



AVG Email Server Edition 2012

Podręcznik użytkownika

Wersja dokumentu 2012.04 (1/4/2012)

Copyright AVG Technologies CZ, s.r.o. Wszelkie prawa zastrzeżone.
Wszystkie pozostałe znaki towarowe są własnością ich właścicieli.

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

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

W produkcji zastosowano bibliotekę 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 Deinstalacja poprzednich wersji	5
2.5 Dodatki Service Pack dla MS Exchange	6
3. Proces instalacji systemu AVG	7
3.1 Uruchamianie instalacji	7
3.2 Aktywacja licencji	8
3.3 Wybór typu instalacji	9
3.4 Instalacja niestandardowa — opcje niestandardowe	10
3.5 Ukończenie instalacji	12
4. Skaner poczty e-mail dla MS Exchange Server 2007/2010	13
4.1 Przegląd	13
4.2 Skaner poczty e-mail dla MS Exchange (routing TA)	16
4.3 Skaner poczty e-mail dla MS Exchange (SMTP TA)	17
4.4 Skaner poczty e-mail dla MS Exchange (VSAPI)	18
4.5 Uwaga techniczna	20
4.6 Akcje związane z wykryciem	21
4.7 Filtrowanie poczty	23
5. Skaner poczty e-mail dla MS Exchange Server 2003	24
5.1 Przegląd	24
5.2 Skaner poczty e-mail dla MS Exchange (VSAPI)	27
5.3 Akcje związane z wykryciem	30
5.4 Filtrowanie poczty	31
6. AVG dla Kerio MailServer	32
6.1 Konfiguracja	32
6.1.1 Ochrona antywirusowa	32
6.1.2 Filtr załączników	32
7. Konfiguracja składnika Anti-Spam	36



7.1 Interfejs składowika Anti-Spam	36
7.2 Zasady działania składowika Anti-Spam	38
7.3 Ustawienia składowika Anti-Spam	38
7.3.1 Kreator szkolenia składowika Anti-Spam	38
7.3.2 Wybierz folder z wiadomościami	38
7.3.3 Opcje filtrowania wiadomości	38
7.4 Wydajność	43
7.5 RBL	44
7.6 Biała lista	45
7.7 Czarna lista	46
7.8 Ustawienia zaawansowane	47
8. Menedżer ustawień AVG	48
9. FAQ i pomoc techniczna	51



1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację systemu **AVG Email Server Edition 2012**.

Gratulujemy zakupu systemu AVG Email Server Edition 2012!

System **AVG Email Server Edition 2012** 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 2012** 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 Email Server Edition 2012 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

2.2. Obsługiwane serwery poczty e-mail

Obsługiwane są następujące serwery poczty e-mail:

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

2.3. Minimalne wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG Email Server Edition 2012**:

- 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 2012**:

- 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 2012** 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 Usuń 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 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/exchange/evaluation/sp2/overview.mspx>

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

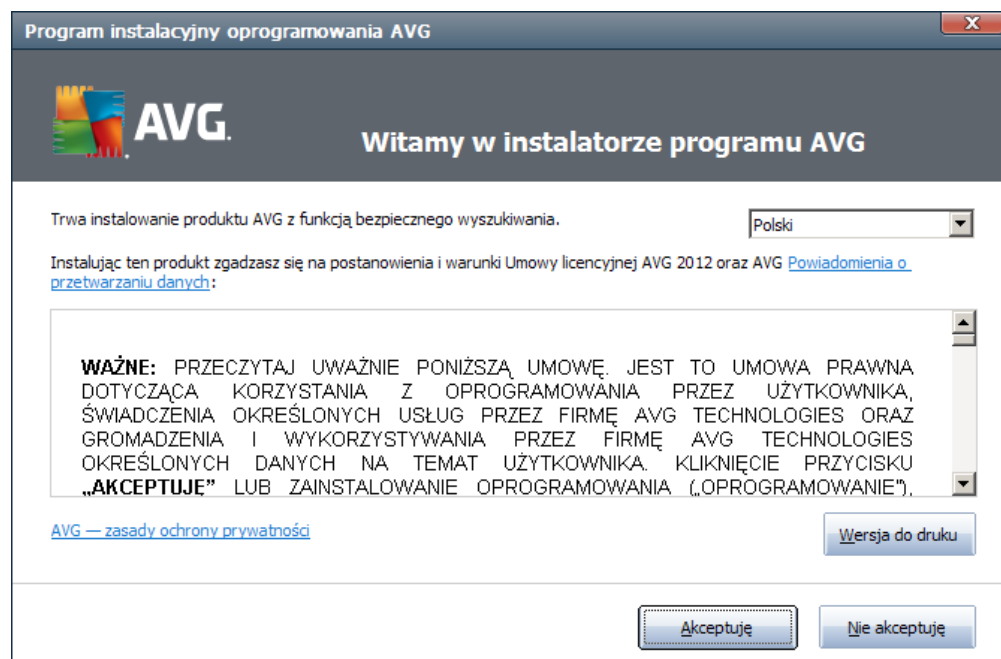
Aby zainstalować na komputerze program AVG, należy najpierw zdobyć najnowszy instalator. Można znaleźć go na dysku CD będącym częścią dystrybucyjnej edycji programu — istnieje jednak ryzyko, że będzie on nieaktualny. Dlatego zaleca się pobranie najnowszego pliku instalacyjnego z internetu. Plik można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

Uwaga: 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**. Można w nim wybrać język używany podczas procesu instalacji i przeczytać warunki umowy. Aby wyświetlić treść umowy licencyjnej w nowym oknie, kliknij przycisk **Wersja do druku**. Kliknij przycisk **Akceptuję**, aby potwierdzić wybór i przejść do kolejnego ekranu.

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



3.2. 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 zakupie oprogramowania AVG poprzez internet. 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.

Program instalacyjny oprogramowania AVG

AVG. Aktywuj licencję

Numer licencji:

Przykład: IQNP6-9BCA8-PUQU2-A5HCK-GP338L-93OCB

Jeśli kupiłeś oprogramowanie AVG 2012 w internecie, numer licencji zostanie do Ciebie wysłany pocztą e-mail. Aby uniknąć błędów przy wpisywaniu numeru licencji, zalecamy skopiowanie go z wiadomości e-mail i wklejenie do pola na tym ekranie.

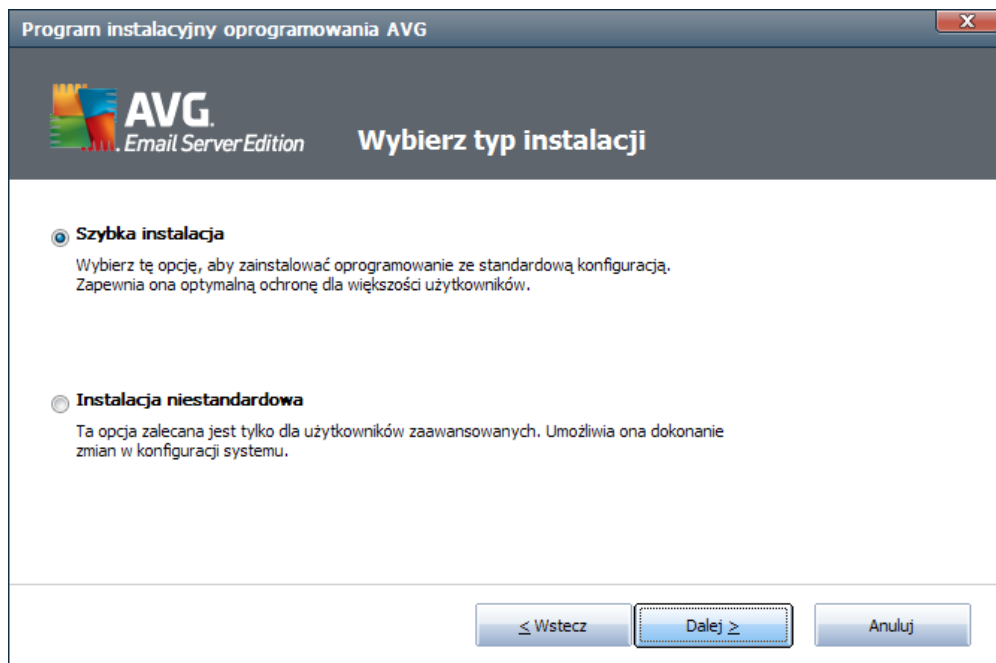
Jeśli oprogramowanie zostało zakupione w sklepie, numer licencji można znaleźć na karcie rejestracyjnej produktu znajdującej się w opakowaniu. Upewnij się, że numer został skopiowany prawidłowo.

≤ Wstecz Dalej ≥ Anuluj

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



3.3. Wybór typu instalacji



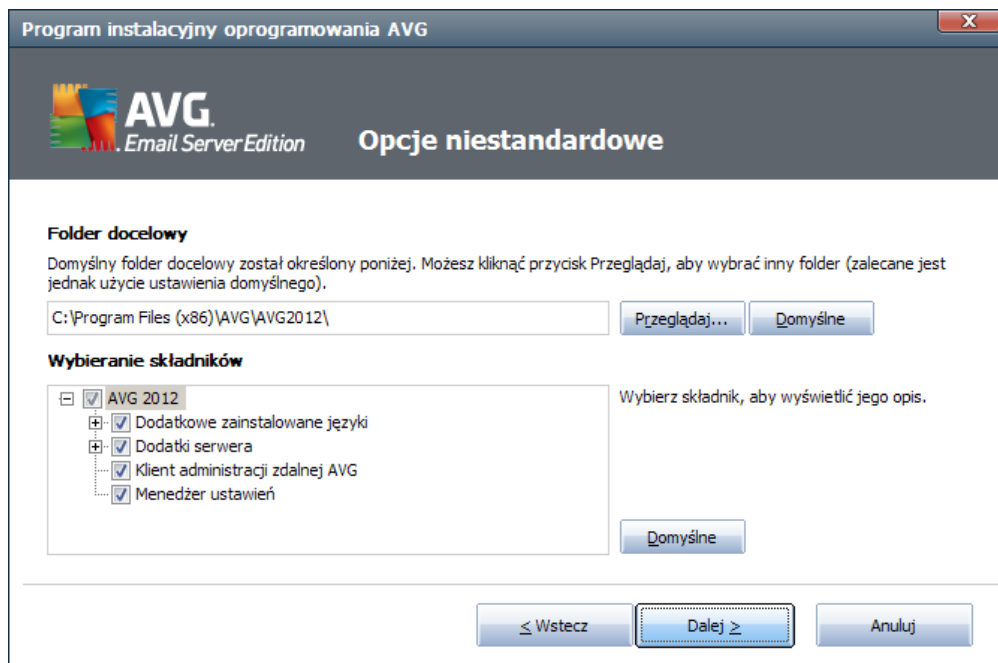
Okno dialogowe **Wybierz typ instalacji** umożliwia wybranie jednej z dwóch opcji: **Instalacja szybka** lub **Instalacja niestandardowa**.

Większość użytkowników zdecydowanie powinna wybrać opcję **Instalacja szybka**, 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).



3.4. Instalacja niestandardowa – opcje niestandardowe



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.

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!

- **Klient Administracji zdalnej AVG** — jeśli system AVG ma mieć możliwość łączenia się z bazą AVG DataCenter (wersje AVG Network Edition), konieczne jest wybranie tej opcji

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

- **Menedżer ustawień systemu** — narzędzie przeznaczone przede wszystkim dla administratorów sieci, pozwalające na kopiowanie, edycję i dystrybucję 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 pozwala określić, jakie języki interfejsu użytkownika mają zostać zainstalowane. Należy w tym celu zaznaczyć opcję **Dodatkowe zainstalowane języki** i wybrać je z odpowiedniego menu.

Podstawowy przegląd poszczególnych składników serwera (**datki serwera**):

- **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.

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

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

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

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

- **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.

Uwaga: Dla różnych wersji serwera MS Exchange dostępne są różne opcje.

Aby kontynuować, kliknij przycisk **Dalej**.



3.5. Ukończenie instalacji

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

Program instalacyjny oprogramowania AVG

AVG
Email Server Edition

Instalacja powiodła się

Dziękujemy za instalację produktu AVG 2012.

Specyfikacja bazy danych AVG Data Center:

Chcę podnieść poziom mojej ochrony, uczestnicząc w [program udoskonalania produktów](#), działającym zgodnie z [Zasadę zachowania prywatności](#) (firma AVG nie będzie gromadziła żadnych danych osobowych, ani kontaktowała się z Tobą)

Zakończ

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

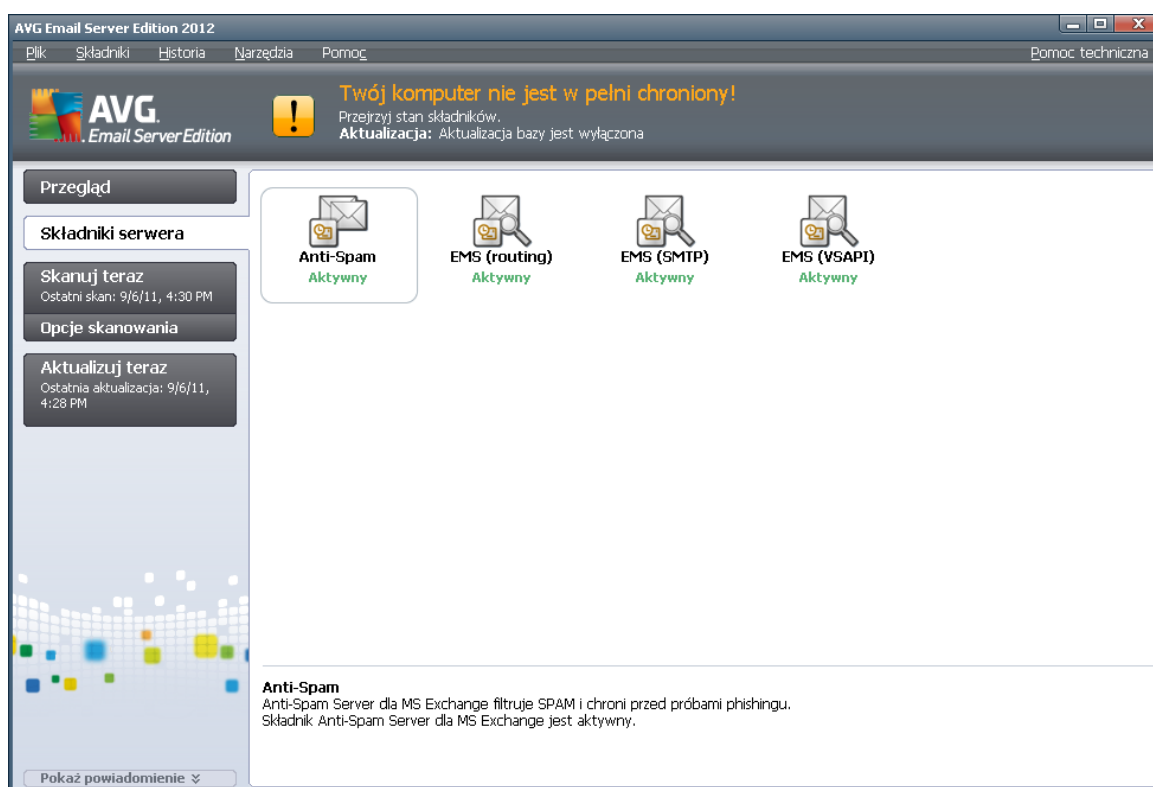
Aby skonfigurować opcje ochrony serwera poczty e-mail, należy przejść do odpowiedniego rozdziału:

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

4. Skaner poczty e-mail dla MS Exchange Server 2007/2010

4.1. Przegląd

Konfiguracja AVG dla MS Exchange Server 2007/2010 jest w pełni zintegrowana z produktem AVG Email Server Edition 2012 pod postacią składników przeznaczonych dla serwerów.



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 przychodzące, wychodzące i wewnętrzne wiadomości e-mail przechodzące przez serwer MS Exchange w roli HUB.
Składnik dostępny tylko dla serwera MS Exchange 2007/2010 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.

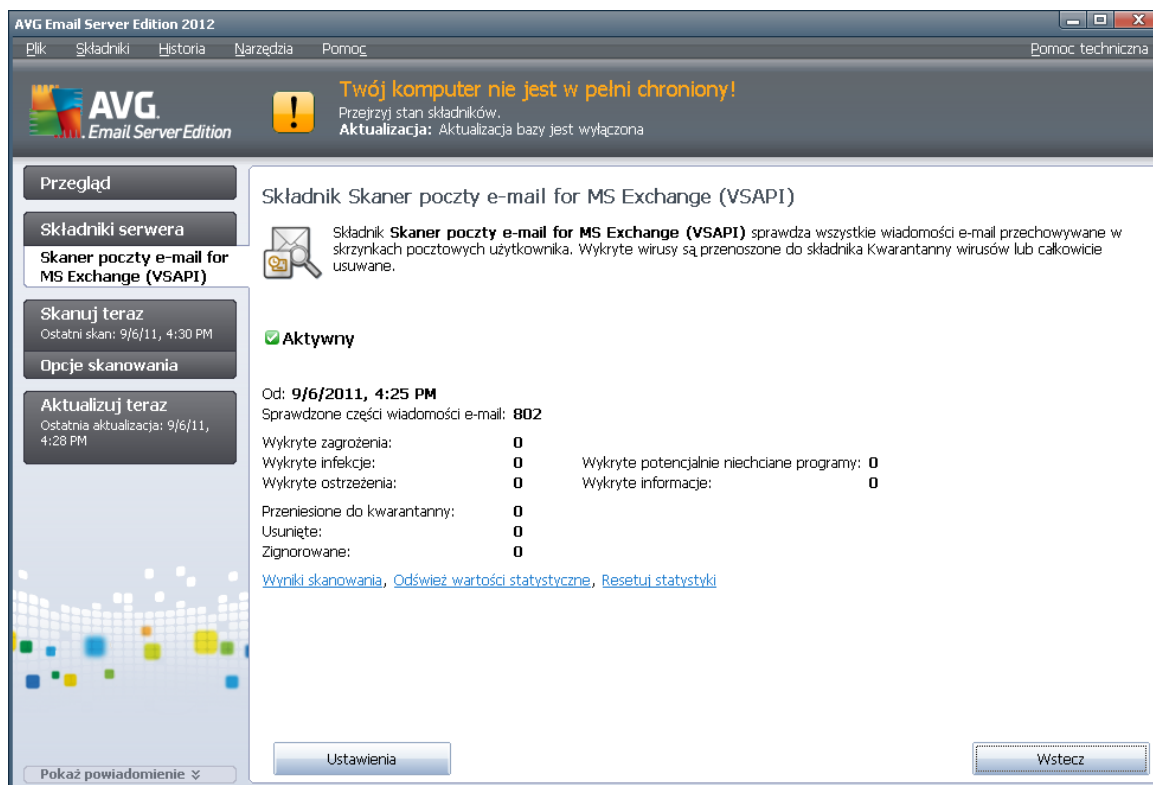
Składnik dostępny tylko dla serwera MS Exchange 2007/2010 w roli EDGE lub HUB.

- **[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 lub usuwane.

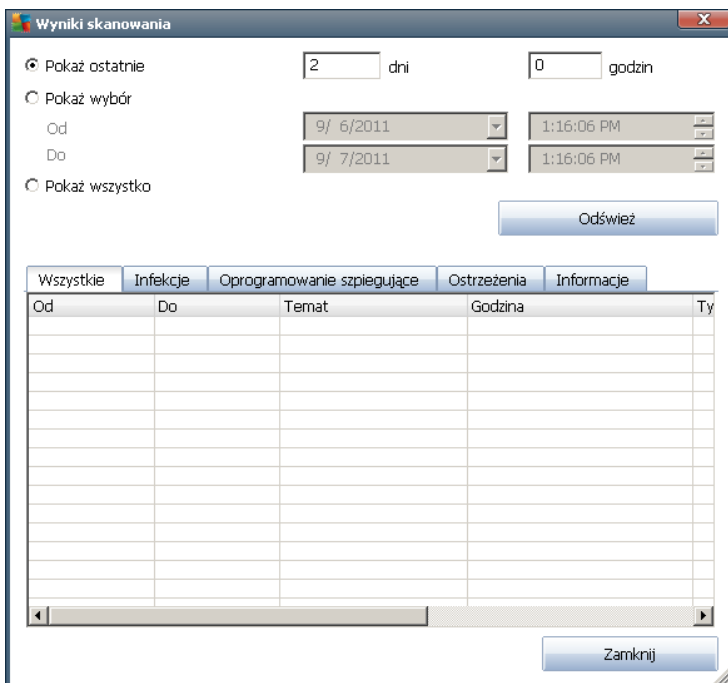
Ważna informacja: Jeśli podczas instalacji używany jest jednocześnie interfejs VSAPI i agent routingu dla serwera w roli Hub, wiadomości e-mail będą skanowane dwukrotnie. Sposób uniknięcia tej sytuacji został opisany w poniższym rozdziale **[Uwaga techniczna](#)**.

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



- ***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:

- **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:

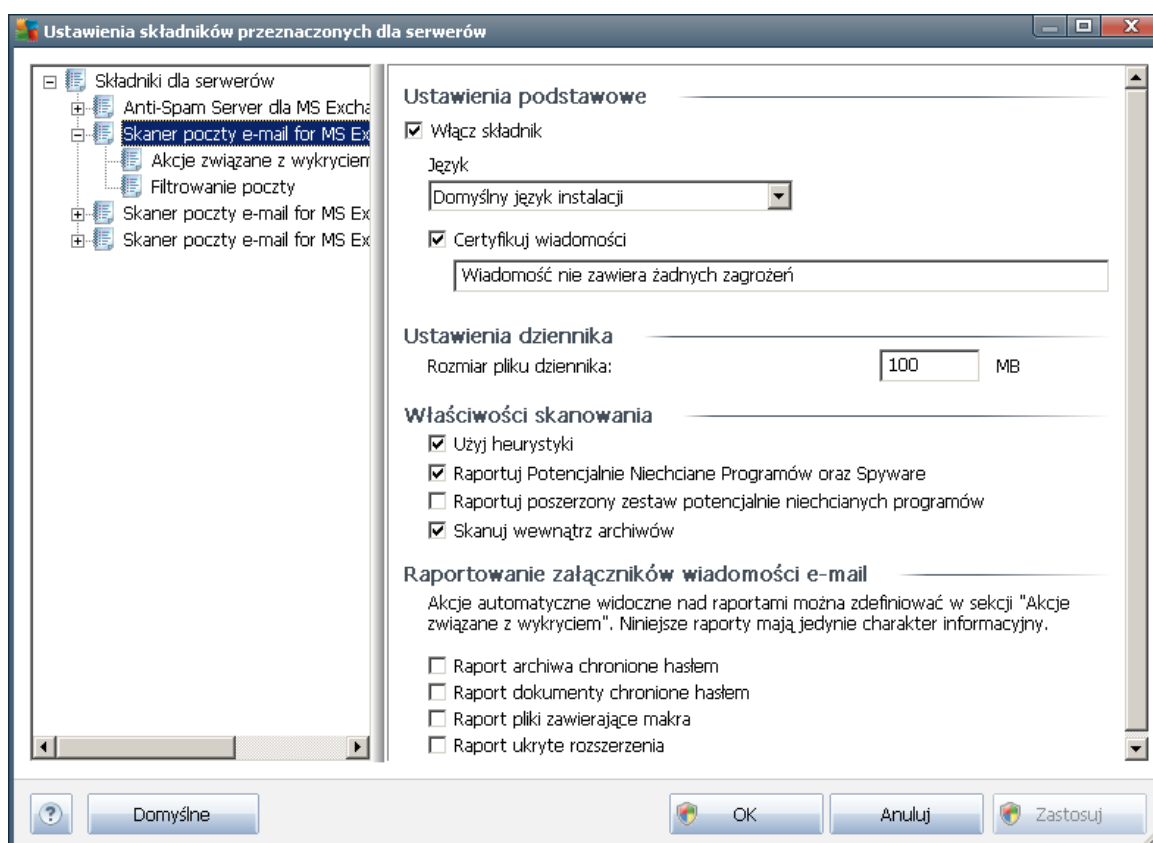
- **Ustawienia** — ten przycisk pozwala otworzyć ustawienia składnika.
- **Wstecz** — ten przycisk umożliwia powrót do okna Przegląd składników serwera.

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

4.2. 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 serwera 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 **Ustawienia dziennika**:

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

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](#)

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.

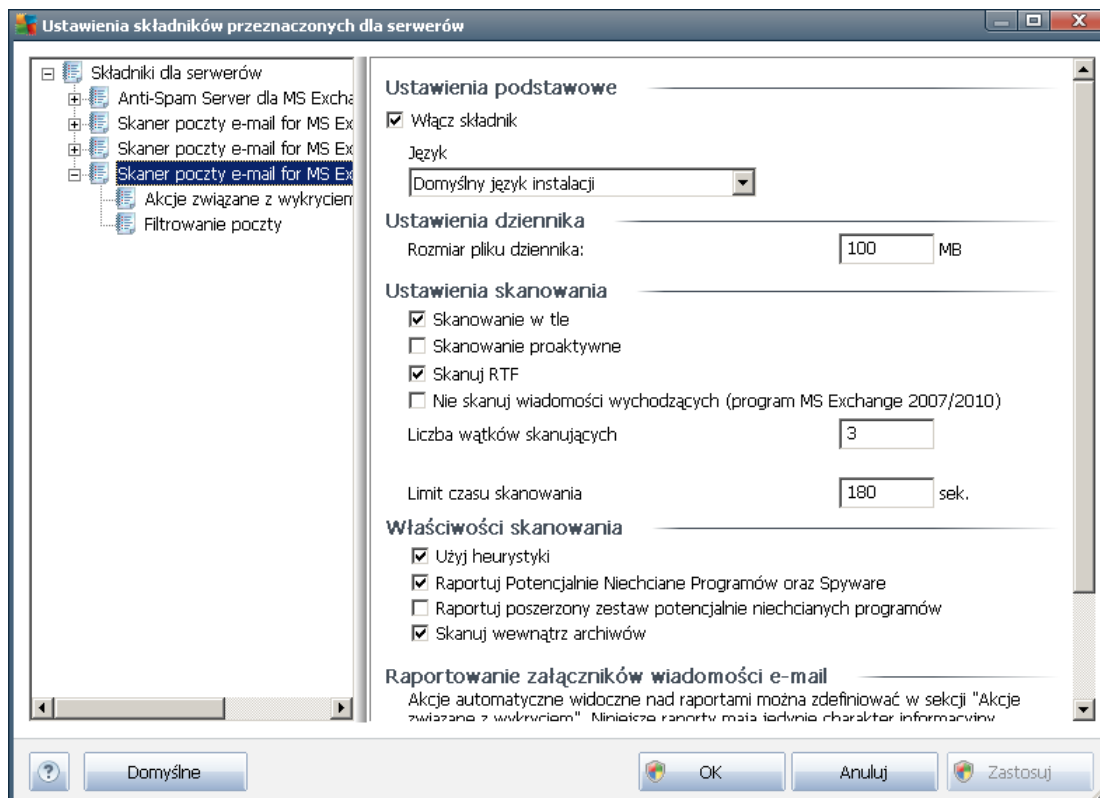
W strukturze drzewa dostępne są następujące podpozycje:

- [Akcje związane z wykryciem](#)

- [Filtrowanie poczty](#)

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

Ta pozycja zawiera ustawienia *Skanera dokumentów dla serwera 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 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 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 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.

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: $(\text{liczba procesorów} * 5) + 1$.

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:

- **Powiadamiał o archiwach chronionych hasłem**
- **Powiadamiał o dokumentach chronionych hasłem**
- **Powiadamiał o plikach zawierających makra**
- **Powiadamiał 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](#)

4.5. Uwaga techniczna

Ta informacja dotyczy sytuacji, w której podczas instalacji używany jest jednocześnie interfejs VSAPI i agent transportowy routingu w roli Hub Exchange. Wówczas wiadomości e-mail będą skanowane dwukrotnie (najpierw przez skaner dostępowy interfejsu VSAPI, a następnie przez agenta transportowego routingu).

Z powodu sposobu działania interfejsu VSAPI możliwe jest wystąpienie niezgodności wyników skanowania i niepotrzebne obciążenie systemu. Dlatego też, aby uniknąć dwukrotnego skanowania, zaleca się wprowadzenie małej poprawki (patrz poniżej), która pozwoli rozwiązać ten problem.



Uwaga: Konfiguracja rejestru powinna być przeprowadzana tylko przez zaawansowanych użytkowników. Przed każdą edycją rejestru zaleca się utworzenie kopii zapasowej i sprawdzenie, w jaki sposób można przywrócić poprzednie ustawienia na wypadek wystąpienia problemów.

Otwórz edytor rejestru (po wybraniu menu **Start/Uruchom** wpisz **regedit** i naciśnij Enter). Przejdź do następującej gałęzi:

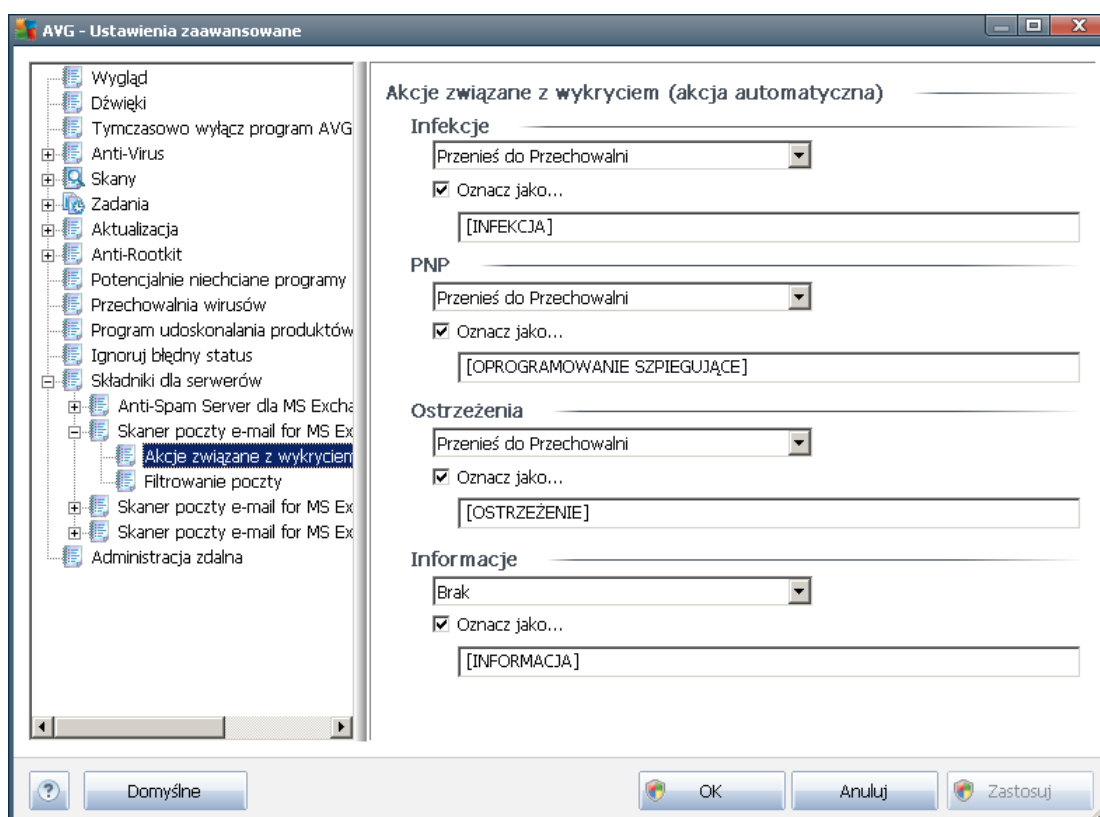
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchange\MSVirusScan

Prawym przyciskiem myszy kliknij prawą część okna i z menu kontekstowego wybierz opcję **Nowy/Wartość DWORD (32-bitowa)**. Nazwij nową wartość **TransportExclusion**. Po jej utworzeniu kliknij ją dwukrotnie, a następnie zmień wartość na **1**.

Na koniec, aby zastosować zmiany dla serwera MS Exchange, ustaw wartość „1” dla opcji **ReloadNow**. Aby to zrobić, dwukrotnie ją kliknij i zmień jej wartość.

Dzięki temu wyłączysz dostępowy skaner wychodzących wiadomości interfejsu VSAPI. Zmiana powinna zostać zastosowana w ciągu kilku minut.

4.6. 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**

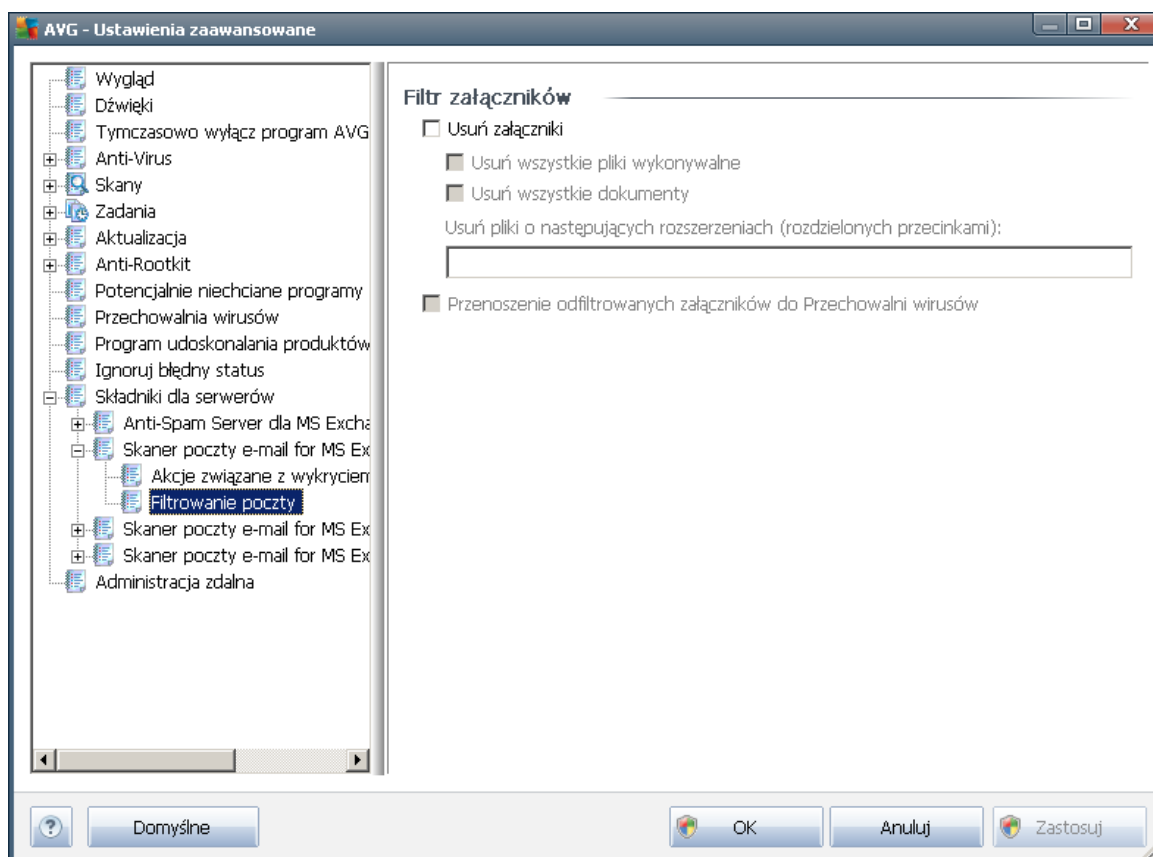
Z menu rozwijanego można wybrać akcję dla każdej pozycji:

- **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.

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

4.7. Filtrowanie poczty



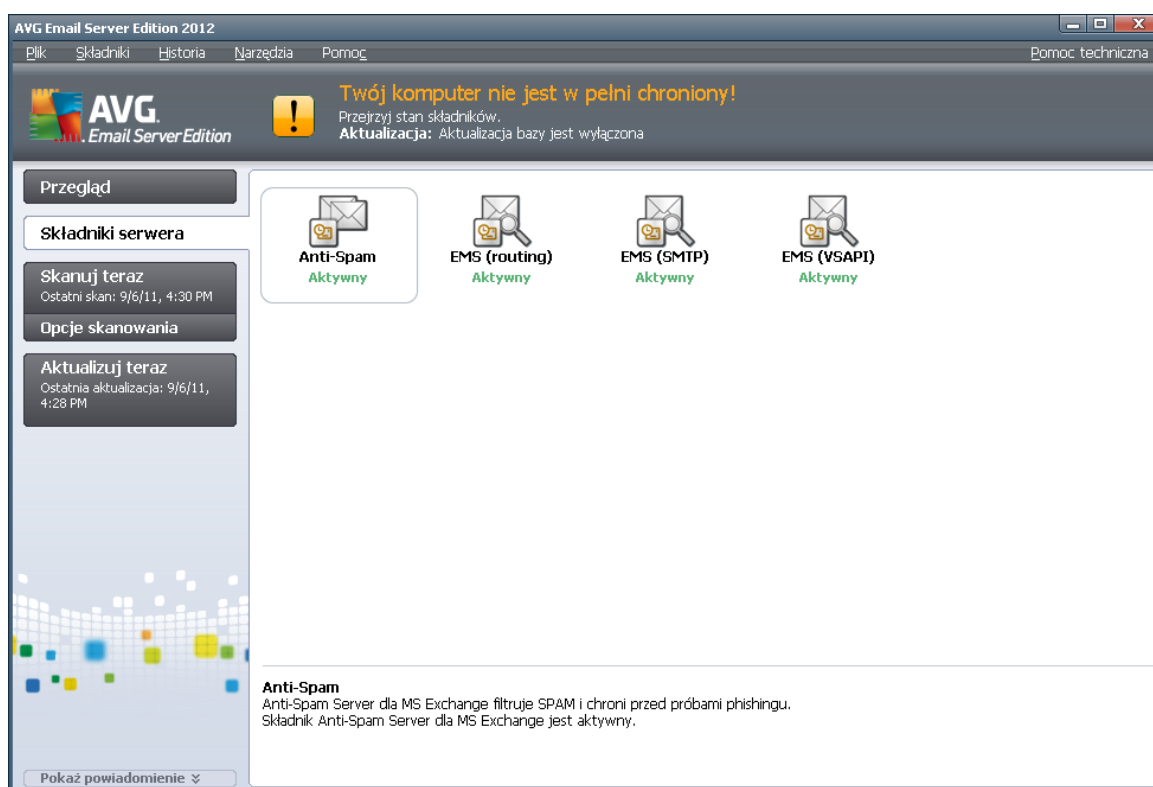
Pozycja **Filtrowanie poczty** umożliwia wybór załączników, które będą automatycznie usuwane. Dostępne są następujące opcje:

- **Usuwać 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 2012**. Wystarczy kliknąć lewym przyciskiem myszy pozycję **Historia**, a następnie wybrać opcję **Przechowalnia wirusów**.

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

5.1. Przegląd

Opcje Skanera poczty e-mail dla MS Exchange Server 2003 są w pełni zintegrowane z produktem AVG Email Server Edition 2012 pod postacią składników 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 składnik, aby otworzyć jego interfejs. Ekran składnika **Anti-Spam** opisany jest w [osobnym rozdziale](#). Interfejs składnika **Skaner poczty e-mail dla MS Exchange (VSAPI)** posiada następujące przyciski i linki:



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:

- **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.

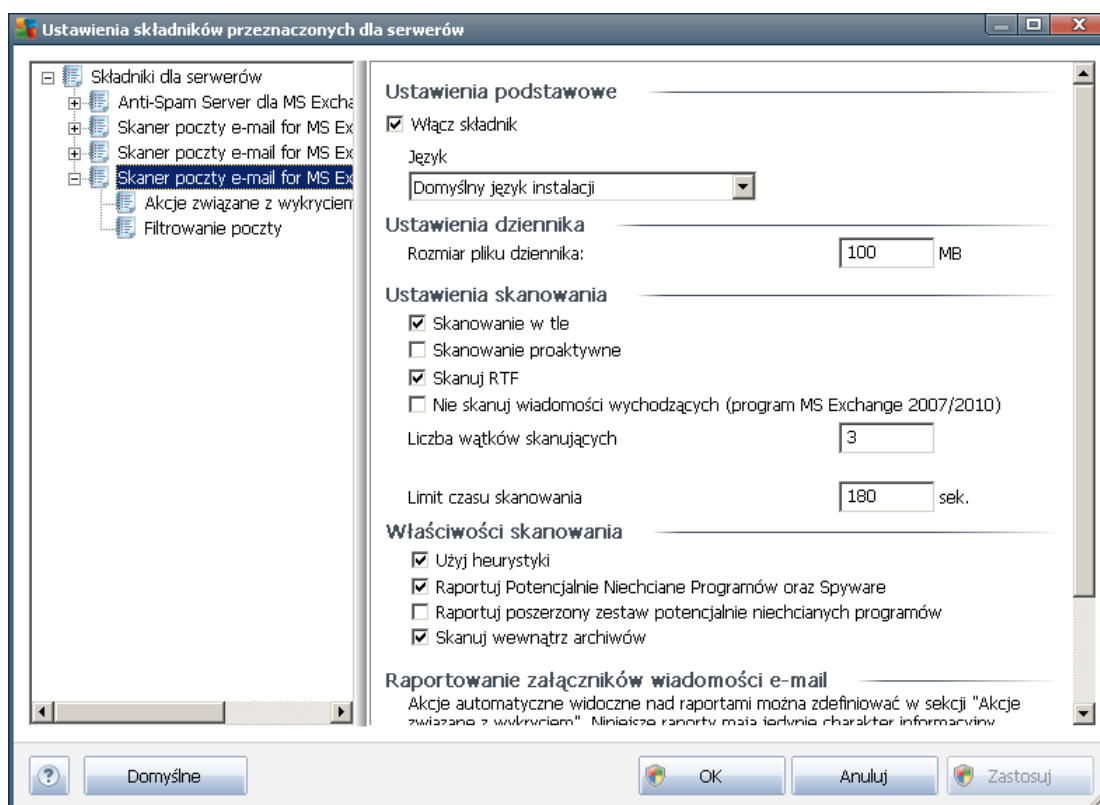
Dostępne przyciski:

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

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

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

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



Sekcja **Ustawienia podstawowe** zawiera następujące opcje:

- **Włącz składnik** — odznaczenie tej opcji spowoduje wyłączenie całego składnika.
- **Język** — 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 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 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.

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: $(\text{liczba procesorów} + 1)$ podzielona przez 2.

Maksymalna liczba wątków jest obliczana według wzoru: $(\text{liczba procesorów} \text{ pomnożona przez } 5) + 1$.

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:

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

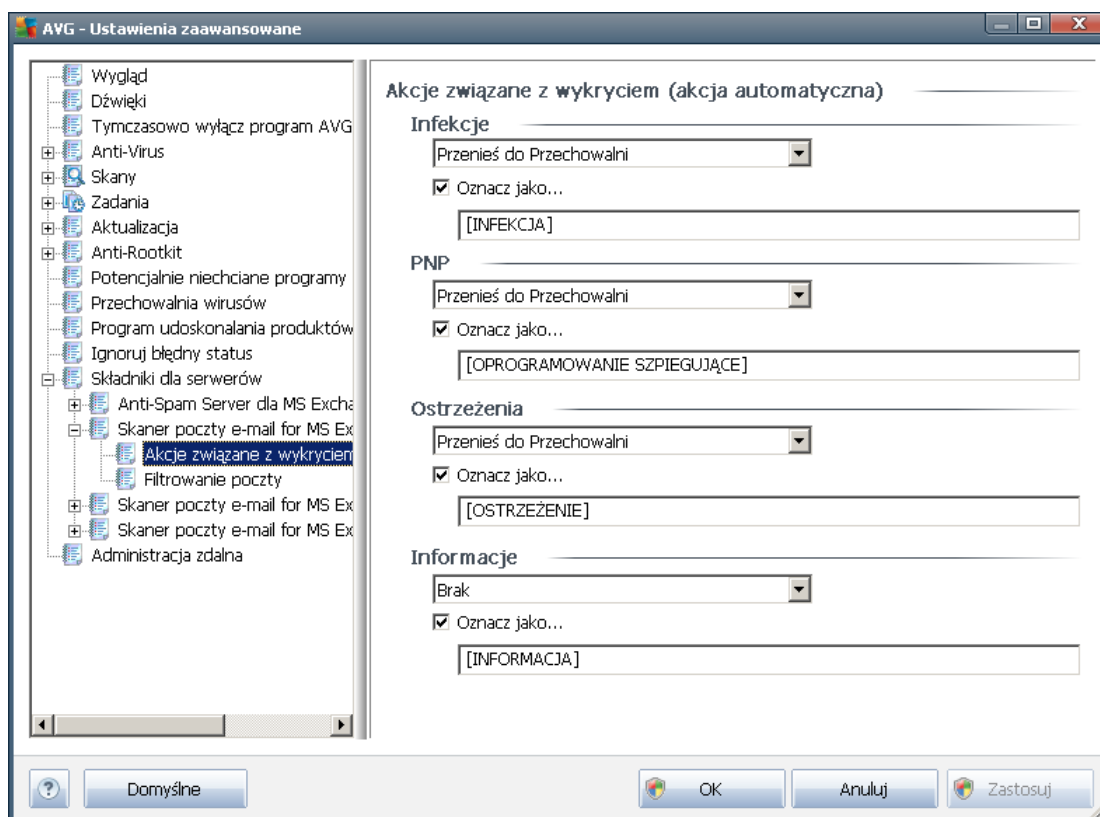
Generalnie, wszystkie te funkcje są rozszerzeniami usług interfejsu Microsoft VSAPI 2.0/2.5. Szczegółowe informacje na temat interfejsu VSAPI 2.0/2.5 można znaleźć dzięki poniższym linkom:

- <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](#)

5.3. Akcje związane z wykryciem



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

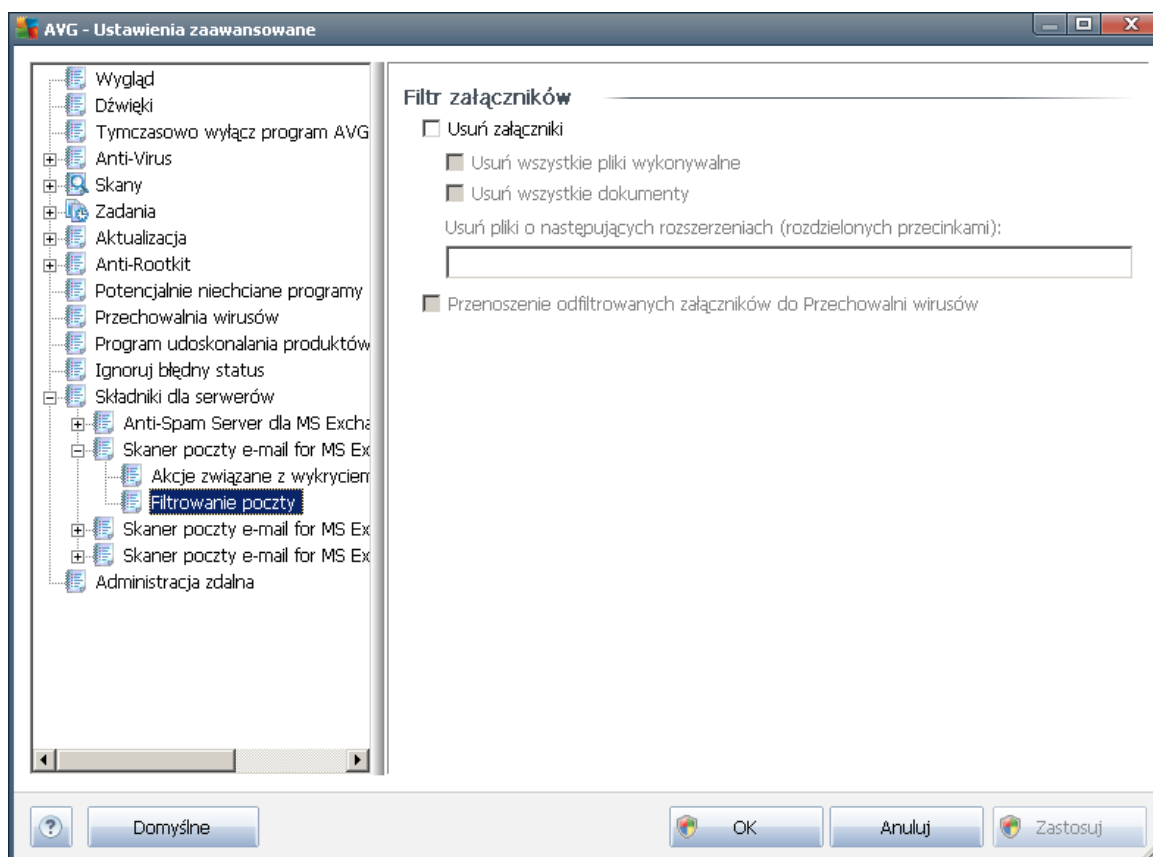
Akcje te są dostępne dla następujących pozycji:

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

Z menu rozwijanego 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.

5.4. Filtrowanie poczty



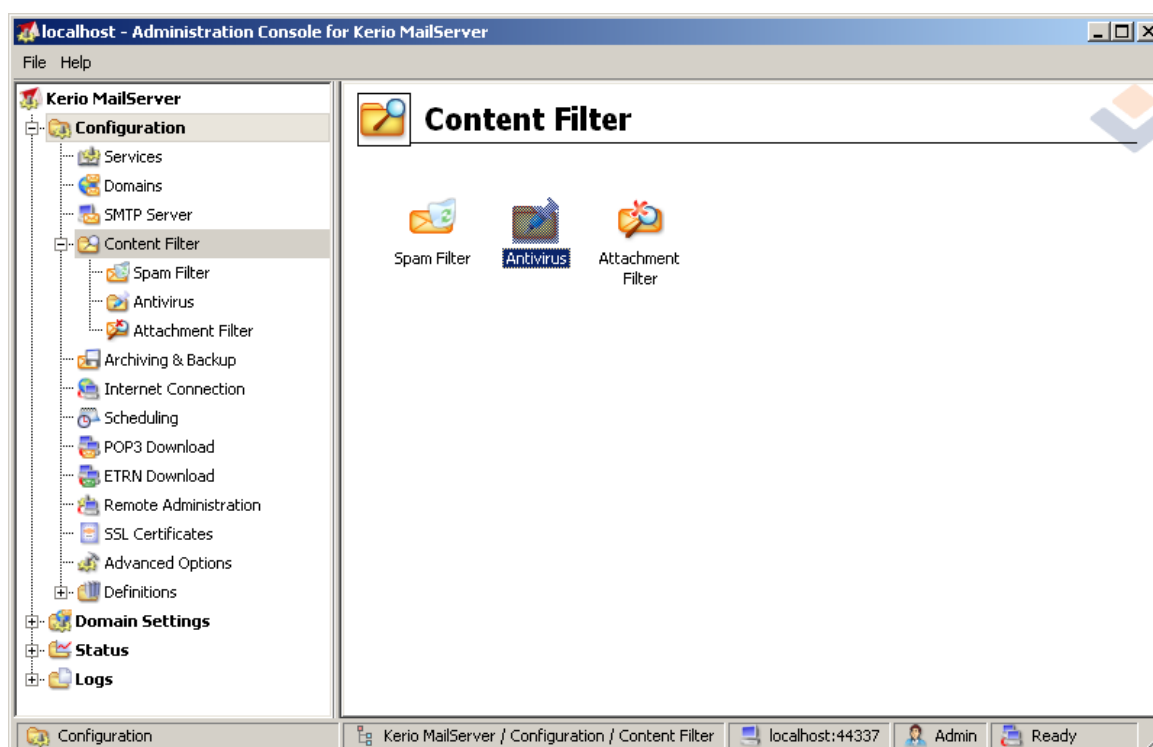
Pozycja **Filtrowanie poczty** umożliwia wybór załączników, które będą automatycznie usuwane. Dostępne są następujące opcje:

- **Usuwać 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 w górnym menu głównego interfejsu programu **AVG Email Server Edition 2012**. Wystarczy kliknąć lewym przyciskiem myszy pozycję **Historia**, a następnie wybrać opcję **Przechowalnia wirusów**.

6. AVG dla Kerio MailServer

6.1. 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**)

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:



Antivirus usage

Use integrated McAfee® antivirus engine

Use external antivirus AVG Email Server Edition Options

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**

If a virus is found in a message

Discard the message

Deliver the message with the malicious code removed

Forward the original message to administrator address:

Forward the filtered message to administrator address:

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.
 - **Przełącz oryginalną wiadomość na adres administratora** — po wybraniu tej opcji wiadomość zainfekowana wirusem będzie przekazywana na adres określony w polu tekstowym.
 - **Przełącz wiadomość spełniającą 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

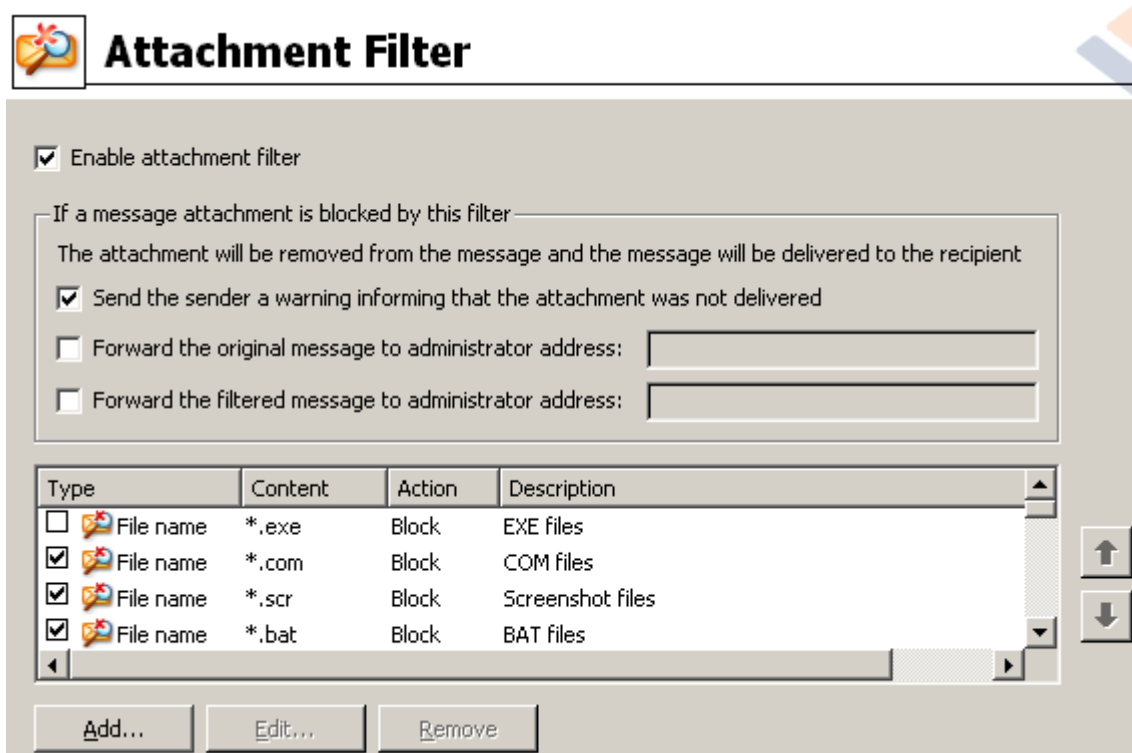
Reject the message as if it was a virus (use the settings above)

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.
- **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.

6.1.2. Filtr załączników

Menu Filtr załączników zawiera listę różnych definicji załączników:



Attachment Filter

Enable attachment filter

If a message attachment is blocked by this filter —

The attachment will be removed from the message and the message will be delivered to the recipient

Send the sender a warning informing that the attachment was not delivered

Forward the original message to administrator address:

Forward the filtered message to administrator address:

Type	Content	Action	Description
<input type="checkbox"/> File name	*.exe	Block	EXE files
<input checked="" type="checkbox"/> File name	*.com	Block	COM files
<input checked="" type="checkbox"/> File name	*.scr	Block	Screenshot files
<input checked="" type="checkbox"/> File name	*.bat	Block	BAT files

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 podjętych 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 Usun, a dodać — za pomocą przycisku **Dodaj...** Można także zmienić istniejący wpis za pomocą przycisku **Edytuj**. Zostanie wówczas wyświetlone poniższe okno:

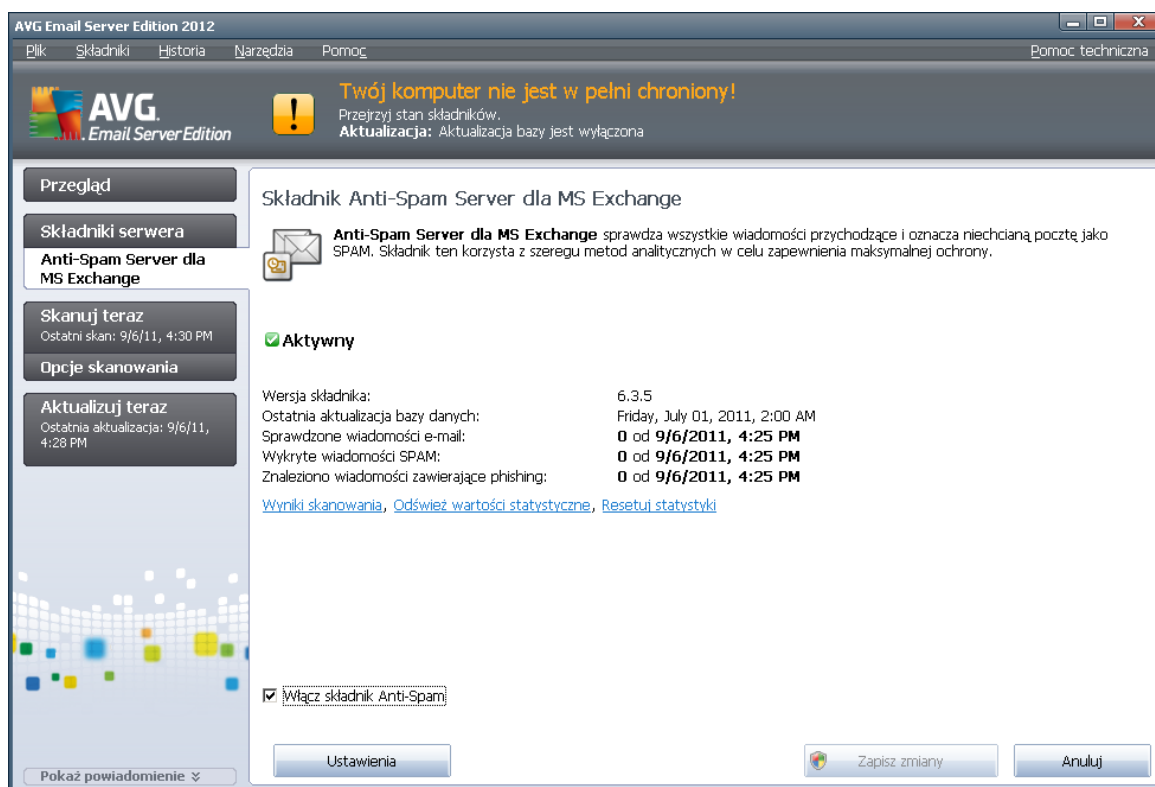


- W polu Opis można wpisać krótki opis załącznika, który ma być filtrowany.
- W polu Jeśli wiadomość e-mail zawiera załącznik można wybrać typ załącznika (Nazwa pliku lub Typ MIME). Dodatkowo można wybrać konkretne rozszerzenie z dostępnej listy lub użyć symboli wieloznacznych.

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

7. Konfiguracja składowika Anti-Spam

7.1. Interfejs składowika Anti-Spam



Okno dialogowe **składowika Anti-Spam** Servermożna znaleźć w sekcji **Składniki serwera** (menu po lewej stronie). Zawiera ono krótką informację o funkcjach składowika 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 składowika Anti-Spam:



Dostępne przyciski:

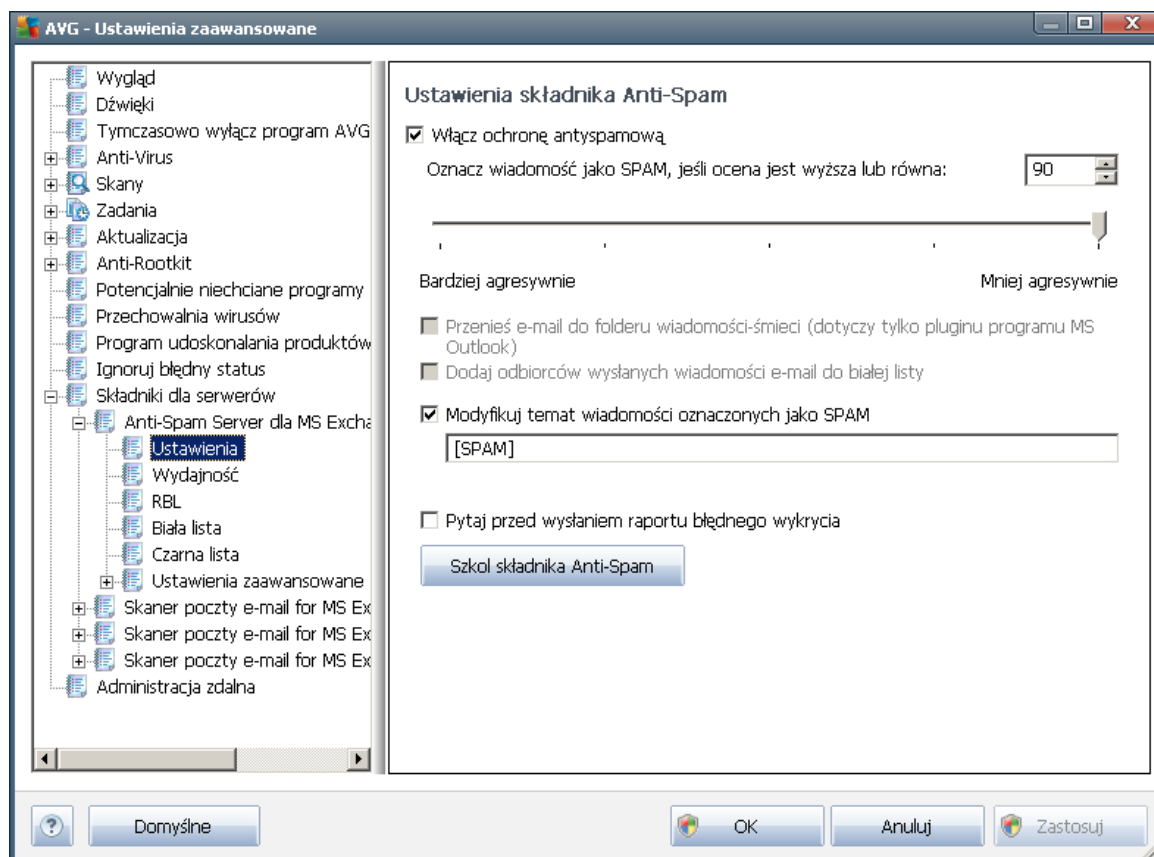
- **Ustawienia** — ten przycisk powoduje otwarcie okna [Ustawienia składowika Anti-Spam](#).
- **Wstecz** — ten przycisk umożliwia powrót do okna Przegląd składowików serwera.

7.2. Zasady działania składowika Anti-Spam

Mianem spamu określa się niechcianą pocztę e-mail (głównie reklamy produktów lub usług, które są hurtowo rozsyłane 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.

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 najsukuteczniejszą dostępną na rynku ochronę.

7.3. Ustawienia składowika Anti-Spam



W oknie dialogowym **Podstawowe ustawienia składowika 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. *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 pożądaných wiadomości (niebędących spamem) mogą zostać błędnie zablokowane.
- **Wartość 60–79** — umiarkowanie agresywna konfiguracja. Wiadomości e-mail, które mogą stanowić [spam](#), są poprawnie odfiltrowywane. Pożądane wiadomości (niebędące spamem) mogą zostać błędnie zablokowane.
- **Wartość 50–59** — bardzo agresywna konfiguracja. Pożądane wiadomości e-mail są odfiltrowywane w równym stopniu, jak wiadomości stanowiące [spam](#). Nie zalecamy stosowania tego progów podczas normalnej pracy.

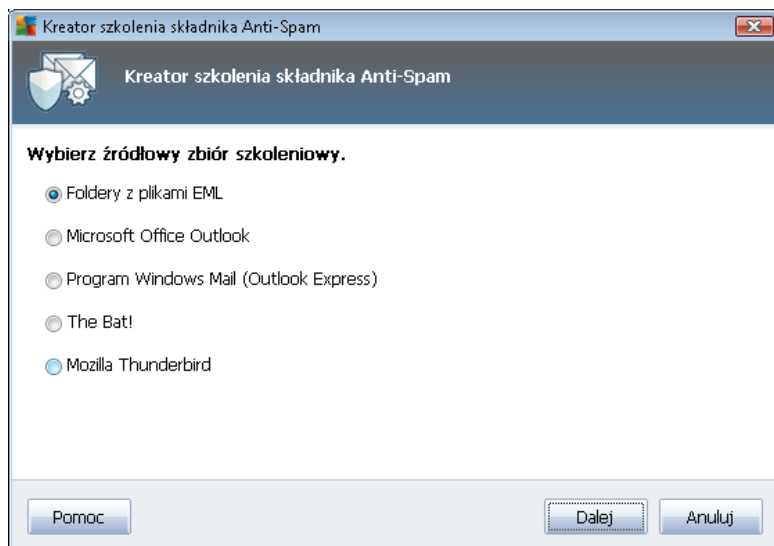
Następnie można zdefiniować, jakie akcje mają zostać podjęte wobec wiadomości e-mail wykrytych jako [spam](#):

- **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 umożliwi 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.

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 wiadomości e-mail, które zostaną użyte do szkolenia. Na ogół używa się do tego celu niechcianych wiadomości 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 wskaż 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.

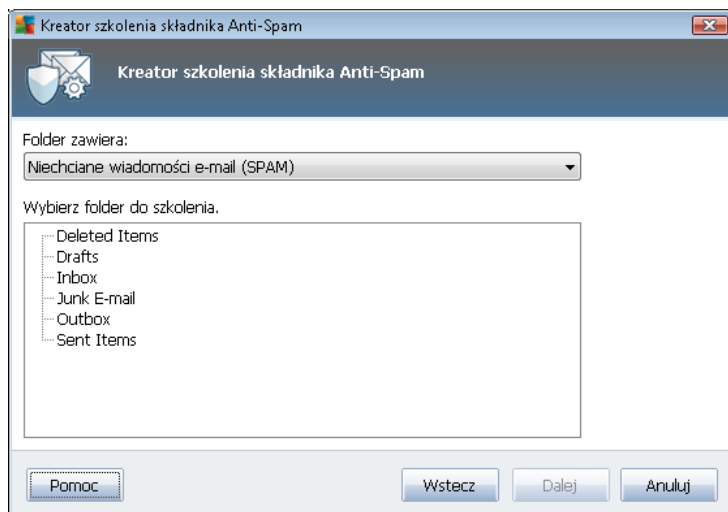
Aby proces szkolenia był prostszy i przebiegał szybciej, warto już wcześniej tak posortować e-maile, aby folder używany w szkoleniu zawierał jedynie wiadomości szkoleniowe (albo spam, albo ham). Nie jest to jednak konieczne, gdyż wiadomości można przefiltrować ręcznie w późniejszym czasie.

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



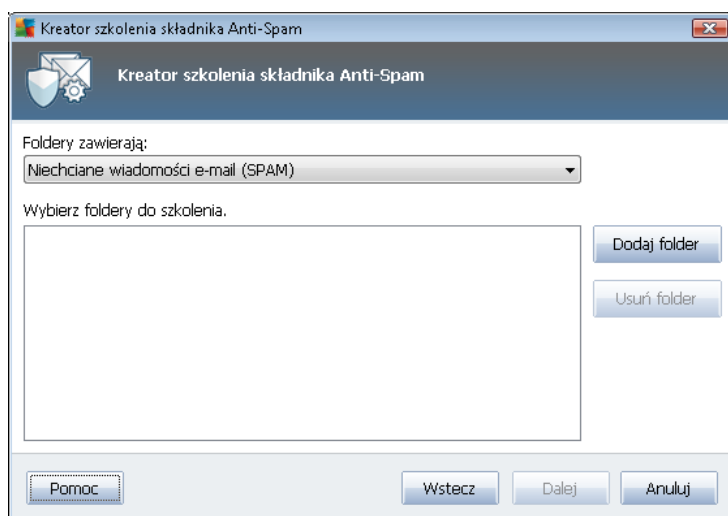
W oknie tym należy wybrać folder z wiadomościami, które mają zostać użyte do szkolenia. Kliknij przycisk **Dodaj folder**, aby zlokalizować folder z plikami .eml (*zapisanymi wiadomościami e-mail*). Wybrany folder zostanie wyświetlony w bieżącym oknie.

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.



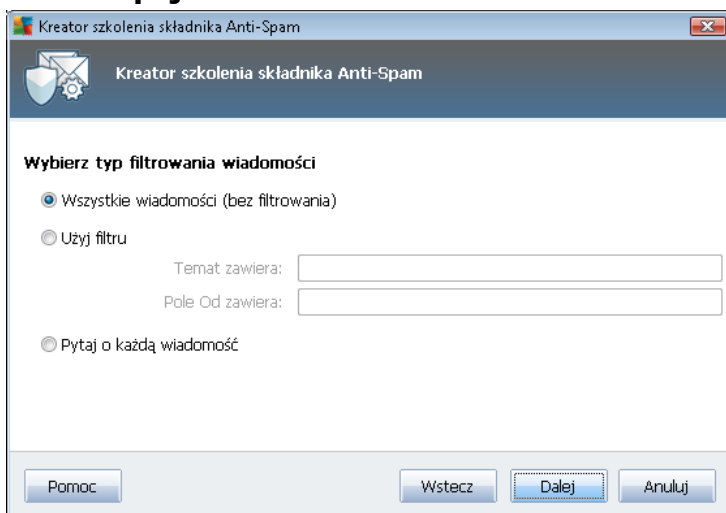
Uwaga: W przypadku programu Microsoft Office Outlook pojawi się najpierw monit o wybranie

profilu 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 żądany 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 wiadomości

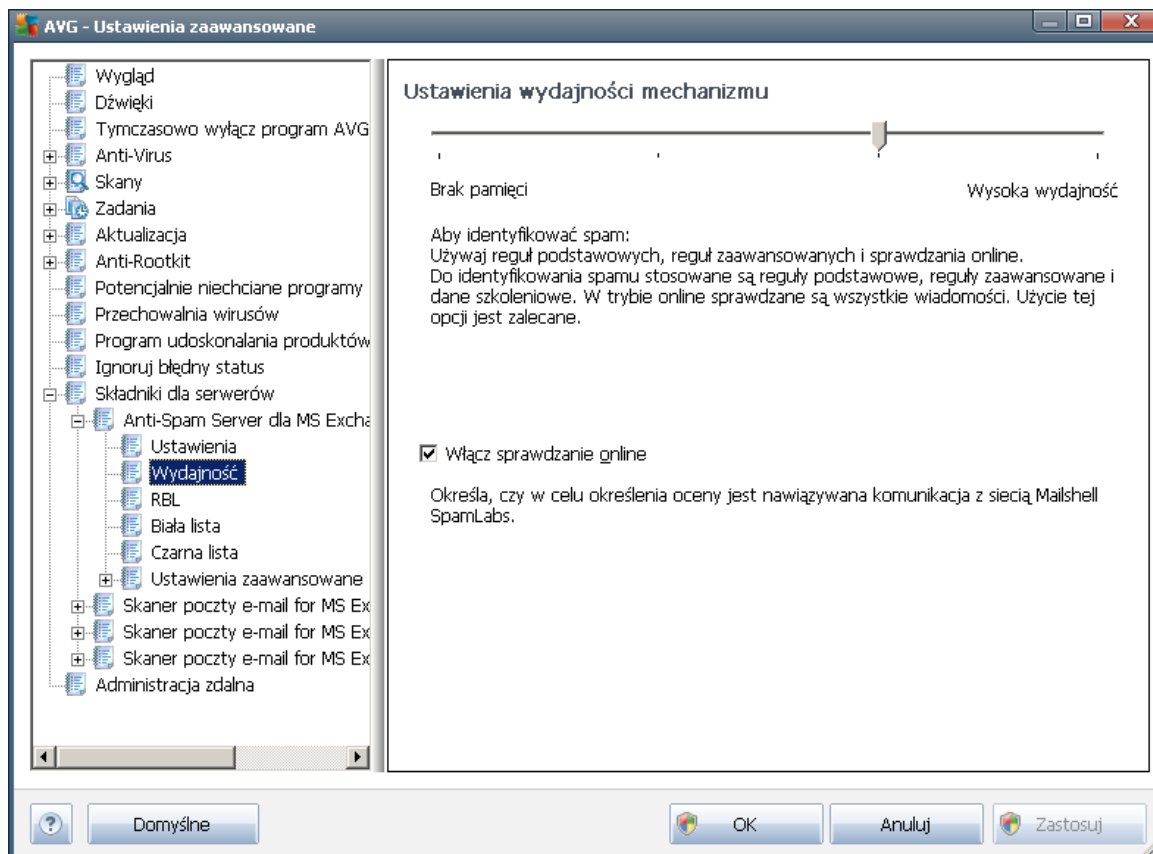


W tym oknie można ustawić filtrowanie wiadomości e-mail.

- **Wszystkie wiadomości (bez filtrowania)** - Jeśli masz pewność, że wszystkie wiadomości w danym folderze są poprawnymi przypadkami treningowymi, zaznacz opcję **Wszystkie wiadomości (bez filtrowania)**.
- **Użyj filtru** - Aby zastosować zaawansowane filtrowanie, zaznacz 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 monitów. W przypadku wypełnienia obu pól tekstowych zostaną użyte także adresy spełniające tylko jeden z dwóch warunków!
- **Pytaj o każdą wiadomość** - Jeśli nie ma pewności co do charakteru wiadomości znajdujących się w folderze i kreator powinien pytać o każdą z nich (*dając możliwość określenia, czy ma zostać użyta w szkoleniu*), należy wybrać opcję **Pytaj o każdą wiadomość**.

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 składnika **Anti-Spam**. Przesuwając suwak w lewo lub w prawo, można zmienić wydajność skanowania na skali między trybami **Brak pamięci** i **Wysoka wydajność**.

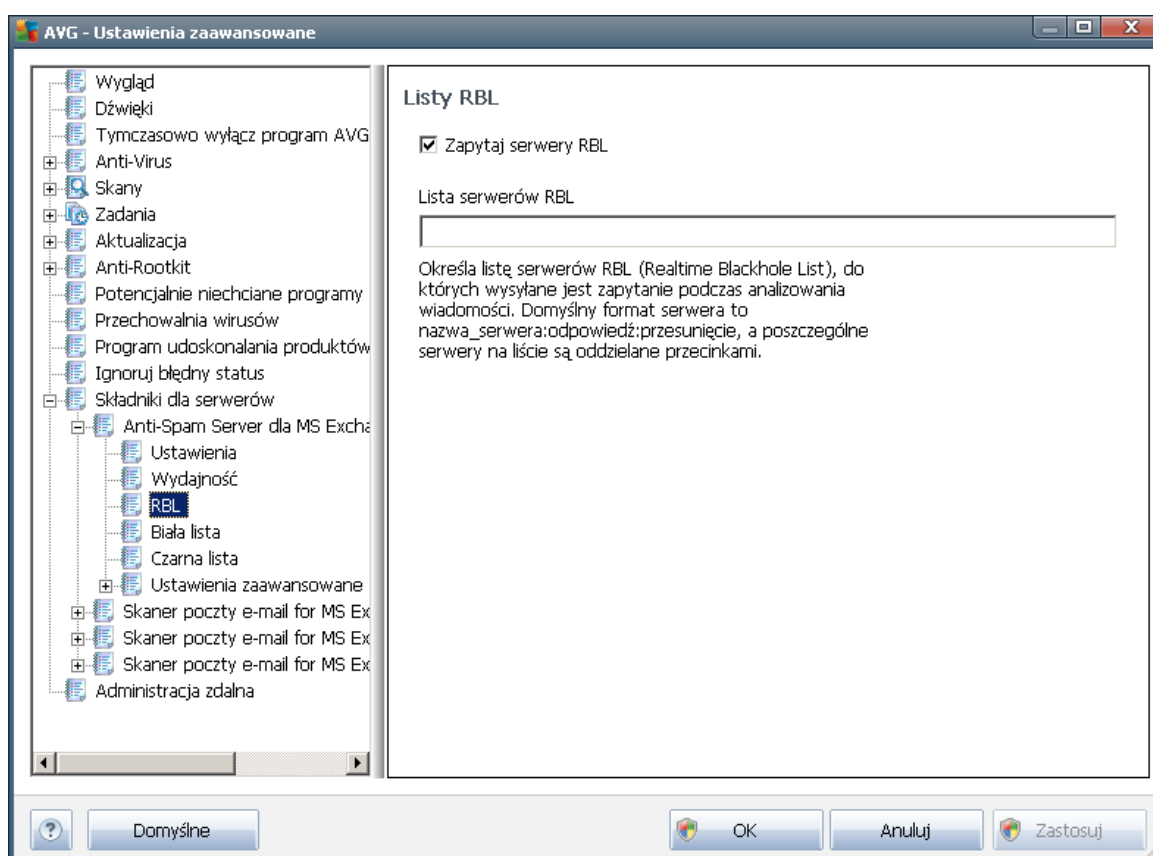
- **Brak pamięci** — w czasie skanowania w poszukiwaniu [spamu](#) nie będą stosowane żadne reguły. Do identyfikacji będą używane tylko dane szkoleniowe. Ten tryb nie jest zalecany do częstego stosowania, chyba że konfiguracja sprzętowa komputera jest bardzo słaba.
- **Wysoka wydajność** — wymaga dużej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

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 okażą 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.

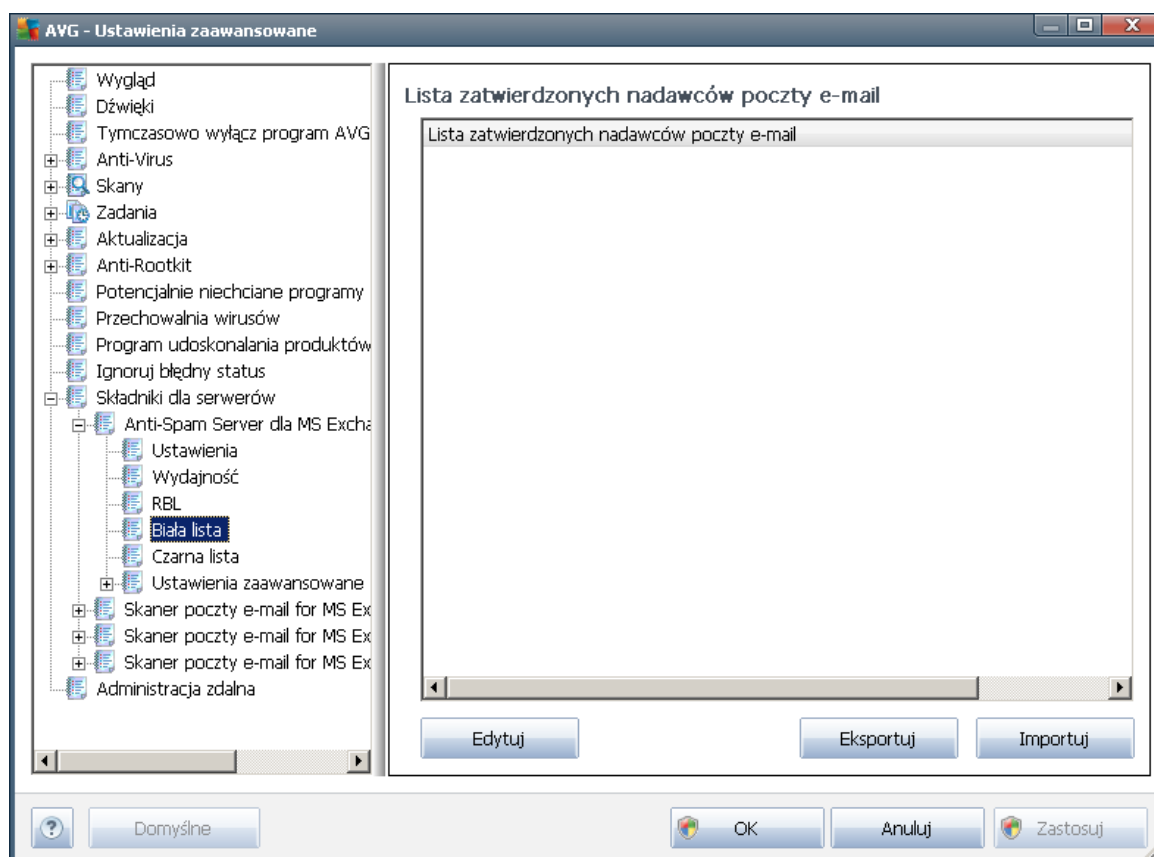
Lista serwerów RBL pozwala określić lokalizację wybranych serwerów RBL. Domyślnie zdefiniowane są tam dwa serwery RBL. Zmiany ustawień domyślnych powinny być dokonywane tylko przez doświadczonych użytkowników i wyłącznie w przypadkach, gdy jest to absolutnie niezbędne!

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.

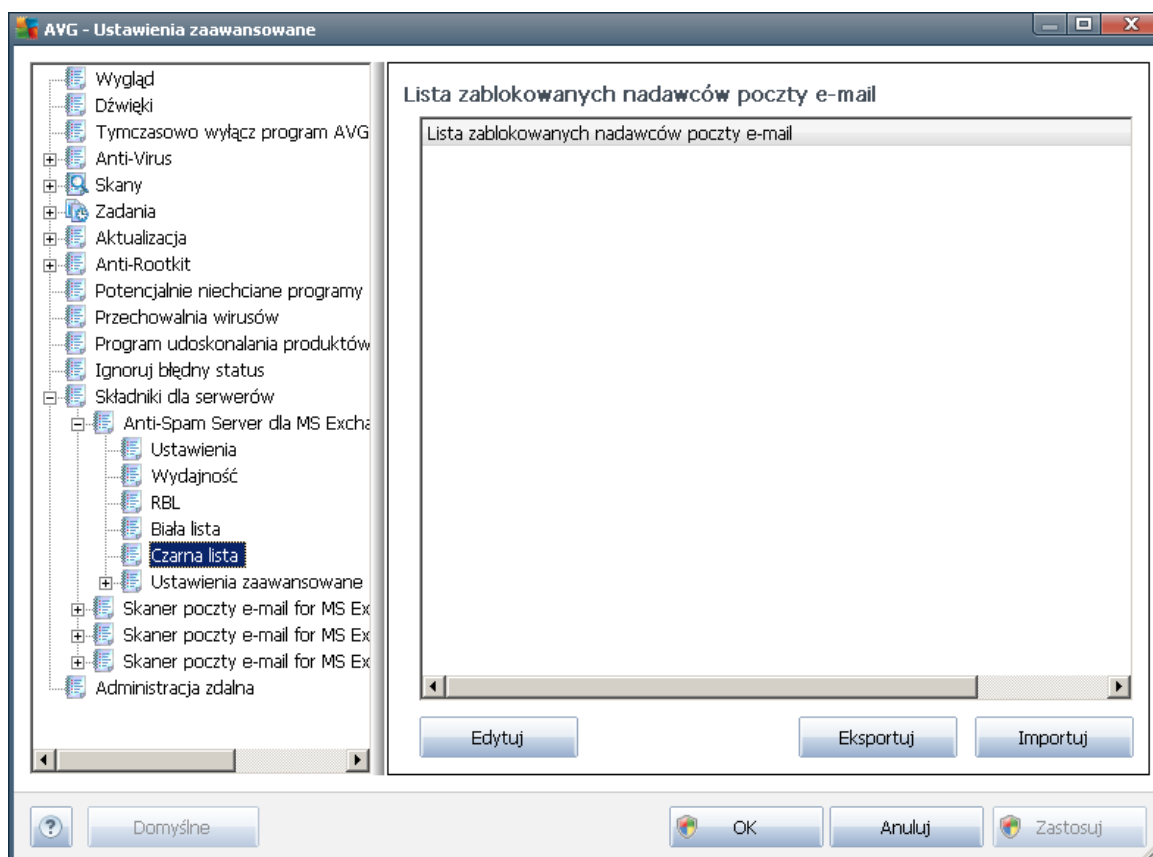
Po przygotowaniu listy adresów i domen, jej elementy można wprowadzić pojedynczo lub zaimportować wszystkie na raz. Dostępne są następujące przyciski kontrolne:

- **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** — 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 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 otrzymywać) 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*). 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 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 edytować 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 podręczna** — 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 AVG

Menedżer ustawień systemu AVG to narzędzie odpowiednie przede wszystkim dla mniejszych sieci, pozwalające na kopiowanie, edycję i dystrybucję 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:

Wszystkie programy/AVG 2012/Menedżer ustawień systemu AVG



• Ustawienia AVG

- **Edytuj ustawienia systemu AVG** — łącze to pozwala otworzyć okno dialogowe z zaawansowanymi ustawieniami lokalnej instalacji AVG. Wszystkie zmiany dokonane w tym miejscu zostaną uwzględnione w lokalnej instalacji systemu AVG.
- **Załaduj i edytuj ustawienia systemu AVG** — jeśli plik konfiguracyjny AVG (.pck) już istnieje, można za pomocą tego przycisku otworzyć go do edycji. Po zatwierdzeniu zmian (przyciskiem **OK** lub **Zastosuj**) zawartość pliku zostanie zastąpiona nowymi ustawieniami!

• Ustawienia Zapory AVG

W tej sekcji możliwe jest wprowadzenie zmian w ustawieniach lokalnej Zapory AVG lub edytowanie ustawień we wcześniej przygotowanym pliku konfiguracyjnym AVG (.pck). Jednak ponieważ Twoja instalacja systemu AVG Email Server Edition 2012 nie obejmuje składnika Zapora, oba łącza będą nieaktywne.

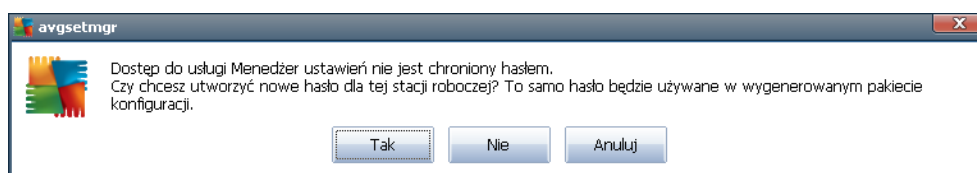
• Opcje ładowania



- **Załaduj zapisane ustawienia do systemu AVG** — łącze to pozwala otworzyć plik konfiguracyjny systemu AVG (.pck) i zastosować go dla lokalnej instalacji systemu AVG.

- **Opcje zapisu**

- **Zapisz lokalne ustawienia systemu AVG w pliku** — łącze to pozwala zapisać plik konfiguracyjny lokalnego systemu AVG (.pck). Jeśli dla dozwolonych akcji nie zostało ustawione hasło, może zostać wyświetlone następujące okno dialogowe:



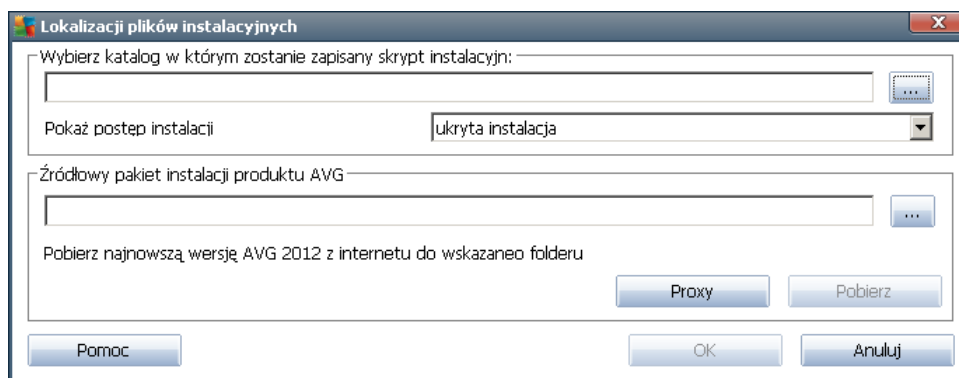
Kliknij **Tak**, jeśli dostęp do dozwolonych pozycji ma być chroniony hasłem, a następnie wprowadź wymagane informacje i zatwierdź swój wybór. Kliknij **Nie**, aby pominąć tworzenie hasła i kontynuować zapisywanie konfiguracji lokalnej instalacji systemu AVG.

- **Opcje klonowania**

- **Zastosuj identyczne ustawienia w całej sieci** — kliknięcie tego łącza pozwala skopiować lokalną instalację systemu AVG poprzez utworzenie pakietu instalacyjnego z niestandardowym zestawem opcji. Klonowanie uwzględnia większość ustawień systemu AVG za wyjątkiem następujących pozycji:

- ✓ *Ustawienia języka*
- ✓ *Ustawienia dźwięków*
- ✓ *Lista elementów dozwolonych i wyjątków potencjalnie niechcianych programów składnika Identity Protection.*

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.

- ✓ *Wyświetlaj tylko postęp instalacji* — instalacja nie będzie wymagała żadnej interakcji ze strony użytkownika, ale jej postęp będzie w pełni widoczny.
- ✓ *Pokaż 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** rozpoczęty zostanie proces klonowania. Może się zdarzyć, że wyświetlone zostanie 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>.

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**.