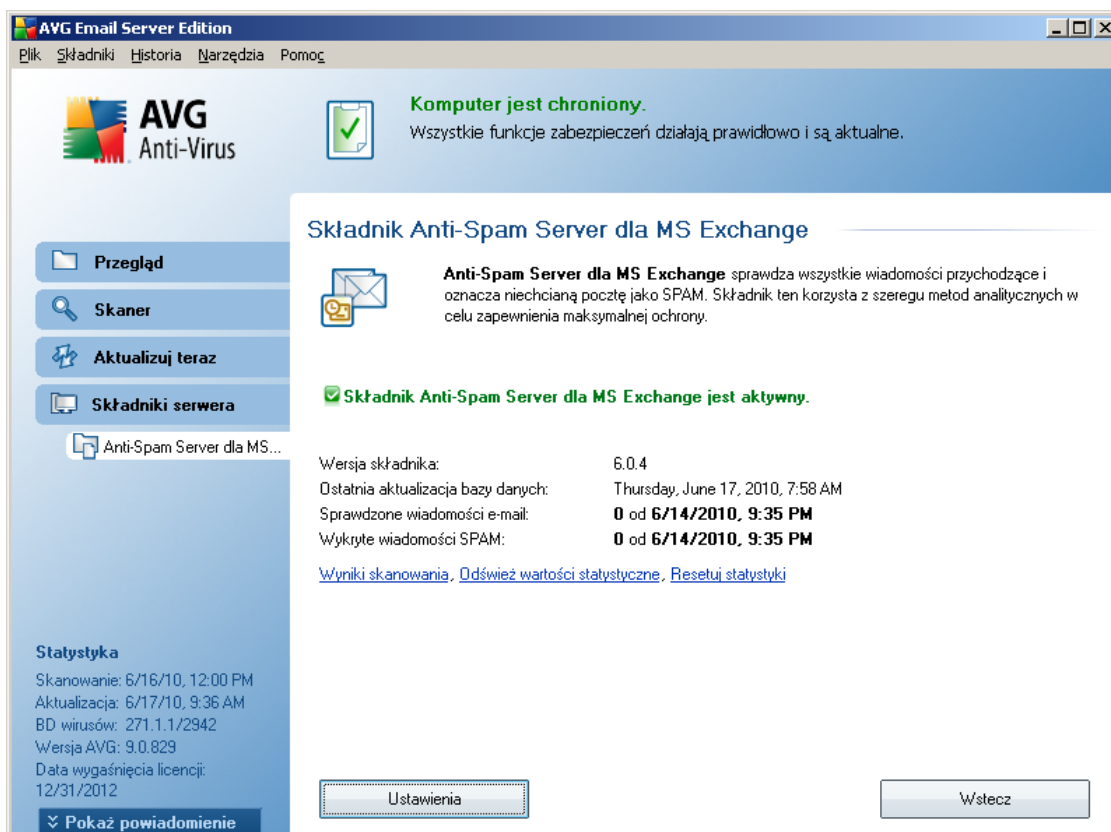


- W polu Opis można wpisać krótki opis załącznika, który ma być filtrowany.
- W polu Jeśli wiadomość e-mail zawiera załącznik można wybrać typ załącznika (Nazwa pliku lub Typ MIME). Dodatkowo można wybrać konkretne rozszerzenie z dostępnej listy lub użyć symboli wieloznacznych.

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

7. Konfiguracja Anti-Spam

7.1. Interfejs składowca Anti-Spam

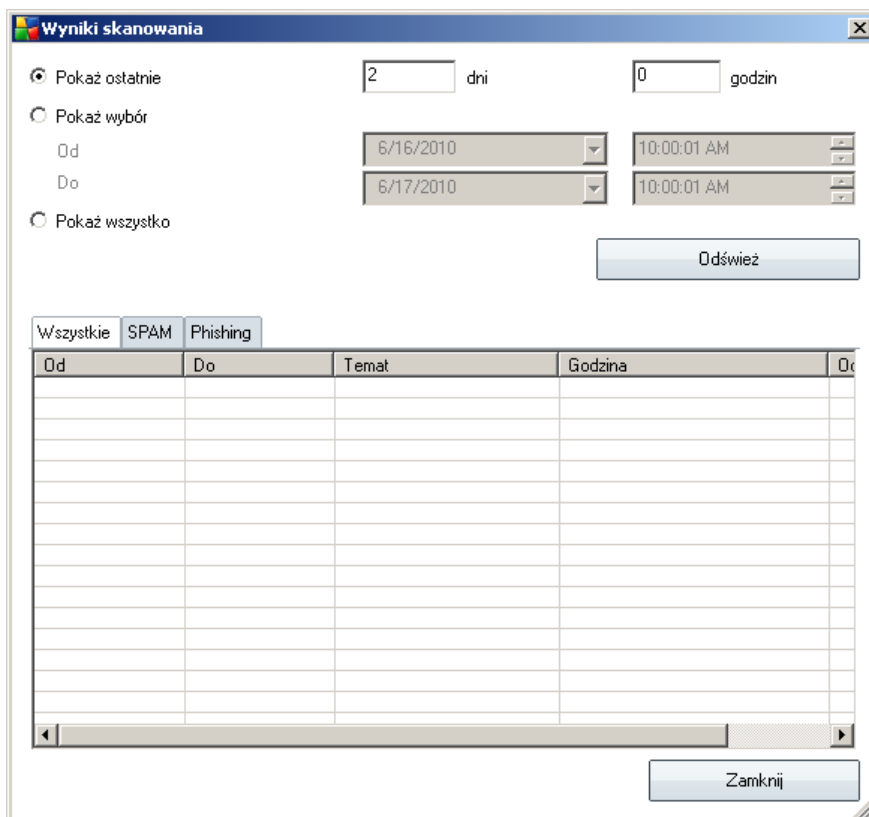


Okno dialogowe **składnika Anti-Spam** Servermożna znaleźć w sekcji **Składniki serwera** (menu po lewej stronie). Zawiera ono krótką informację o funkcjach składnika oraz podsumowanie jego bieżącego stanu (*Składnik Anti-Spam Server for MS Exchange jest aktywny.*), a także statystyki.

Dostępne linki:

- **Wyniki skanowania**

Otwiera nowe okno dialogowe, w którym dostępny jest przegląd wyników skanowania składnika Anti-Spam:



W tym miejscu można sprawdzić wiadomości wykryte jako SPAM (niepożądane) lub jako próba Phishingu (kradzieży danych osobowych, kont bankowych itp.). Domyslnie wyświetlane są tylko wyniki z ostatnich dwóch dni. Okres, dla którego wyniki są wyświetlane, można dostosować za pomocą następujących opcji:

- **Pokaż ostatnie** - wprowadź preferowaną ilość dni i godzin.
- **Pokaż wybrane** - wprowadź niestandardowy przedział czasu i daty.
- **Pokaż wszystko** - wyświetla wszystkie dostępne wyniki.

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

- **Odśwież wartości statystyczne** - aktualizuje powyższe statystyki.
- **Resetuj wartości statystyczne** - zeruje wszystkie statystyki.

Dostępne przyciski:

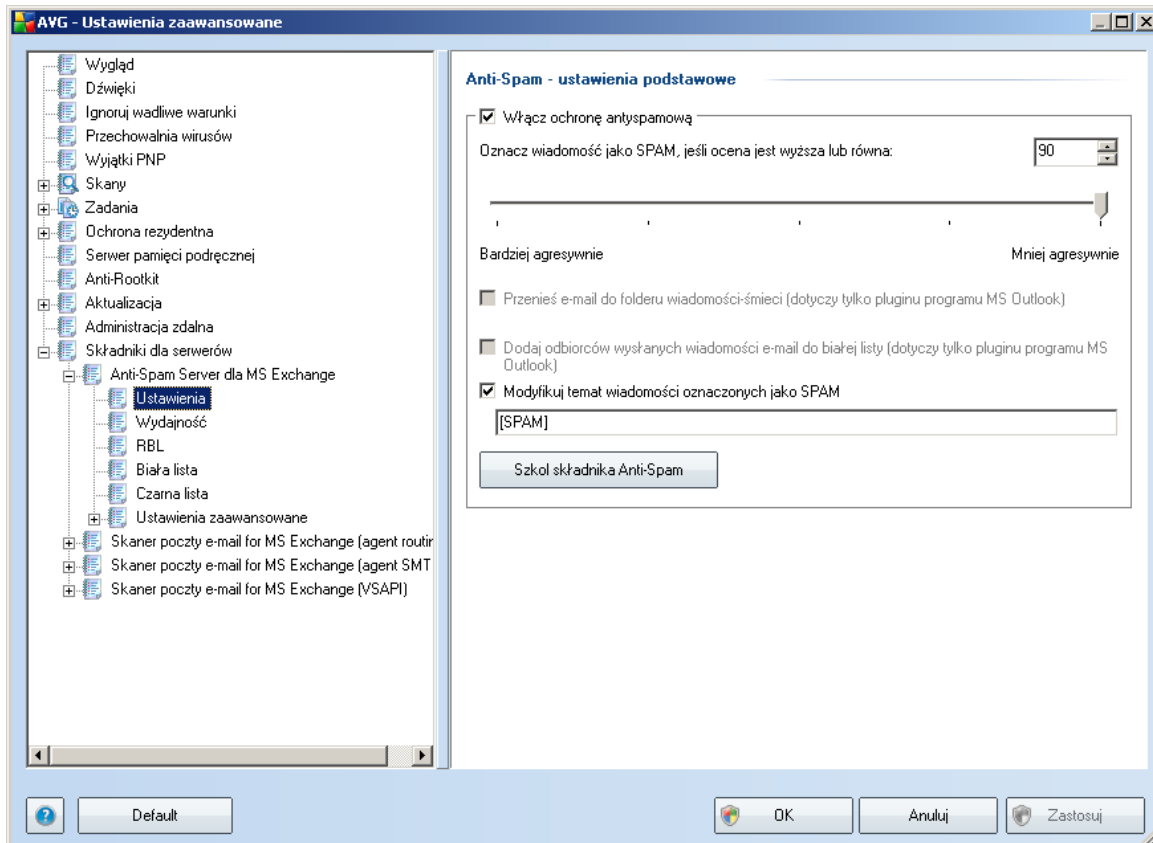
- **Ustawienia** - ten przycisk powoduje otwarcie okna [Ustawienia składowika Anti-Spam](#).
- **Wstecz** - ten przycisk umożliwia powrót do okna Przegląd składowików serwera.

7.2. Zasady działania składowika Anti-Spam

Mianem spamu określa się niechciana pocztę e-mail (głównie reklamy produktów lub usług, które są hurtowo rozsyłane do wielkiej liczby odbiorców jednocześnie, zapelniając ich skrzynki pocztowe). Spamerem 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.

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

7.3. Anti-Spam - Ustawienia



W oknie dialogowym **Podstawowe ustawienia składnika Anti-Spam** 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. *wskaznik informujący, jak bardzo jej treść przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. Wartość opcji **Oznacz wiadomość jako spam, jeśli ocena jest wyższa niż lub równa** można dostosować, wpisując odpowiednią liczbę (od 0 do 100) bądź przesuwając suwak w lewo lub w prawo (tylko od 50 do 90).

Zwykle zaleca się stosowanie progów z przedziału od 50 do 90, a jeśli nie ma pewności co do właściwego ustawienia - równego 90. Poniżej przedstawiono opis progów oceny:

- **Wartosc 90–99** - 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 trafiać do Twojej skrzynki odbiorczej.
- **Wartosc 80–89** - wiadomosci e-mail, które stanowią potencjalny [spam](#), są poprawnie odfiltrowywane. Niektóre z pozadanych wiadomosci (niebedacych spamem) mogą zostać błędnie zablokowane.
- **Wartosc 60–79** - umiarkowanie agresywna konfiguracja. Wiadomosci e-mail, które mogą stanowić [spam](#), są poprawnie odfiltrowywane. Pozadane wiadomosci (niebedace spamem) mogą zostać błędnie zablokowane.
- **Wartosc 1–59** - bardzo agresywna konfiguracja. Pozadane wiadomosci e-mail są odfiltrowywane w równym stopniu, jak wiadomosci stanowiące [spam](#). Nie zalecamy stosowania tego progu podczas normalnej pracy.
- **Wartosc 0** - w tym trybie dostarczane są tylko wiadomosci od nadawców z [bialej listy](#). Wszystkie pozostałe wiadomosci e-mail są uznawane za [spam](#). **Nie zalecamy stosowania tego progu podczas normalnej pracy.**

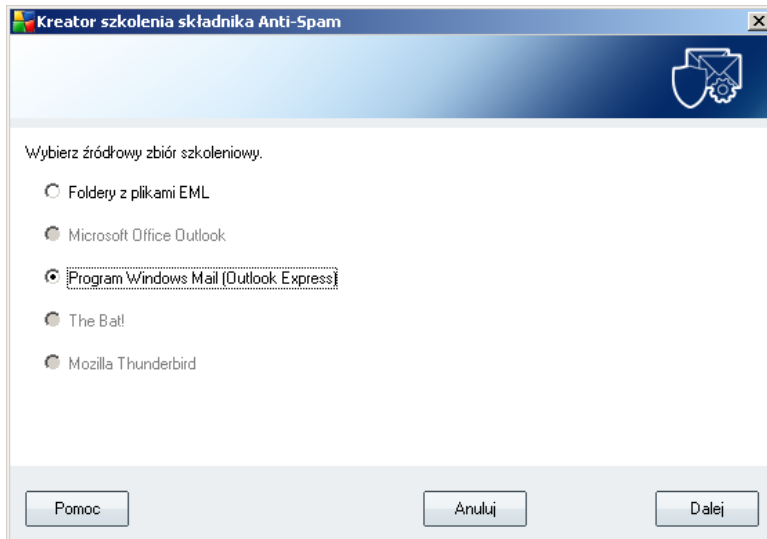
Następnie można zdefiniować, jakie akcje mają zostać podjęte wobec wiadomosci e-mail wykrytych jako [spam](#):

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

Przycisk **Rozpocznij szkolenie składnika Anti-Spam** pozwala uruchomić [Kreator szkolenia składnika Anti-Spam](#) opisany szczegółowo w [następnym rozdziale](#).

7.3.1. Kreator szkolenia składnika Anti-Spam

W pierwszym oknie dialogowym **kreatora szkolenia składnika Anti-Spam** należy wybrać źródło wiadomosci e-mail, które zostaną użyte do szkolenia. Na ogół używa się do tego celu niechcianych wiadomosci reklamowych, oraz e-maili błędnie oznaczonych jako spam.



Dostępne są następujące opcje:

- **Konkretny klient poczty e-mail** - jeśli używasz jednego z wymienionych klientów poczty e-mail (*MS Outlook, Outlook Express, The Bat!, Mozilla Thunderbird*), po prostu wskaz go na wyświetlonej liście.
- **Folder z plikami EML** - jeśli jest używany jakikolwiek inny program pocztowy, należy zgromadzić wszystkie wiadomości w jednym folderze (w formacie *.eml*). Możesz skorzystać z tego, że wiele klientów poczty domyślnie przechowuje pliki *.eml* w określonym folderze na dysku. Następnie należy zaznaczyć opcję **Folder z plikami EML**, oraz wskazać odpowiedni folder w następnym kroku.

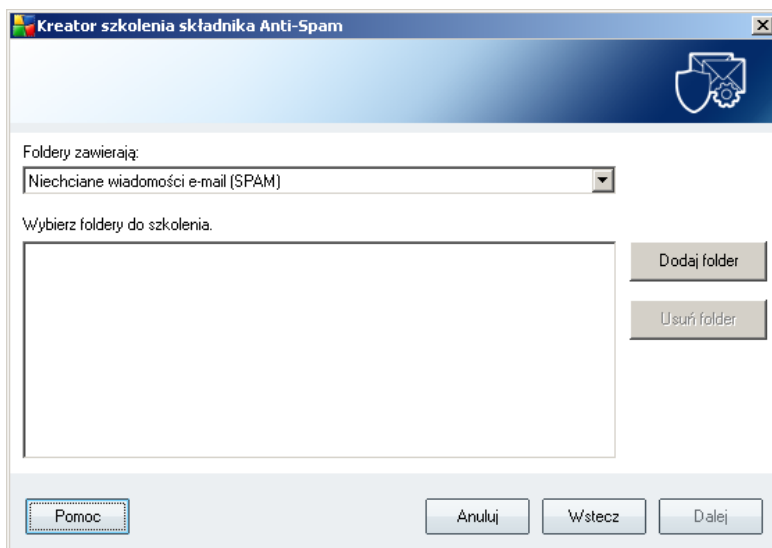
Aby proces szkolenia był prostszy i przebiegał szybciej, warto już wcześniej tak posortować e-maile, aby folder używany w szkoleniu zawierał jedynie wiadomości szkoleniowe (albo spam, albo ham). Nie jest to jednak konieczne, gdyż wiadomości można przefiltrować ręcznie w późniejszym czasie.

Aby kontynuować, zaznacz odpowiednią opcję i kliknij przycisk **Dalej**.

7.3.2. Wybierz folder z wiadomościami

Okno wyświetlane w tym kroku zależy od poprzedniego wyboru.

Foldery z plikami EML



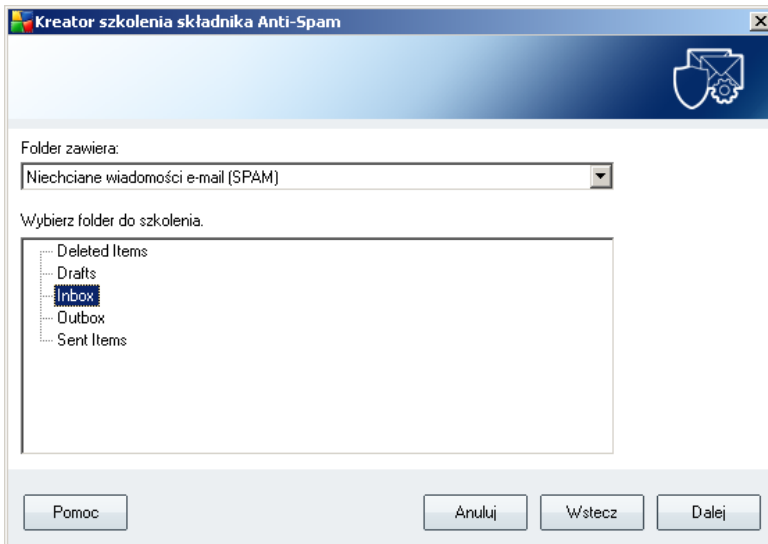
W oknie tym należy wybrać folder z wiadomościami, które mają zostać użyte do szkolenia. Kliknij przycisk **Dodaj folder**, aby zlokalizować folder z plikami .eml (zapisanymi wiadomościami e-mail). Wybrany folder zostanie wyświetlony w bieżącym oknie.

Z menu rozwijanego **Foldery zawierają** wybierz jedną z dwóch opcji - czy folder zawiera pożądane wiadomości (HAM), czy niechciane reklamy (SPAM). Należy pamiętać, że w następnym kroku będzie możliwa szczegółowa selekcja plików, więc folder nie musi zawierać tylko szkoleniowych wiadomości e-mail. Można też usunąć z listy niechciane foldery, klikając przycisk **Usuń folder**.

Po zakończeniu ustawień należy kliknąć przycisk **Dalej** i przejść do [Opcji filtrowania wiadomości](#).

Określony klient poczty e-mail

Po potwierdzeniu jednej z opcji pojawi się nowe okno dialogowe.

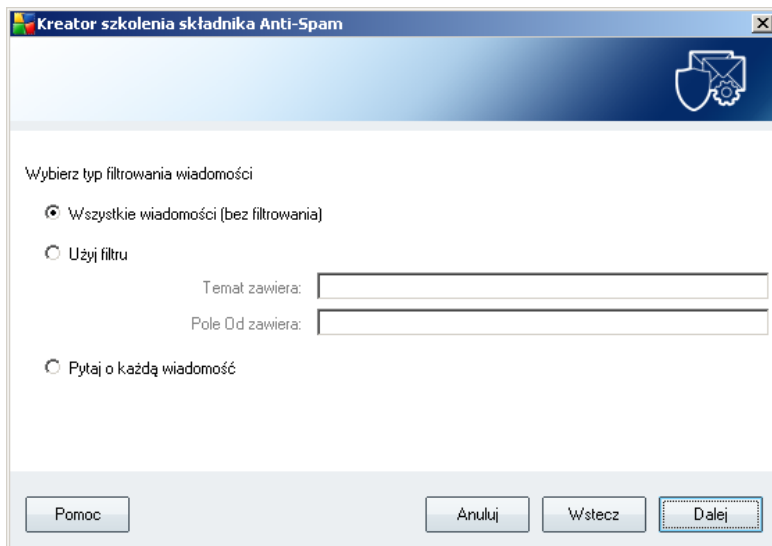


Uwaga: W wypadku programu Microsoft Office Outlook pojawi się najpierw monit proszący o wybranie profilu programu MS Office Outlook.

Z menu rozwijanego **Foldery zawierają** wybierz jedną z dwóch opcji - czy folder zawiera pożądane wiadomości (*HAM*), czy niechciane reklamy (*SPAM*). Należy pamiętać, że w następnym kroku będzie możliwa szczegółowa selekcja plików, więc folder nie musi zawierać tylko szkoleniowych wiadomości e-mail. W głównej części okna pojawi się drzewo nawigacyjne wybranego klienta poczty e-mail. Zlokalizuj zadany folder i podświetl go za pomocą myszy.

Po zakończeniu ustawień należy kliknąć przycisk **Dalej** i przejść do [Opcji filtrowania wiadomości](#).

7.3.3. Opcje filtrowania wiadomosci



W tym oknie można ustawić filtrowanie wiadomości e-mail.

Jeśli wybrany folder na pewno zawiera tylko wiadomości, które mają zostać użyte do szkolenia, należy wybrać opcję **Wszystkie wiadomości (bez filtrowania)**.

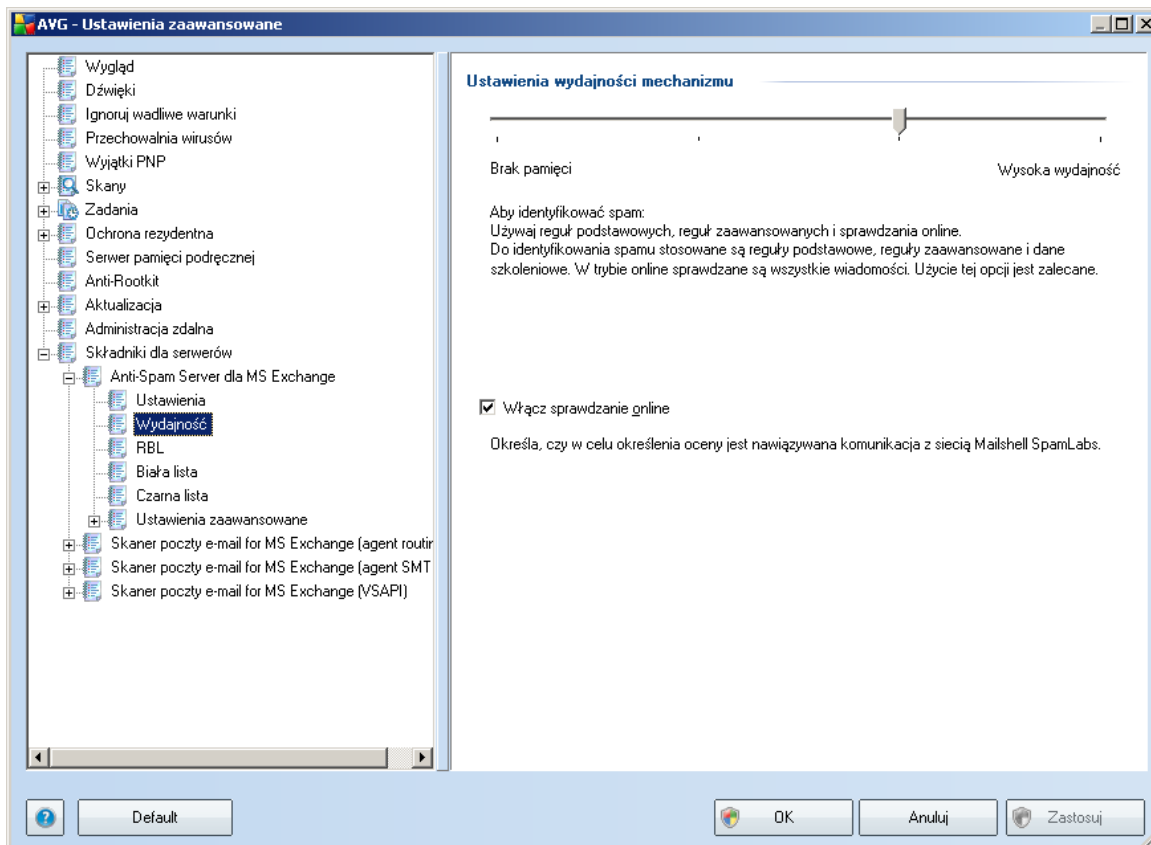
Jeśli nie ma pewności co do wiadomości znajdujących się w folderze, a Kreator ma pytać o każdą z nich oddzielnie (dając możliwość określenia, czy ma ona zostać użyta do szkolenia), należy wybrać opcję **Pytaj o każdą wiadomość**.

Aby zastosować bardziej zaawansowane filtrowanie, należy wybrać opcję **Użyj filtru**. Można będzie wówczas podać wyraz (*nazwę*), część wyrazu lub frazę, która ma być wyszukiwana w tematach i/lub adresach nadawców wiadomości. Wszystkie wiadomości dokładnie spełniające kryteria wyszukiwania zostaną użyte do szkolenia, bez dalszych monitorów.

Uwaga: W przypadku wypełnienia obu pól tekstowych zostaną użyte także adresy spełniające tylko jeden z dwóch warunków!

Gdy już zdecydujesz się na jedną z opcji, kliknij przycisk **Dalej**. Kolejne okno dialogowe ma charakter informacyjny i sygnalizuje, że kreator jest gotowy do przetwarzania wiadomości. Aby rozpocząć szkolenie, należy ponownie kliknąć przycisk **Dalej**. Szkolenie rozpocznie się zgodnie z wybranymi wcześniej parametrami.

7.4. Wydajność



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

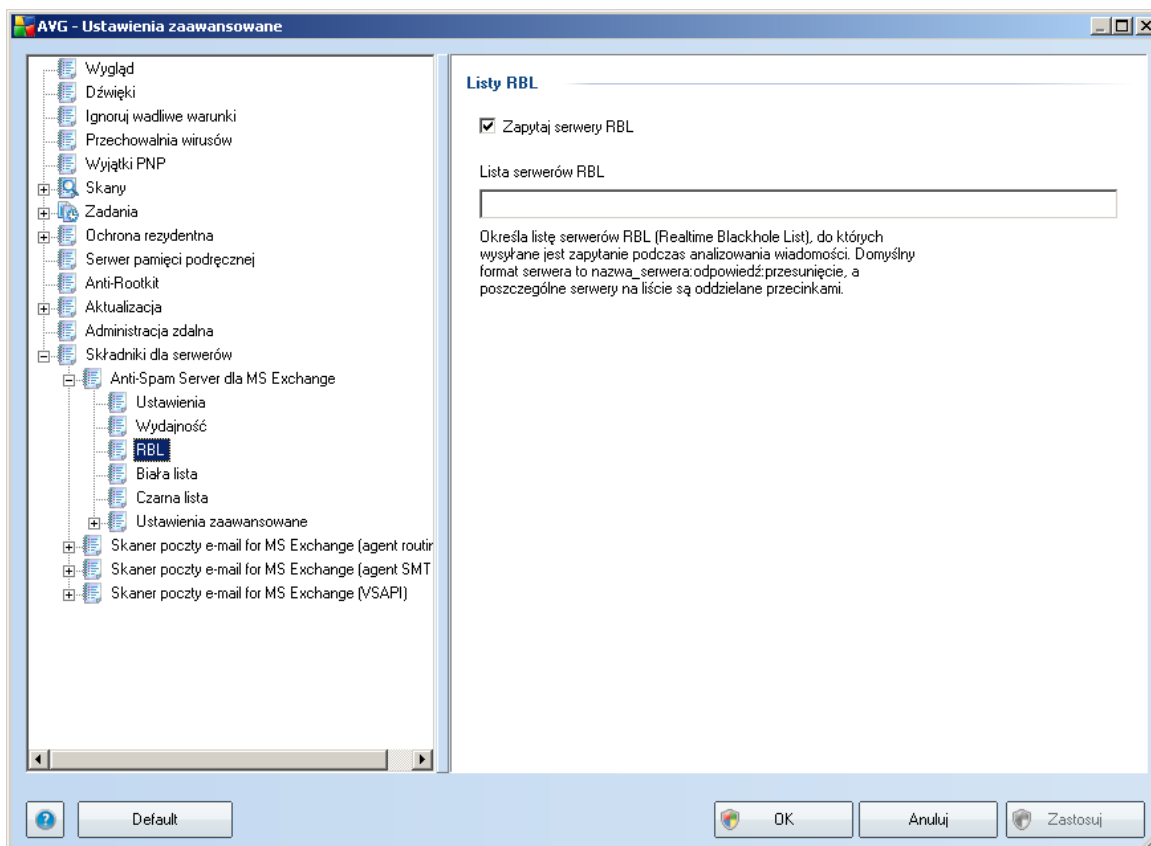
- **Brak pamięci** - w czasie skanowania w poszukiwaniu [spamu](#) nie będą stosowane żadne reguły. Do identyfikacji będą używane tylko dane szkoleniowe. Ten tryb nie jest zalecany do częstego stosowania - chyba że konfiguracja sprzętowa komputera jest bardzo słaba.
- **Wysoka wydajność** - wymaga dużej 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 spamersów i inne bazy danych.

Opcja **Włącz sprawdzanie online** jest domyślnie włączona. Pozwala ona skuteczniej wykrywać spam dzięki komunikacji 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!

7.5. RBL

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



W oknie tym można włączyć/wyłączyć funkcję **Zapytaj serwery RBL**.

Serwer RBL (*Realtime Blackhole List*) to specjalny serwer DNS z obszerną bazą danych znanych nadawców spamu. Jeżeli funkcja ta jest włączona, wszystkie wiadomości e-

mail zostaną sprawdzone przy użyciu bazy serwera RBL i oznaczone jako [spam](#), w przypadku gdy okaza się identyczne z którymkolwiek wzorem w bazie danych.

Bazy danych serwerów RBL zawierają zawsze aktualne sygnatury spamu, co zapewnia najskuteczniejsze i najdokładniejsze wykrywanie [niechcianych wiadomości](#). Funkcja ta jest szczególnie przydatna dla użytkowników otrzymujących duże ilości spamu, który zazwyczaj nie jest wykrywany przez silnik AVG Anti-Spam.

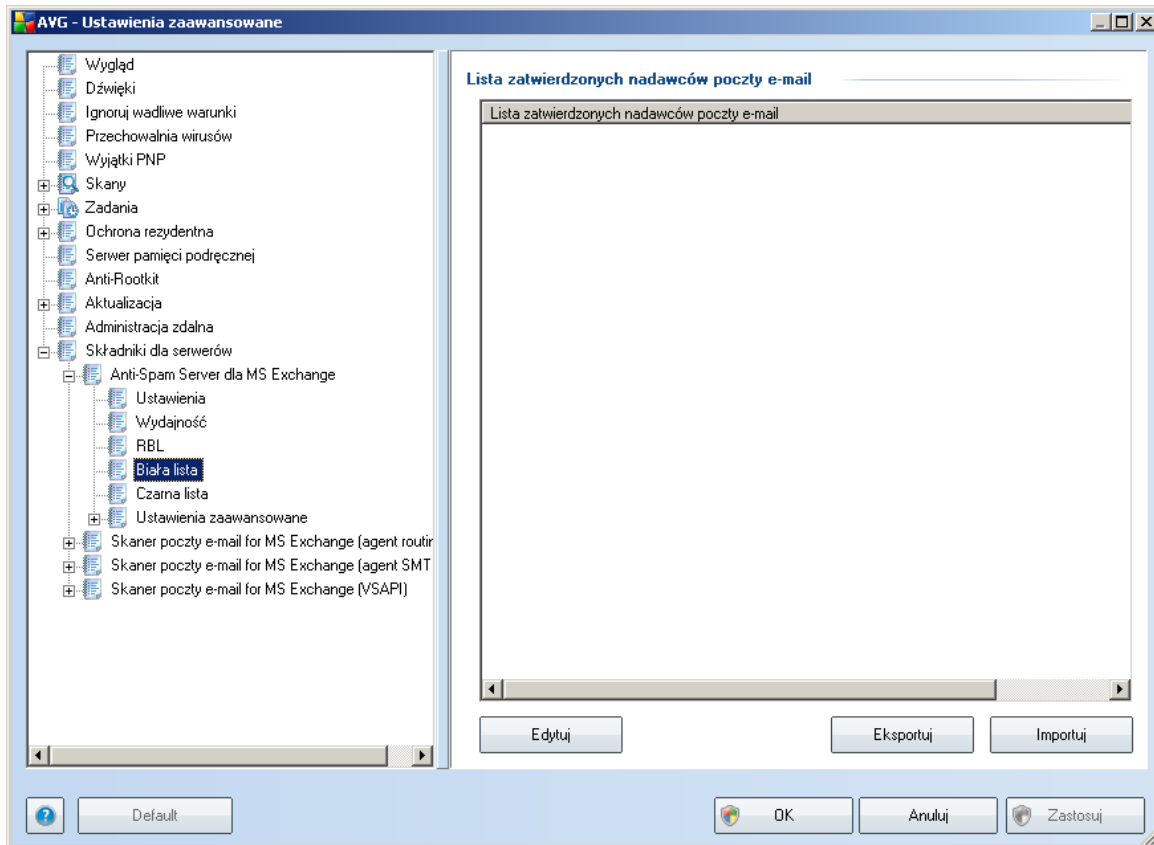
Lista serwerów RBL pozwala określić lokalizację wybranych serwerów RBL. Domyślnie zdefiniowane są tam dwa serwery RBL. Zmiany ustawień domyślnych powinny być dokonywane tylko przez doświadczonych użytkowników i wyłącznie w przypadkach, gdy jest to absolutnie niezbędne!

Uwaga: Włączenie tej funkcji może w niektórych systemach i konfiguracjach spowolnić proces odbierania poczty e-mail, ponieważ każda wiadomość musi być zweryfikowana przy użyciu bazy danych serwera RBL.

Do serwera nie są wysyłane żadne dane osobiste!

7.6. Biała lista

Kliknięcie pozycji **Biała lista** pozwala otworzyć globalną listę zablokowanych adresów indywidualnych nadawców i domen, z których 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.

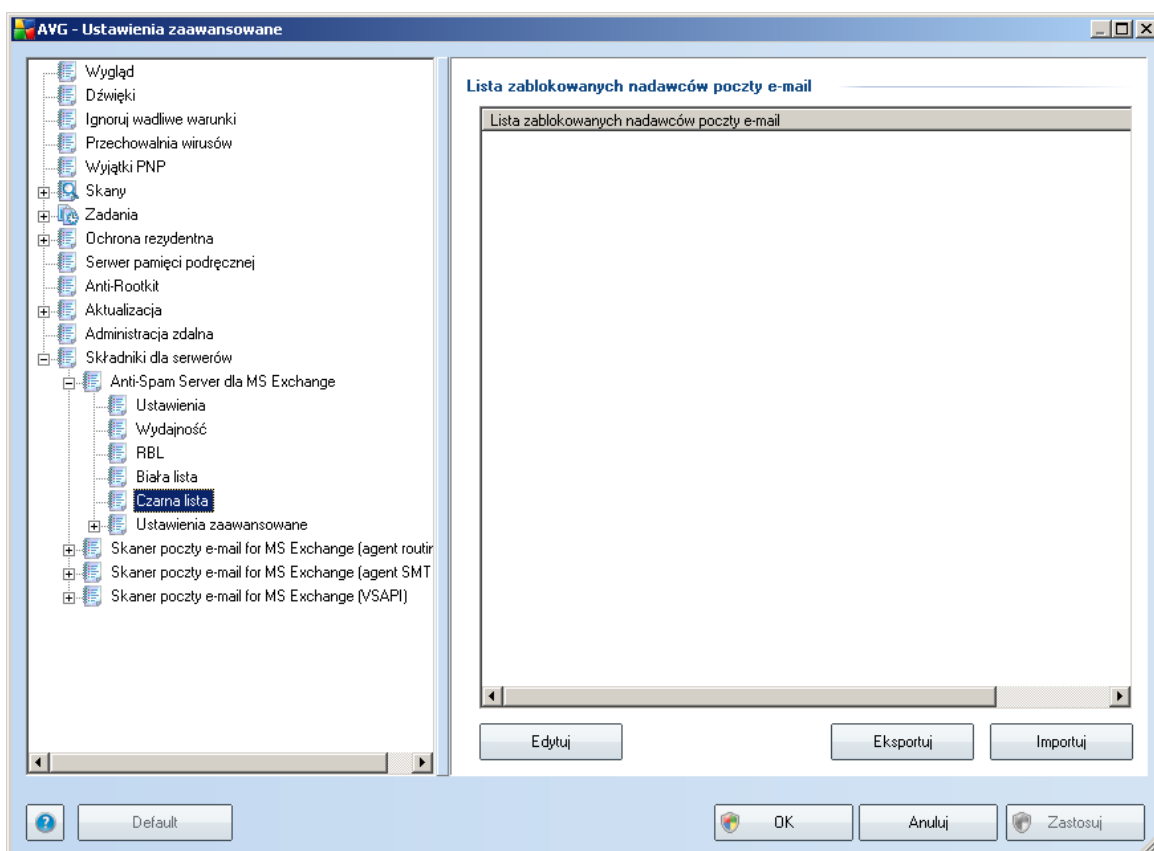
Po przygotowaniu listy adresów i domen, jej elementy można wprowadzić pojedynczo lub zaimportować wszystkie na raz. Dostępne są następujące przyciski kontrolne:

- **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** - jeżeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, można go zaimportować za pomocą tego przycisku. Wprowadzany plik musi być w zwykłym formacie tekstowym i zawierać każdy element (adres lub nazwę domeny) w osobnym wierszu.

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

7.7. Czarna lista

Kliknięcie pozycji **Czarna lista** pozwala otworzyć globalną listę zablokowanych adresów indywidualnych nadawców i 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 otrzymać) spam. Wszystkie wiadomości e-mail wysłane z tych adresów/domen będą identyfikowane jako spam.

Po przygotowaniu listy adresów i domen, jej elementy można wprowadzić pojedynczo

lub zaimportować 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). Każda pozycja (nadawca lub nazwa domeny) należy wprowadzić w osobnym wierszu.
- **Importuj** - jeżeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, można go zaimportować za pomocą tego przycisku. Wprowadzany plik musi być w zwykłym formacie tekstowym i zawierać każdy element (adres lub nazwę domeny) w osobnym wierszu.
- **Eksportuj** - jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zostaną zapisane w zwykłym pliku tekstowym.

7.8. Ustawienia zaawansowane

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

Aby mimo wszystko zmienić konfigurację składnika Anti-Spam na bardzo zaawansowanym poziomie, 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:

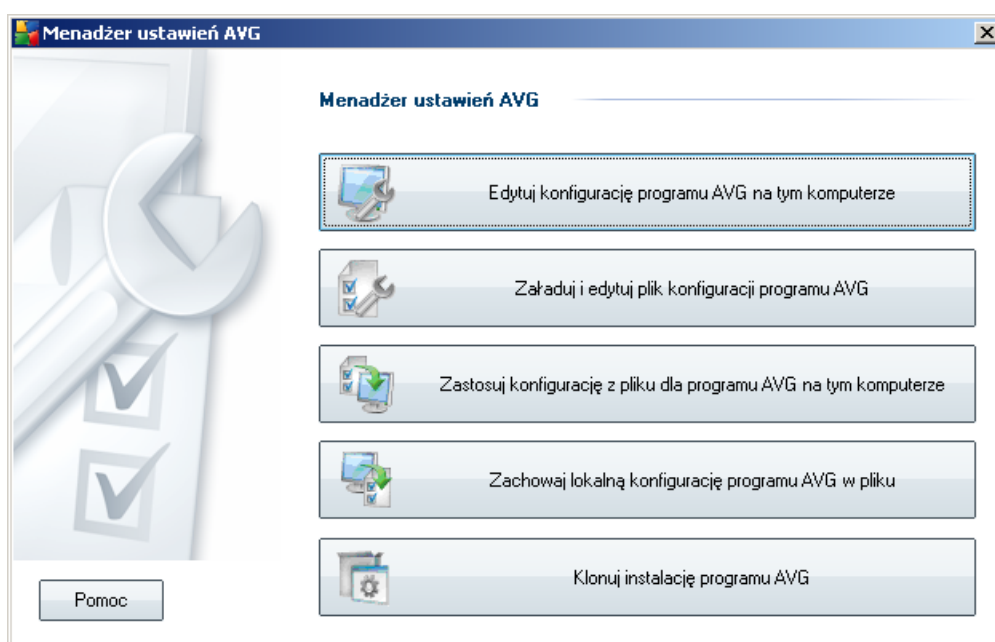
- **Pamięć podrečna** - sygnatury, reputacja domen, LegitRepute
- **Szkolenie** - maksymalna liczba wpisów słów, próg automatycznego szkolenia, waga
- **Filtry** - lista języków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, fałszywi nadawcy
- **RBL** - serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba adresów IP
- **Połączenie internetowe** - limit czasu, serwer proxy, uwierzytelnianie na serwerze proxy

8. Menedżer ustawień systemu AVG

Menedżer ustawień systemu AVG to narzędzie odpowiednie przede wszystkim dla mniejszych sieci, pozwalające na kopiowanie, edycje i dystrybucje konfiguracji systemu AVG. Konfiguracja może zostać zapisana na urządzeniu przenośnym (dysk USB itp.), a następnie ręcznie zastosowana na wybranej stacji roboczej.

Narzędzie to jest elementem instalacji systemu AVG i można uzyskać do niego dostęp z menu Start systemu Windows:

Wszystkie programy/AVG 9.0/Menedżer ustawień systemu AVG



- **Edytuj konfigurację 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 zostaną uwzględnione w lokalnej instalacji systemu AVG.

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

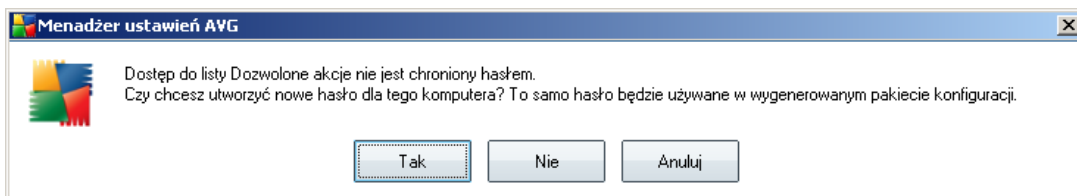
Jeśli plik konfiguracyjny systemu AVG (.pck) już istnieje, można go otworzyć do edycji za pomocą tego przycisku. Po zatwierdzeniu zmian przyciskiem **OK** lub **Zastosuj** plik zostanie zastąpiony nowymi ustawieniami!

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

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

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

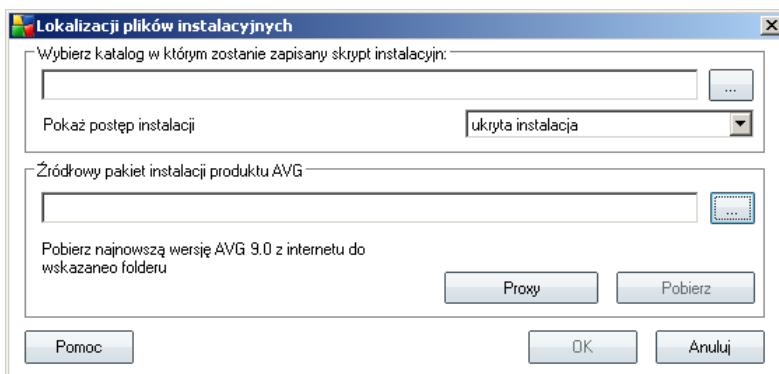
Ten przycisk pozwala zapisać plik konfiguracyjny (.pck) lokalnej instalacji systemu AVG. Jeśli dla dozwolonych akcji nie zostało ustawione hasło, może zostać wyświetlone następujące okno dialogowe:



Kliknij odpowiedź **Tak**, jeśli dostęp do dozwolonych pozycji ma być chroniony hasłem, a następnie wprowadź wymagane informacje i zatwierdź swój wybór. Kliknij odpowiedź **Nie**, aby pominąć tworzenie hasła i kontynuować zapisywanie konfiguracji lokalnej instalacji systemu AVG w pliku.

- **Klonuj instalację systemu AVG**

Ta opcja pozwala wykonać dokładną kopię lokalnej instalacji systemu AVG dzięki utworzeniu pakietu instalacyjnego o niestandardowych parametrach. Aby kontynuować, należy wybrać folder, w którym ma zostać zapisany skrypt.



Następnie z menu rozwijanego należy wybrać jedną z następujących opcji:

- **Instalacja ukryta** - podczas procesu instalacji nie będą wyświetlane żadne informacje.
- **Wyswietlaj tylko postęp instalacji** - instalacja nie będzie wymagała żadnej interakcji ze strony użytkownika, ale jej postęp będzie w pełni widoczny.
- **Pokaz kreatora instalacji** - instalacja będzie widoczna, a użytkownik będzie musiał ręcznie potwierdzać wszystkie kroki.

Aby pobrać najnowszy pakiet instalacyjny systemu AVG bezpośrednio ze strony AVG do wybranego folderu, należy kliknąć przycisk **Pobierz**. Możliwe jest też ręczne umieszczenie pakietu instalacyjnego systemu AVG w tym folderze.

Za pomocą przycisku **Proxy** można zdefiniować ustawienia serwera proxy, jeśli sieć wymaga tego do pomyślnego nawiązania połączenia.

Po kliknięciu przycisku **OK** rozpoczety zostanie krótkotrwały proces klonowania. Może się zdarzyć, że zostanie wyświetlone okno dialogowe z prośbą o ustawienie hasła dla dozwolonych pozycji (patrz wyżej). Po zakończeniu procesu, w wybranym folderze powinien zostać utworzony plik **AvgSetup.bat**. Po uruchomieniu pliku **AvgSetup.bat**, system AVG zostanie zainstalowany zgodnie z parametrami wybranymi powyżej.



9. 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>.

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**.