AVG 9.0 File Server

Podrecznik uzytkownika

Wersja dokumentu 90.7 (31. 3. 2010)

Spis tresci

1. Wprowadzenie

Ten podrecznik uzytkownika zawiera kompleksowa dokumentacje systemu **AVG 9.0 File Server**.

Gratulujemy zakupu systemu AVG 9.0 File Server!

System **AVG 9.0 File Server** nalezy do linii uznanych i nagradzanych produktów AVG, które zapewniaja uzytkownikom spokój ducha, a ich komputerom - pelne bezpieczenstwo. Podobnie jak pozostale produkty, system **AVG 9.0 File Server** zaprojektowano od podstaw pod katem zapewnienia slynnego juz poziomu ochrony w nowy, bardziej przyjazny dla uzytkownika sposób.

Nowy produkt **AVG 9.0 File Server** laczy ulepszony interfejs z agresywniejszym i szybszym skanowaniem. Dla wygody uzytkownika zautomatyzowano najczesciej uzywane funkcje i dodano nowe, „inteligentne" opcje, które pozwalaja precyzyjnie dostosowac funkcje ochronne programu do swoich potrzeb. Koniec z poswiecaniem wydajnosci na rzecz ochrony!

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

2. Wymagania instalacyjne

2.1. Obslugiwane systemy operacyjne

System **AVG 9.0 File Server** sluzy do ochrony stacji roboczych dzialajacych pod nastepujacymi systemami operacyjnymi:

- Windows 2000 Server,
- Windows 2003 Server i Windows 2003 Server x64 Edition
- Windows 2008 Server i Windows 2008 Server x64 Edition

(a takze z nowszymi dodatkami SP dla niektórych systemów operacyjnych)

2.2. Minimalne wymagania sprzetowe

Minimalne wymagania sprzetowe dla systemu **AVG 9.0 File Server**:

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

Zalecane wymagania sprzetowe dla systemu **AVG 9.0 File Server**:

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

3. Opcje instalacji systemu AVG

System AVG mozna zainstalowac za pomoca instalatora znajdujacego sie na oryginalnym dysku CD lub pobranego z witryny AVG (http://www.avg.com).

Przed rozpoczeciem instalacji systemu AVG zalecamy odwiedzenie naszej witryny (http://www.avg.com) w celu sprawdzenia, czy jest dostepny nowy plik instalacyjny. Dzieki temu mozesz miec pewnosc, ze instalujesz najnowsza dostepna wersje systemu AVG 9.0 File Server.

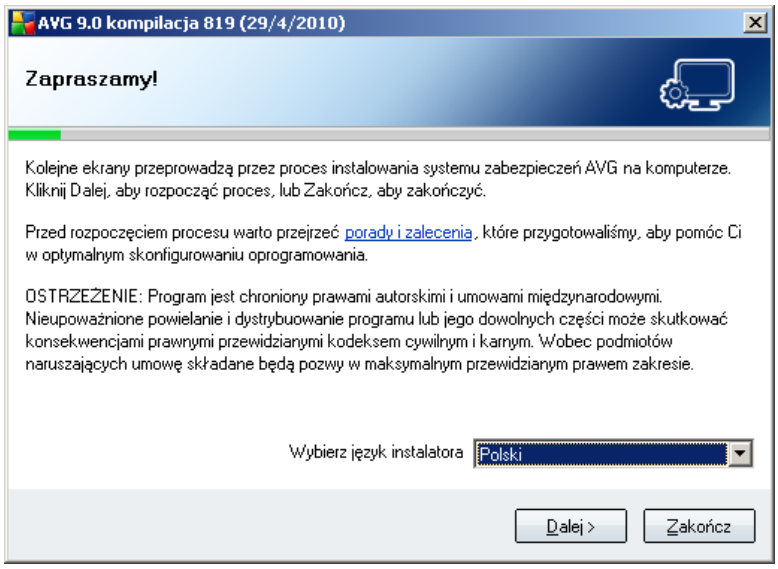
Podczas samego procesu instalacji konieczne bedzie podanie numeru licencji/ sprzedazy. Nalezy wiec przygotowac go przed rozpoczeciem instalacji. Numer sprzedazy znajduje sie na opakowaniu dysku CD. W przypadku zakupienia pakietu AVG przez internet, numer licencji dostarczany jest poprzez e-mail.

4. Proces instalacji systemu AVG

Do zainstalowania systemu **AVG 9.0 File Server** na komputerze konieczny jest najnowszy plik instalacyjny. Mozna znalezc go na dysku CD bedacym czescia dystrybucyjnej edycji programu - istnieje jednak w tym wypadku ryzyko, ze bedzie on nieaktualny. Dlatego zaleca sie pobranie najnowszego pliku instalacyjnego z internetu. Dostepny jest on na oficjalnej stronie AVG (http://www.avg.com) w sekcji ***Pobierz***.

Instalacja to sekwencja okien dialogowych zawierajacych krótkie opisy poszczególnych etapów. Ponizej znajduja sie objasnienia kazdego z nich:

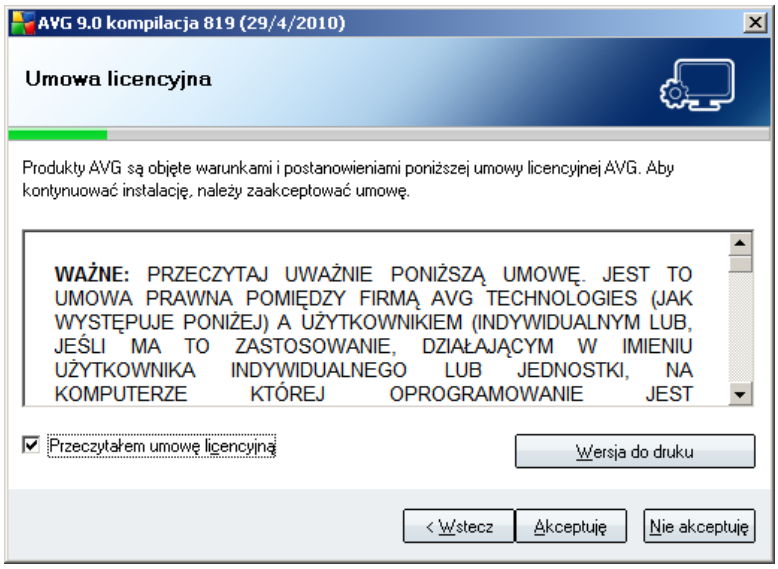
4.1. Uruchamianie instalacji



Proces instalacji rozpoczyna okno ***Witamy w instalatorze AVG***. Mozna w nim wskazac jezyk, który ma byc uzywany podczas instalacji. W dolnej czesci okna znajdziesz menu ***Wybierz jezyk instalatora***. Kliknij przycisk ***Dalej***, aby potwierdzic wybór i przejsc do kolejnego ekranu.

Uwaga: *Jezyk wybrany na poczatku procesu instalacji bedzie pózniej uzywany jako jezyk aplikacji AVG. Mozna go jednak w latwy sposób zmienic w sekcji Interfejs uzytkownika AVG -> Narzedzia -> Ustawienia zaawansowane -> Wyglad.*

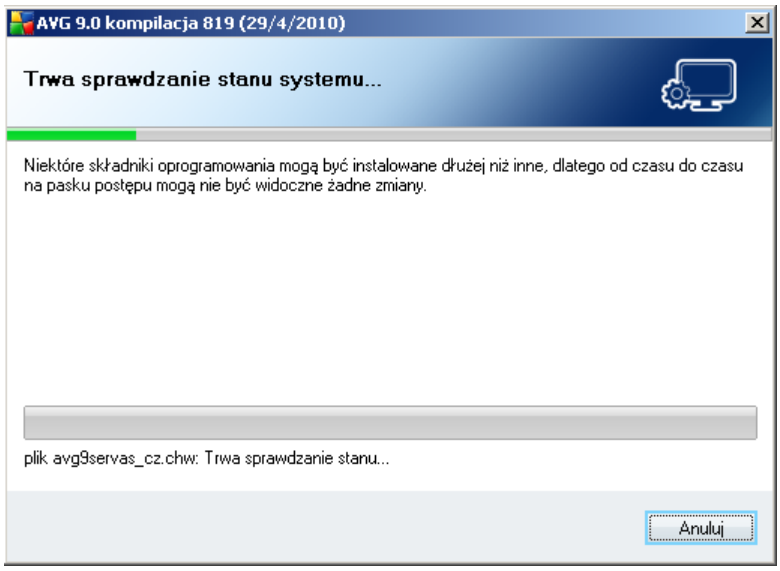
4.2. Umowa licencyjna



Okno dialogowe ***Umowa licencyjna*** zawiera pelna tresc umowy licencyjnej AVG. Przeczytaj ja uwaznie i potwierdz jej akceptacje, zaznaczajac pole ***Przeczytalem warunki umowy licencyjnej*** i wciskajac przycisk ***Dalej***.

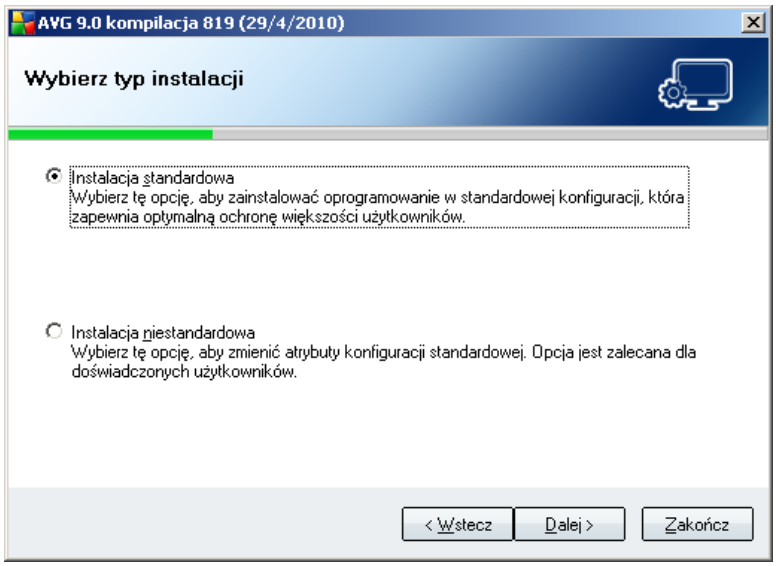
Jesli nie zgadzasz sie na postanowienia umowy, kliknij przycisk ***Nie akceptuje***; instalacja zostanie natychmiast przerwana.

4.3. Sprawdzanie stanu systemu



Po potwierdzeniu umowy licencyjnej nastapi przekierowanie do okna ***Sprawdzanie stanu systemu***. W oknie tym nie trzeba wykonywac zadnych czynnosci; system jest sprawdzany przed rozpoczeciem instalacji AVG. Nalezy poczekac na ukonczenie procesu; przejscie do kolejnego okna nastapi automatycznie.

4.4. Wybieranie typu instalacji



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

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

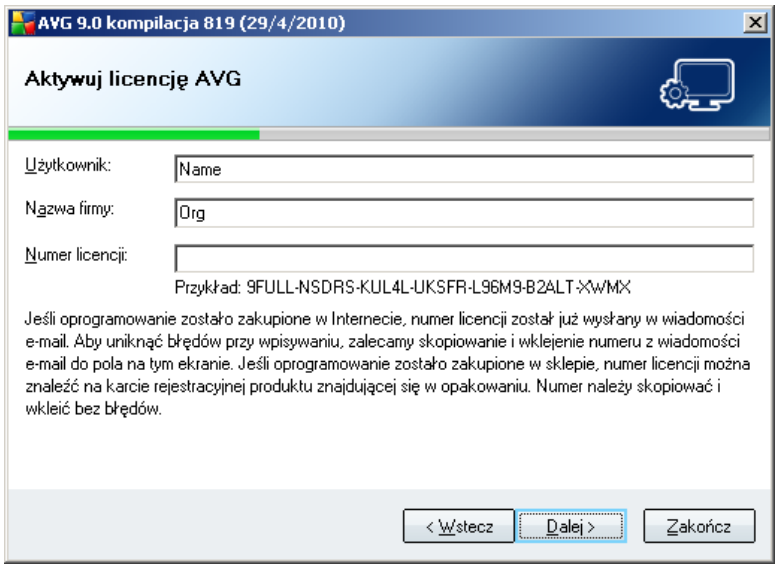
Instalacje niestandardowa powinni wybierac tylko doswiadczeni uzytkownicy, którzy maja uzasadnione powody, aby nie instalowac systemu AVG z domyslnymi ustawieniami (np. chca dostosowac go do specyficznych wymagan systemowych).

4.5. Uaktywnienie licencji AVG

W oknie dialogowym ***Aktywacja licencji AVG*** nalezy wprowadzic swoje dane rejestracyjne. W polu ***Nazwa uzytkownika*** wprowadz swoje imie i nazwisko, a w polu ***Nazwa firmy*** - nazwe organizacji.

Nastepnie wprowadz numer licencji (lub numer sprzedazy) w polu tekstowym ***Numer licencji***. Numer sprzedazy mozna znalezc na opakowaniu dysku CD z oprogramowaniem **AVG 9.0 File Server**. Numer licencji jest wysylany za posrednictwem poczty e-mail po dokonaniu zakupu oprogramowania **AVG 9.0 File**

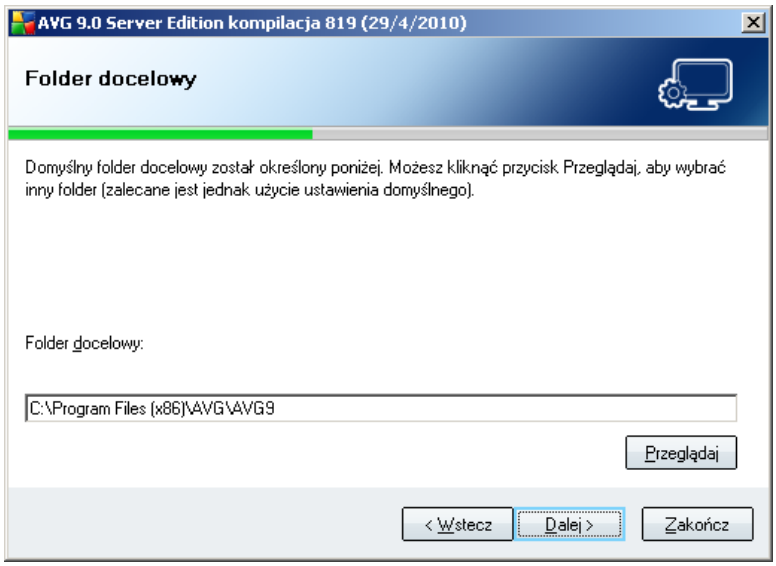
Server online. Wazne jest dokladne wprowadzenie wspomnianego numeru. Jesli numer jest dostepny w formie cyfrowej (*w wiadomosci e-mail*), zaleca sie skopiowanie go i wklejenie w odpowiednim polu.



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

Jesli w poprzednim kroku zostala wybrana instalacja standardowa, nastapi przekierowanie bezposrednio do okna ***Instalowanie systemu AVG***. Jesli zostala wybrana instalacja niestandardowa, zostanie wyswietlone okno ***Folder docelowy***.

4.6. Instalacja niestandardowa - Folder docelowy

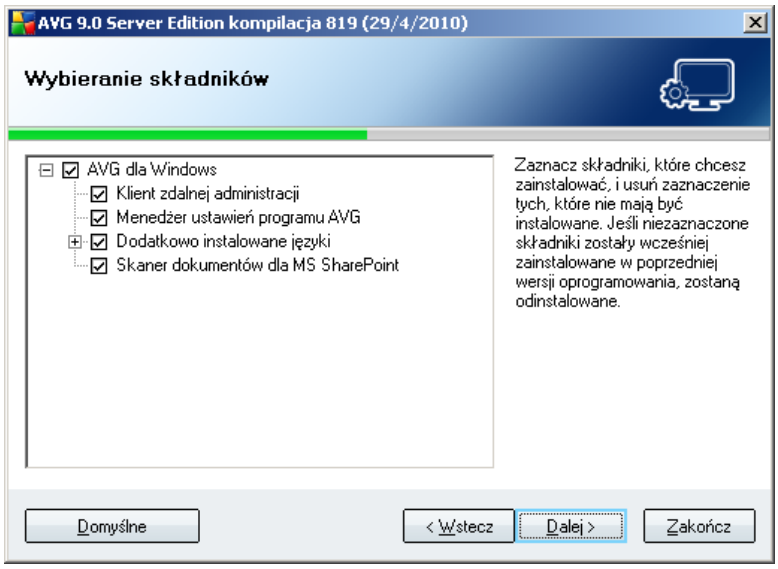


Okno dialogowe ***Folder docelowy*** umozliwia okreslenie lokalizacji, w której ma zostac zainstalowany system **AVG 9.0 File Server**. Domyslnie pakiet AVG jest instalowany w folderze "Program Files" na dysku C:. Jesli wybrany folder nie istnieje, zostanie wyswietlone nowe okno dialogowe z pytaniem o zgode na jego utworzenie.

Aby zmienic te lokalizacje, kliknij przycisk ***Przegladaj*** i w wyswietlonym oknie wybierz odpowiedni folder.

Kliknij przycisk ***Dalej***, aby potwierdzic wybór.

4.7. Instalacja niestandardowa - Wybór skladników



Okno dialogowe ***Wybór składników*** zawiera przeglad mozliwych do zainstalowania skladników systemu**AVG 9.0 File Server**. Jesli ustawienia domyslne nie sa dla Ciebie odpowiednie, mozesz dodac lub usunac zadane skladniki.

- ***Wybór jezyka***

  Na tej samej liscie mozna takze zdefiniowac jezyk (lub jezyki) instalowanego systemu AVG. Nalezy w tym celu zaznaczyc opcje ***Dodatkowe zainstalowane jezyki*** i wybrac je z odpowiedniego menu.

- ***Administracja zdalna***

  Jesli planujesz korzystac z Administracji zdalnej AVG, zaznacz takze odpowiednia pozycje na liscie.

- ***Menedzer ustawien systemu AVG***

  Menedzer ustawien systemu AVG to mala aplikacja, która umozliwia latwe i szybkie konfigurowanie instalacji lokalnych programu AVG (nawet tych, które nie dzialaja pod kontrola Administracji zdalnej). Uzywa on plików konfiguracyjnych (w formacie .pck), które mozna latwo utworzyc za pomoca Menedzera ustawien systemu AVG na dowolnym komputerze z zainstalowana aplikacja AVG. Nastepnie mozna skopiowac je na nosnik wymienny i uzywac na kazdym innym komputerze. Oczywiscie to samo dotyczy Menedzera ustawien systemu AVG. Wiecej

informacji na temat tej aplikacji mozna znalezc **tutaj**.

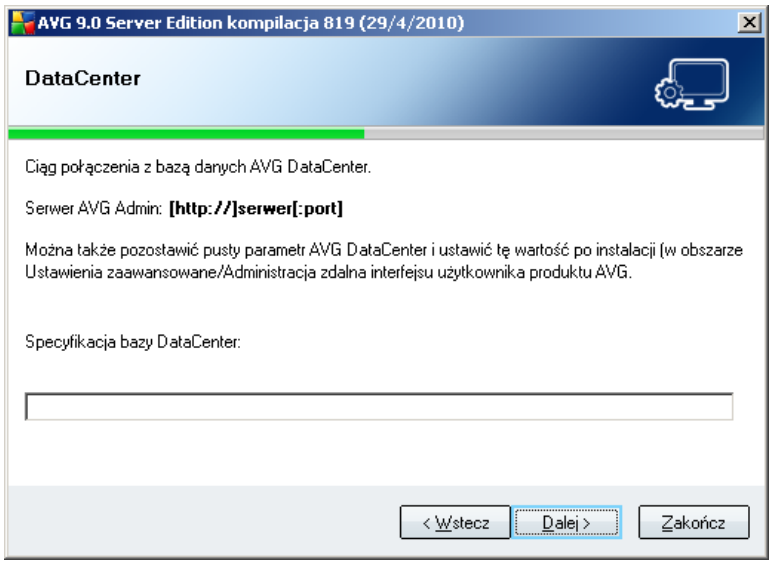
- ***Skaner dokumentów dla MS SharePoint***

  Ten skladnik skanuje dokumenty przechowywane na serwerze MS SharePoint i chroni je przed potencjalnymi zagrozeniami. Jest to podstawowy element systemu **AVG 9.0 File Server**, wiec stanowczo zalecamy jego instalacje.

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

4.8. AVG DataCenter

Jesli uzywasz sieciowej licencji systemu AVG i w poprzednim oknie dialogowym (***Instalacja niestandardowa - Wybór skladników***) wybrano do zainstalowania skladnik ***Administracja zdalna***, nalezy okreslic parametry bazy ***AVG DataCenter***:

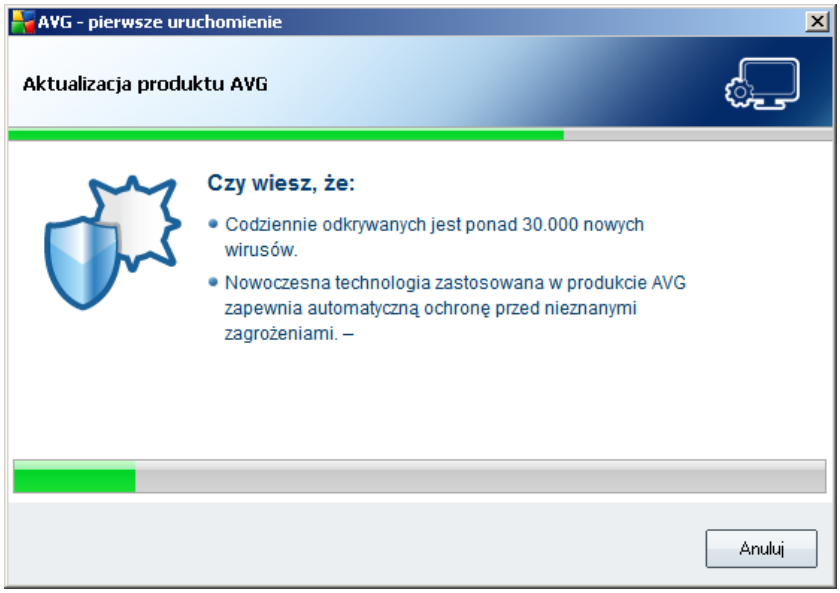


W polu tekstowym ***Specyfikacja bazy AVG DataCenter*** podaj parametry polaczenia z baza ***AVG DataCenter*** (w formacie *serwer:port*). Jesli nie masz tych informacji, mozesz pozostawic to pole puste i dokonac konfiguracji pózniej w oknie ***Ustawienia zaawansowane / Administracja zdalna***.

Uwaga: *Szczególowe informacje dotyczace Administracji zdalnej systemu AVG mozna znalezc w podreczniku uzytkowania systemu AVG Network Edition; podrecznik mozna pobrac ze strony internetowej systemu AVG (http://www.avg.com).*

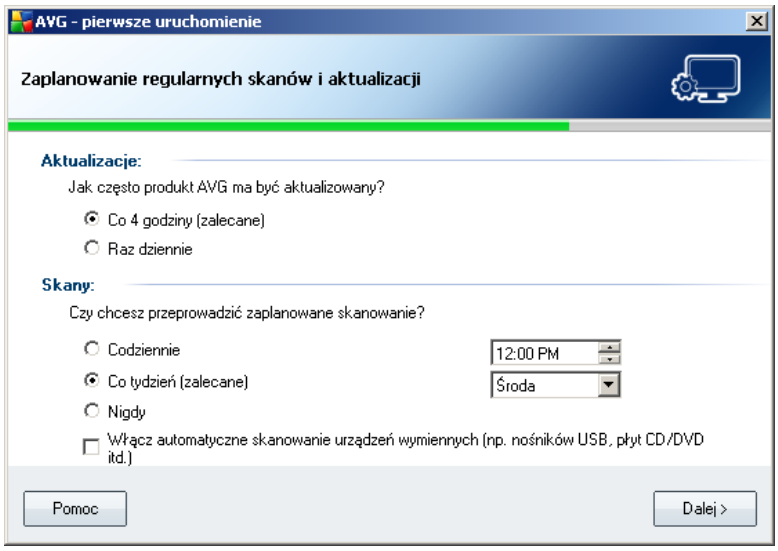
4.9. Instalowanie systemu AVG

Okno dialogowe ***Instalowanie systemu AVG*** zawiera informacje o postepie instalacji i nie wymaga dzialan ze strony uzytkownika:



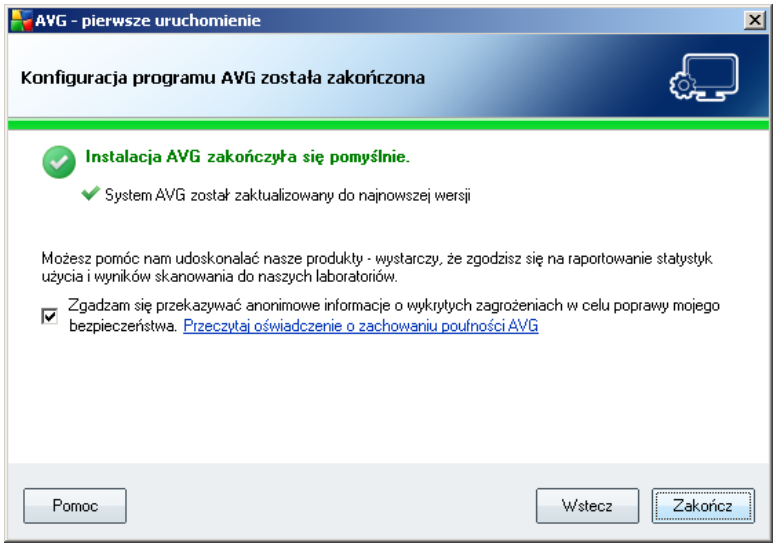
Po zakonczeniu instalacji automatycznie nastapi przekierowanie do nastepnego okna dialogowego.

4.10. Zaplanowanie regularnych skanów i aktualizacji



W oknie dialogowym ***Planowanie cyklicznych skanów i aktualizacji*** okreslic mozna czestotliwosc sprawdzania dostepnosci nowych plików aktualizacji i czasu, w którym nalezy uruchomic skan zaplanowany. Zaleca sie zachowanie wartosci domyslnych. Aby kontynuowac, kliknij przycisk ***Dalej***.

4.11. Zakonczenie konfiguracji ochrony produktu AVG



System**AVG 9.0 File Server** zostal skonfigurowany.

W tym oknie dialogowym nalezy wskazac, czy informacje o znalezionych zagrozeniach i szkodliwych witrynach maja byc anonimowo przesylane do laboratorium wirusów AVG. Jesli tak, nalezy zaznaczyc opcje ***Zgadzam sie dostarczac ANONIMOWE informacje o wykrytych zagrozeniach, aby podniesc swój poziom ochrony***.

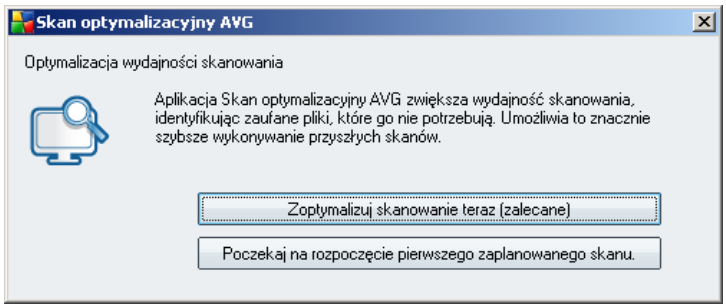
Na koniec nalezy wcisnac przycisk ***Zakoncz.***

5. Po instalacji

5.1. Optymalizacja skanowania

Funkcja optymalizacji skanowania przeszukuje foldery *Windows* i *Program Files*w poszukiwaniu odpowiednich plików (*obecnie sa to pliki *.exe, *.dll i *.sys*) i zapisuje informacje o nich. Przy kolejnych próbach uzyskania dostepu do nich, nie beda one wiecej skanowane, dzieki czemu czas przyszlych testów ulegnie znacznemu skróceniu.

Po zakonczeniu procesu instalacji zostanie wyswietlone nowe okno dialogowe z opcja optymalizacji skanowania:



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

5.2. Rejestracja produktu

Po ukonczeniu instalacji systemu **AVG 9.0 File Server** nalezy zarejestrowac produkt online na stronie internetowej AVG (http://www.avg.com) w sekcji ***Rejestracja*** (*postepujac zgodnie z wyswietlanymi tam instrukcjami*). Rejestracja umozliwia pelny dostep do konta uzytkownika AVG, biuletynu aktualizacji AVG i innych uslug oferowanych wylacznie zarejestrowanym klientom.

5.3. Dostep do Interfejsu uzytkownika

Dostep do ***interfejsu uzytkownika AVG*** mozna uzyskac na kilka sposobów:

- klikajac dwukrotnie ikone AVG na pasku zadan,
- klikajac dwukrotnie ikone AVG na pulpicie,

- z poziomu menu ***Start/Programy/AVG 9.0/Interfejs uzytkownika AVG.***

5.4. Skanowanie calego komputera

Istnieje pewne ryzyko, ze wirus dostal sie do komputera przed zainstalowaniem systemu **AVG 9.0 File Server**. Z tego powodu nalezy uruchomic test ***Skan calego komputera***, aby upewnic sie, ze jest on w pelni bezpieczny.

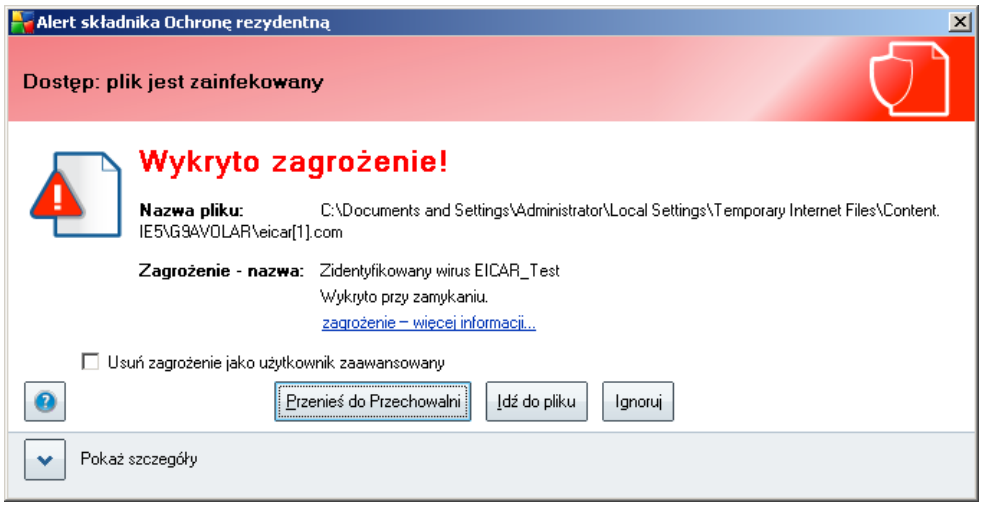
Instrukcje dotyczace uruchamiania testu ***Skan calego komputera*** zawiera rozdzial ***Skanowanie AVG***.

5.5. Test Eicar

Aby potwierdzic, ze system **AVG 9.0 File Server** zostal zainstalowany poprawnie, mozna przeprowadzic test EICAR.

Test EICAR jest standardowa i calkowicie bezpieczna metoda sluzaca do sprawdzania prawidlowosci dzialania systemu antywirusowego. Mozna go bezpiecznie rozpowszechniac, poniewaz nie jest prawdziwym wirusem i nie zawiera zadnych fragmentów zlosliwego kodu. Wiekszosc produktów rozpoznaje go jako wirusa (*chociaz zwykle zglasza go pod jednoznaczna nazwa, np. „EICAR-AV-Test”*). Wirusa EICAR mozna pobrac z witryny stowarzyszenia EICAR, dostepnej pod adresem www.eicar.com . Mozna tam równiez znalezc wszystkie niezbedne informacje na temat testu EICAR.

Spróbuj pobrac plik ***eicar.com*** i zapisac go na dysku twardym komputera. Natychmiast po zatwierdzeniu pobierania pliku testowego, ***Ochrona Rezydentna*** ***zareaguje wyswietleniem ostrzezenia.*** Pojawienie sie komunikatu ***Ochrony rezydentnej*** potwierdza, ze oprogramowanie AVG jest prawidlowo zainstalowane na komputerze.



Jesli system AVG nie rozpozna pliku testowego EICAR jako wirusa, nalezy ponownie sprawdzic jego konfiguracje!

5.6. Konfiguracja domyslna AVG

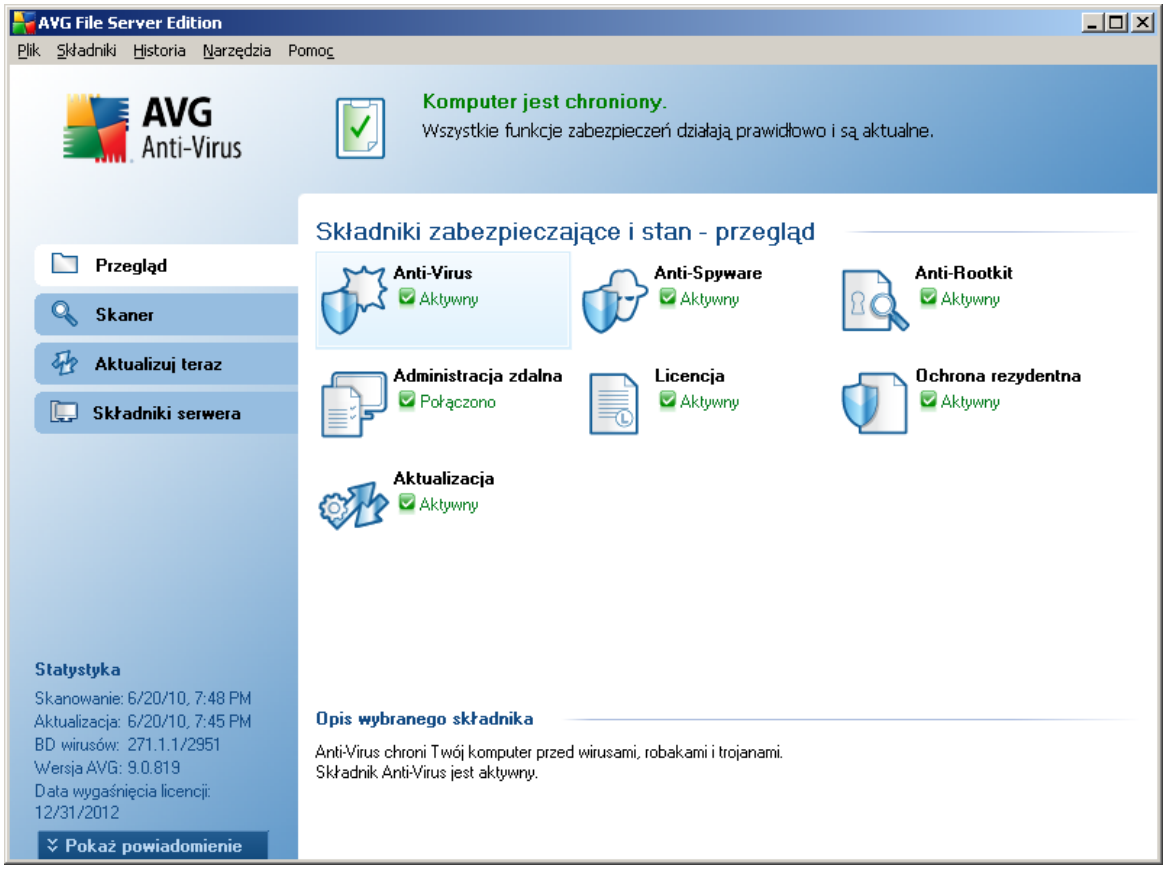
Konfiguracja domyslna (*ustawienia stosowane zaraz po instalacji*) systemu **AVG 9.0 File Server** jest wstepnie definiowana przez producenta i ma na celu zapewnienie optymalnej wydajnosci wszystkich skladników oraz funkcji.

Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach! Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników.

Mniejsze zmiany ustawien skladników AVG mozna wprowadzac bezposrednio z ich interfejsu uzytkownika. Jesli konfiguracja systemu AVG powinna zostac lepiej dopasowana do potrzeb, nalezy uzyc ***zaawansowanych ustawien AVG***, wybierajac z menu systemowego pozycje ***Narzedzia/Ustawienia zaawansowane*** i edytujac opcje w otwartym oknie dialogowym ***AVG - Ustawienia zaawansowane***.

6. Interfejs uzytkownika AVG

Otwarcie systemu **AVG 9.0 File Server** nastepuje w jego oknie glównym:



Główne okno Interfejsu Uzytkownika AVG jest podzielone na kilka sekcji:

- ***Menu glówne*** *(górny wiersz okna)* to standardowe narzedzie nawigacyjne umozliwiajace dostep do wszystkich skladników, uslug i funkcji programu AVG - szczegóły >>
- ***Informacje o stanie bezpieczenstwa*** *(prawa czesc górnej sekcji okna)* zawiera informacje dotyczace biezacego stanu programu AVG - szczegóły >>
- ***Szybkie linki*** *(lewa kolumna)* umozliwiaja uzyskanie szybkiego dostepu najwazniejszych i najczesciej uzywanych funkcji programu AVG - szczegóły >>

- ***Przeglad skladników*** *(centralna czesc okna)* zawiera przeglad zainstalowanych skladników programu AVG - szczegóły >>

- ***Statystyka*** *(lewa dolna sekcja okna)* zawiera najwazniejsze dane statystyczne dotyczace dzialania programu - szczegóły >>

- ***Ikona na pasku zadan*** *(prawy dolny róg ekranu, na pasku systemowym)* sygnalizuje biezacy stan programu AVG - szczegóły >>

6.1. Menu systemowe

Menu systemowe to standardowa metoda nawigacji we wszystkich aplikacjach w systemie Windows. Jest polozone poziomo w górnej czesci glównego okna systemu **AVG 9.0 File Server**. Menu systemowe zapewnia dostep do poszczególnych skladników AVG, funkcji i uslug.

Menu systemowe jest podzielone na piec sekcji:

6.1.1. Plik

- ***Zakoncz*** - powoduje zamkniecie **AVG 9.0 File Server**interfejsu uzytkownika. System AVG dziala jednak w tle, a komputer jest nadal chroniony!

6.1.2. Skladniki

Pozycja ***Skladniki*** w menu glównym zawiera linki do wszystkich zainstalowanych skladników AVG; kliknieciе któregos z nich powoduje otwarcie domyslnego okna interfejsu odpowiedniego skladnika:

- ***Przeglad systemu*** - pozwala przelaczyc widok do domyslnego okna Interfejsu uzytkownika AVG, zawierajacego przeglad zainstalowanych skladników.

- ***Skladniki serwera*** - pozwala przelaczyc do domyslnego okna dialogowego interfejsu uzytkownika, zawierajacego przeglad zainstalowanych skladników wraz z ich stanem.

- ***Anti-Virus*** - otwiera domyslne okno interfejsu skladnika ***Anti-Virus***.

- ***Anti-Rootkit*** - otwiera domyslne okno interfejsu skladnika ***Anti-Rootkit***.

- ***Anti-Spyware*** - otwiera domyslne okno interfejsu skladnika ***Anti-Spyware***.

- ***Administracja zdalna*** - otwiera domyslne okno skladnika ***Administracja zdalna*** (skladnik ten laczy system AVG z Administracja zdalna AVG, pozwalajac administratorowi sieci na zdalne zarzadzanie aplikacjami klienckimi). Skladnik

Administracja zdalna bedzie dostepny tylko, jesli wybrano jego instalacje w kroku ***Wybór skladników****.

- ***SharePoint*** - otwiera domyslne okno skladnika ***Skaner dokumentów dla MS SharePoint***.
- ***Licencja*** - otwiera domyslne okno interfejsu skladnika ***Licencja***.
- ***Ochrona rezydentna*** - otwiera domyslne okno interfejsu skladnika ***Ochrona rezydentna***.
- ***Menedzer aktualizacji*** - otwiera domyslne okno interfejsu ***Menedzera aktualizacji***.

6.1.3. Historia

- ***Wyniki skanowania*** - przelacza do interfejsu skanera AVG, konkretnie do okna dialogowego ***Przeglad wyników skanowania***
- ***Zagrozenia wykryte przez Ochrone rezydentna*** - otwiera okno dialogowe zawierajace przeglad zagrozen wykrytych przez skladnik ***Ochrona rezydentna***
- ***Przechowalnia wirusów*** - powoduje otwarcie interfejsu ***Przechowalni wirusów***, do której program AVG przenosi wszystkie niemozliwe do wyleczenia infekcje. W czasie tej kwarantanny zainfekowane pliki sa izolowane i nie zagrazaja bezpieczenstwu komputera, a jednoczesnie istnieje mozliwosc ich naprawy w przyszlosci.
- ***Dziennik historii zdarzen*** - powoduje otwarcie interfejsu dziennika historii z przegladem wszystkich zarejestrowanych akcji **AVG 9.0 File Server** .

6.1.4. Narzedzia

- ***Skanuj komputer*** - przelacza do Interfejsu skanera AVGi uruchamia skanowanie calego komputera
- ***Skanuj wybrany folder*** - przelacza do Interfejsu skanera AVGi umozliwia zdefiniowanie (w ramach struktury katalogów i dysków) plików oraz folderów, które maja byc przeskanowane
- ***Skanuj plik*** umozliwia uruchomienie na zadanie testu pojedynczego pliku wybranego z drzewa katalogów.
- ***Aktualizuj*** automatycznie uruchamia proces aktualizacji systemu **AVG 9.0 File Server**

- ***Aktualizuj z katalogu*** - uruchamia proces aktualizacji korzystajac z pliku zlokalizowanego w okreslonym folderze na dysku lokalnym. Jednak ta opcja jest zalecana do uzytku jedynie w sytuacjach awaryjnych, np. gdy nie ma polaczenia z internetem (*komputer zostal zainfekowany i odlaczony od internetu, komputer jest podlaczony do sieci bez dostepu do internetu itp.*). W nowo otwartym oknie nalezy wskazac folder, w którym zostal wczesniej umieszczony plik aktualizacyjny i uruchomic proces.

- ***Ustawienia zaawansowane*** otwiera okno dialogowe ***AVG - Ustawienia zaawansowane***, w którym mozna edytowac konfiguracje systemu **AVG 9.0 File Server**. Na ogól zaleca sie zachowanie domyslnych ustawien zdefiniowanych przez producenta oprogramowania AVG.

6.1.5. Pomoc

- ***Spis tresci*** - otwiera pliki pomocy systemu AVG.

- ***Uzyskaj pomoc online*** - otwiera witryne firmy AVG (http://www.avg.com) na stronie centrum pomocy technicznej dla klientów.

- ***Strona Mój AVG*** - otwiera witryne systemu AVG (http://www.avg.com).

- ***Informacje o wirusach i zagrozeniach*** - powoduje otwarcie ***Encyklopedii Wirusów*** online, w której znalezc mozna szczególowe informacje na temat znanych wirusów.

- ***Pobierz program AVG Rescue CD*** - otwiera w przegladarce internetowej witryne AVG ***Pomoc techniczna/Pobierz***. W odpowiednim polu tekstowym wprowadz numer licencji i pobierz najnowsza wersje programu AVG Rescue CD (*czyli przenosna wersje systemu AVG przeznaczona do naprawy systemów operacyjnych, które nie moga byc uruchomione w normalny sposób, np. z powodu infekcji wirusowej*).

- ***Aktywuj ponownie*** - otwiera okno ***Aktywacja programu AVG*** zawierajace dane wprowadzone na etapie ***personalizacja programu AVG*** (podczas procesu instalacji). W oknie tym mozna wprowadzic numer licencji w celu zastapienia numeru sprzedazy (*uzytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przyklad podczas uaktualnienia do nowej wersji produktu AVG*).

- ***Zarejestruj teraz*** - jest linkiem do strony rejestracji w witrynie systemu AVG (http://www.avg.com). Nalezy tam podac swoje dane rejestracyjne - jedynie klientom, którzy zarejestrowali swój produkt AVG, przysluguje bezplatna pomoc techniczna.

- ***AVG - informacje*** - otwiera okno dialogowe ***Informacje***. Okno to sklada sie z pieciu kart zawierajacych informacje na temat nazwy programu, wersji silnika antywirusowego i jego bazy danych, systemu, umowy licencyjnej oraz danych kontaktowych firmy ***AVG Technologies CZ***.

6.2. Status bezpieczenstwa

Sekcja ***Informacje o stanie bezpieczenstwa*** znajduje sie w górnej czesci Interfejsu uzytkownika AVG. Znajdziesz tam informacje o biezacym stanie bezpieczenstwa systemu **AVG 9.0 File Server**. W obszarze tym moga byc wyswietlane nastepujace ikony:

 Ikona zielona oznacza, ze system AVG jest w pelni funkcjonalny. Komputer jest calkowicie chroniony, bazy danych sa aktualne, a wszystkie zainstalowane skladniki dzialaja prawidlowo.

 Ikona pomaranczowa oznacza, ze co najmniej jeden skladnik jest nieprawidlowo skonfigurowany; nalezy sprawdzic jego wlasciwosci i ustawienia. W systemie AVG nie wystapil jednak zaden problem krytyczny, a uzytkownik prawdopodobnie wylaczyl tylko z jakiegos powodu jeden lub wiecej skladników. System AVG nadal chroni komputer, nalezy jednak sprawdzic ustawienia skladnika, który zglasza problem. Jego nazwa jest wyswietlana w sekcji ***Informacje o stanie bezpieczenstwa***.

Ikona ta jest takze wyswietlana, gdy z jakiegos powodu stan bledu skladników ma byc ignorowany (*opcja "Ignoruj stan skladnika" jest dostepna po kliknieciu prawym przyciskiem ikony odpowiedniego skladnika w głównej sekcji okna AVG*). W pewnych sytuacjach uzycie tej opcji moze byc pomocne, jednak nie nalezy jej naduzywac.

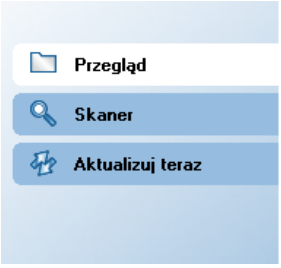
 Ikona czerwona oznacza, ze stan systemu AVG jest krytyczny! Jeden lub wiecej skladników nie dziala, a system AVG nie moze chronic komputera. Nalezy natychmiast usunac zgloszony problem. Jesli nie jest to mozliwe, nalezy skontaktowac sie z zespolem Pomocy Technicznej AVG.

Stanowczo zaleca sie reagowanie na zmiany ***Statusu Bezpieczenstwa*** i natychmiastowe rozwiazywanie ewentualnych problemów. Brak reakcji naraza komputer na powazne zagrozenia!

Uwaga: *Dostep do informacji o stanie systemu AVG zapewnia przez caly czas również ikona na pasku zadan.*

6.3. Linki

Szybkie linki *(z lewej strony interfejsu uzytkownika AVG)* pozwalaja natychmiast uzyskiwac dostep do najwazniejszych i najczesciej uzywanych funkcji systemu AVG:



- ***Przeglad*** - pozwala przelaczac miedzy biezacym interfejsem AVG a interfejsem domyslnym, zawierajacym przeglad wszystkich zainstalowanych skladników - zobacz rozdzial ***Przeglad skladników >>***
- ***Skaner*** - otwiera interfejs skanowania AVG, w którym mozna uruchamiac test, planowac skany i edytowac ich parametry (zobacz rozdzial ***Skanowanie AVG >>***
- ***Aktualizuj teraz*** - otwiera odpowiedni interfejs i uruchamia proces aktualizacji systemu AVG (zobacz rozdzial ***Aktualizacje AVG >>***
- ***Skladniki serwera*** - pozwala przelaczac miedzy biezacym interfejsem AVG a interfejsem domyslnym, zawierajacym przeglad wszystkich skladników serwera. Zobacz rozdzial ***Skladniki serwera***

Linki te sa dostepne przez caly czas. Klikniecie jednego z nich w celu uruchomienia okreslonego procesu powoduje wyswietlenie innego okna dialogowego, ale sama sekcja linków nie ulegnie zmianie.

6.4. Przeglad skladników

Sekcja ***Przeglad skladników*** znajduje sie w srodkowej czesci interfejsu uzytkownika AVG. Obszar ten podzielony jest na dwie czesci:

- Przeglad wszystkich zainstalowanych skladników (panel z odpowiednimi ikonami oraz informacjami o tym, czy dany skladnik jest aktywny, czy nie)
- Opis wybranego skladnika.

Sekcja **Przeglad skladników** systemu ***AVG 9.0 File Server*** zawiera informacje o nastepujacych skladnikach:

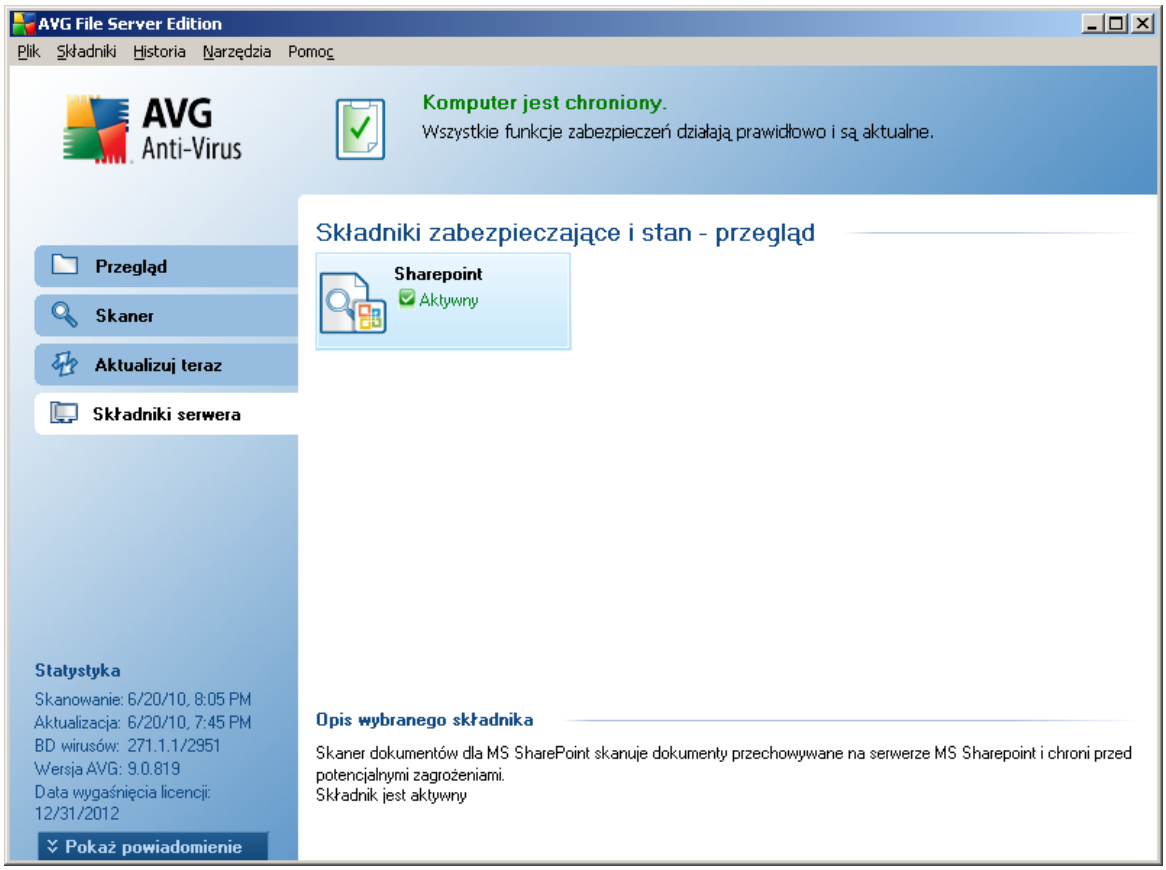
- ***Anti-Virus*** - zapewnia ochrone przed wirusami, które moga zainfekowac komputer - szczegóły >>
- ***Anti-Spyware*** - skanuje uruchamiane aplikacje w tle - szczegóły >>
- ***Administracja zdalna*** - laczy system AVG z Administracja zdalna AVG, pozwalajac administratorowi na zdalne wywolywanie pewnych akcji aplikacji. Skladnik Administracja zdalna bedzie dostepny tylko, jesli wybrano jego instalacje w kroku ***Wybór skladników****.
- ***Anti-Rootkit*** - wykrywa programy i technologie próbujace ukryc w systemie szkodliwe oprogramowanie - szczegóły >>

- ***Licencja*** - zawiera pelna tresc umowy licencyjnej AVG - szczegóły >>
- ***Ochrona rezydentna*** - dziala w tle; skanuje pliki przy ich kopiowaniu, otwieraniu i zapisywaniu - szczegóły >>
- ***Menedzer aktualizacji*** - kontroluje wszystkie aktualizacje systemu AVG - szczegóły >>

Pojedyncze klikniecie ikony dowolnego skladnika powoduje podswietlenie go w sekcji przegladu. Jednoczesnie u dolu interfejsu uzytkownika pojawia sie opis funkcji wybranego skladnika. Dwukrotne klikniecie ikony powoduje otwarcie interfejsu konkretnego skladnika (z jego opcjami i statystykami).

Klikniecie prawym przyciskiem ikony skladnika powoduje otwarcie menu kontekstowego. Mozna w nim nie tylko otworzyc graficzny interfejs skladnika, ale takze wybrac opcje ***Ignoruj stan skladnika***. Opcji tej nalezy uzyc, jesli stan bledu skladnika jest znany, ale z pewnego powodu system AVG ma byc nadal uzywany, a uzytkownik nie ma byc ostrzegany za pomoca ikony na pasku zadan.

6.5. Skladniki serwera



Sekcja ***Skladniki serwera*** znajduje sie w srodkowej czesci Interfejsu uzytkownika AVG . Obszar ten podzielony jest na dwie czesci:

- Przeglad wszystkich zainstalowanych skladników (panel z odpowiednimi ikonami oraz informacjami o tym, czy dany skladnik jest aktywny, czy nie)
- Opis wybranego skladnika.

Sekcja **Skladniki serwera** systemu ***AVG 9.0 File Server*** zawiera informacje o nastepujacych skladnikach:

- ***Skaner dokumentów dla MS SharePoint*** skanuje dokumenty na serwerze MS SharePoint i chroni je przed zagrozeniami - szczegóły >>

Pojedyncze klikniecie ikony dowolnego skladnika powoduje podswietlenie go w sekcji

przegladu. Jednoczesnie u dolu interfejsu uzytkownika pojawia sie opis funkcji wybranego skladnika. Dwukrotne klikniecie ikony powoduje otwarcie interfejsu konkretnego skladnika (z jego opcjami i statystykami).

Klikniecie prawym przyciskiem ikony skladnika powoduje otwarcie menu kontekstowego. Mozna w nim nie tylko otworzyc graficzny interfejs skladnika, ale takze wybrac opcje ***Ignoruj stan skladnika***. Opcji tej nalezy uzyc, jesli stan bledu skladnika jest znany, ale z pewnego powodu system AVG ma byc nadal uzywany, a uzytkownik nie ma byc ostrzegany za pomoca ikony na pasku zadan.

6.6. Statystyki

Obszar·***Statystyki*** znajduje sie w lewym dolnym rogu Interfejsu uzytkownika AVG. Sekcja ta zawiera szereg informacji o dzialaniu programu:

- ***Skanowanie*** - data ostatniego przeprowadzonego testu.
- ***Aktualizacja*** - data uruchomienia ostatniej aktualizacji.
- ***BD wirusów*** - aktualnie uzywana wersja bazy wirusów.
- ***Wersja AVG*** - zainstalowana wersja systemu AVG *(numer w formacie 9.0.xx, gdzie 9.0 to wersja linii produktów, a xx - numer kompilacji).*
- ***Data wygasniecia licencji*** - data wygasniecia licencji systemu AVG.

6.7. Ikona na pasku zadan

Ikona AVG (*na pasku zadan systemu Windows*) wskazuje obecny stan systemu **AVG 9.0 File Server**. Ikona ta jest zawsze widoczna, niezaleznie od tego, czy Interfejs uzytkownika AVG jest otwarty, czy tez nie.

Jesli , ***ikona na pasku zadan*** jest kolorowa, wszystkie skladniki systemu AVG sa aktywne i w pelni funkcjonalne. Moze ona byc kolorowa takze wtedy, gdy system AVG zasygnalizowal bledy, ale uzytkownik akceptuje je i celowo ***ignoruje stan skladników*** .

Ikona z wykrzyknikiem wskazuje problem (*nieaktywny skladnik, stan bledu itp.*). W takim przypadku nalezy dwukrotnie kliknac ***ikone AVG***, aby otworzyc Interfejs uzytkownika i sprawdzic stan skladników.

Ikona na pasku zadan dostarcza równiez informacji na temat biezacych dzialan systemu AVG i mozliwych zmian w programie (*np. uruchomienia automatycznego, zaplanowanego skanowania lub aktualizacji, zmiany stanu skladników, bledu itp.*) w

wyskakujacym okienku:

Dwukrotne klikniecie ***ikony na pasku zadan*** pozwala takze szybko, w dowolnym momencie uzyskac dostep do Interfejsu uzytkownika systemu AVG. Klikniecie ***ikony na pasku zadan*** prawym przyciskiem myszy otwiera menu kontekstowe zawierajace nastepujace opcje:

- ***Otwórz Interfejs uzytkownika AVG*** - otwiera Interfejs uzytkownika.
- ***Skany*** - kliknij, aby otworzyc menu kontekstowe wstepnie zdefiniowanych skanów (*Skan calego komputera*, *Skan okreslonych plików lub folderów*, *Skan Anti-Rootkit*) i wybierz zadany skan. Zostanie on uruchomiony natychmiast.
- ***Aktualizuj teraz*** - uruchamia natychmiastowa aktualizacje.
- ***Pomoc*** - otwiera plik pomocy na stronie startowej.

7. Skladniki AVG

7.1. Anti-Virus

7.1.1. Zasady dzialania skladnika Anti-Virus

Silnik skanujacy programu antywirusowego skanuje wszystkie pliki i wykonywane na nich operacje (otwieranie, zamykanie itd.) w poszukiwaniu znanych wirusów. Kazdy wykryty wirus jest blokowany (aby nie mógl wykonywac zadnych szkodliwych dzialan), a nastepnie usuwany lub izolowany. Wiekszosc programów antywirusowych korzysta takze z analizy heurystycznej - pliki sa skanowane w poszukiwaniu charakterystycznych cech wirusów - tak zwanych sygnatur. Oznacza to, ze skaner antywirusowy moze wykryc nowe, nieznane dotad wirusy, jesli posiadaja one pewne popularne wlasciwosci.

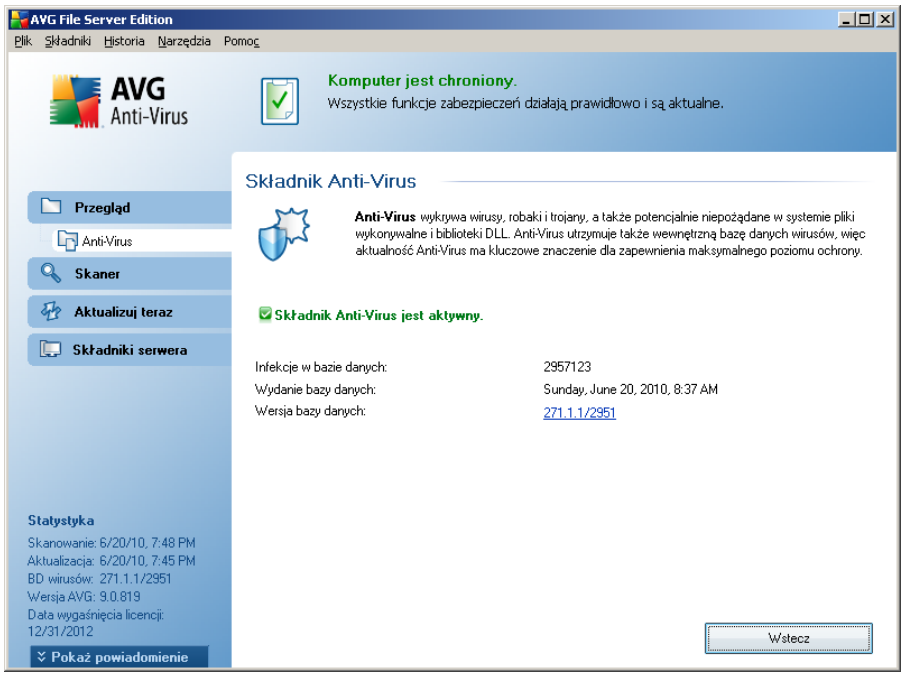
Wazna zaleta ochrony antywirusowej jest fakt, ze nie pozwala ona na uruchomienie zadnych znanych wirusów na komputerze!

Korzystanie z tylko jednej technologii nie zapewnia stuprocentowej skutecznosci wykrywania wirusów, dlatego skladnik ***Anti-Virus*** wykorzystuje jednoczesnie kilka metod:

- Skanowanie - wyszukiwanie ciagów bajtów typowych dla danego wirusa.
- Analiza heurystyczna - dynamiczna emulacja kodu skanowanego obiektu w srodowisku maszyny wirtualnej.
- Wykrywanie generyczne - wykrywanie instrukcji typowych dla danego wirusa lub grupy wirusów.

Program AVG jest równiez w stanie analizowac i wykrywac wykonywalne aplikacje i biblioteki DLL, które moga byc potencjalne niepozadane w Twoim systemie. Takie zagrozenia (rózne rodzaje oprogramowania szpiegujacego, reklamowego itp.) nazywane sa równiez Potencjalnie Niechcianymi Programami. Ponadto program AVG skanuje rejestr systemu w poszukiwaniu podejrzanych wpisów, a takze monitoruje tymczasowe pliki internetowe i sledzace pliki cookie. Umozliwia to traktowanie wszystkich potencjalnie szkodliwych obiektów w ten sam sposób jak infekcji.

7.1.2. Interfejs skladnika Anti-Virus



Interfejs skladnika ***Anti-Virus*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (Skladnik *Anti-Virus jest aktywny.*), a takze krótki przeglad statystyk:

- ***Infekcje w bazie danych*** - liczba wirusów zdefiniowanych w najnowszej wersji bazy danych.
- ***Ostatnia aktualizacja bazy danych*** - data i godzina ostatniej aktualizacji bazy wirusów.
- ***Wersja bazy danych*** - numer ostatniej wersji bazy danych; numer ten rosnie przy kazdej aktualizacji.

Interfejs tego skladnika zawiera tylko jeden przycisk (***Wstecz***) - klikniecie go powoduje powrót do domyslnego interfejsu uzytkownika systemu AVG (przegladu skladników).

Uwaga: *Dostawca oprogramowania AVG skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu glównego****Narzedzia / Ustawienia zaawansowane*** *i*

skorzystac z interfejsu AVG - Ustawienia zaawansowane.

7.2. Anti-Spyware

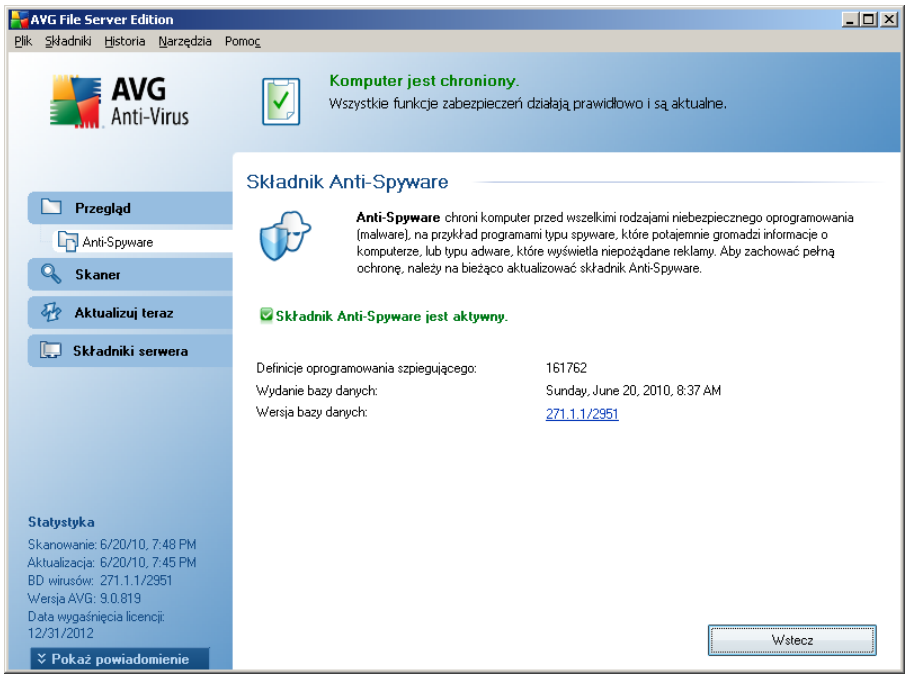
7.2.1. Zasady dzialania skladnika Anti-Spyware

Oprogramowanie szpiegujace (spyware) jest zazwyczaj definiowane jako pewien rodzaj szkodliwego oprogramowania, które gromadzi informacje z komputera uzytkownika bez jego wiedzy i pozwolenia. Niektóre aplikacje szpiegujace moga byc instalowane celowo i czesto zawieraja reklamy, wyskakujace okna i inne nieprzyjemne elementy.

Obecnie zródlem wiekszosci infekcji sa potencjalnie niebezpieczne witryny internetowe. Powszechne sa równiez inne metody rozprzestrzeniania, na przyklad poprzez e-mail lub w efekcie dzialalnosci robaków i wirusów. Najskuteczniejsza ochrona jest stosowanie stale pracujacego w tle skladnika ***Anti-Spyware***, który dziala jak ochrona rezydentna i skanuje aplikacje podczas ich uruchamiania.

Istnieje jednak ryzyko, ze szkodliwe oprogramowanie znalazlo sie na komputerze przed zainstalowaniem systemu **AVG 9.0 File Server**, lub ze uzytkownik zaniedbal jego aktualizacje, nie korzystajac z aktualnych baz wirusów i nowych wersji programu. Z tego powodu AVG umozliwia pelne przeskanowanie komputera pod katem obecnosci oprogramowania szpiegujacego (za pomoca interfejsu skanera). Wykrywa on równiez szkodliwe oprogramowanie, które jest uspione lub nie stwarza zagrozenia, czyli takie, które zostalo pobrane, ale nie aktywowane.

7.2.2. Interfejs skladnika Anti-Spyware



Interfejs skladnika ***Anti-Spyware*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (Skladnik *Anti-Spyware jest aktywny.*), oraz statystyki:

- ***Definicje oprogramowania szpiegujacego*** - liczba sygnatur programów typu spyware zdefiniowanych w najnowszej wersji bazy danych.
- ***Ostatnia aktualizacja bazy danych*** - data i godzina ostatniej aktualizacji.
- ***Wersja bazy danych*** - numer ostatniej wersji bazy danych; numer ten rosnie przy kazdej aktualizacji.

Interfejs uzytkownika tego skladnika zawiera tylko jeden przycisk - ***Wstecz***) - klikniecie go spowoduje powrót do domyslnego interfejsu uzytkownika systemu AVG (przegladu skladników).

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu AVG - Ustawienia zaawansowane.*

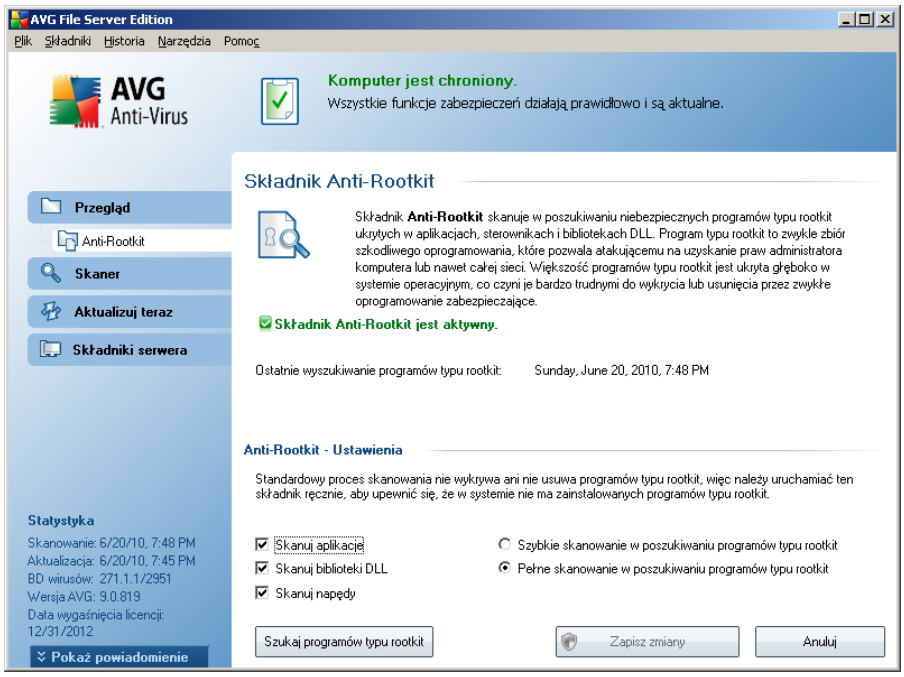
7.3. Anti-Rootkit

Program typu rootkit to aplikacja zaprojektowana w celu przejecia calkowitej kontroli nad systemem komputerowym bez zgody jego wlascicieli czy upowaznionych administratorów. Bezposredni dostep do sprzetu jest rzadko wymagany, poniewaz programy typu rootkit w pelni zdalnie kontroluja system operacyjny komputera. Zwykle ukrywaja one swoja obecnosc mylac lub unikajac standardowych mechanizmów bezpieczenstwa systemu operacyjnego. Wiele z nich jest jednoczesnie konmi trojanskimi, które dodatkowo staraja sie przekonac uzytkowników, ze ich systemy sa bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorujacymi) oraz plików lub danych przed samym systemem operacyjnym.

7.3.1. Zasady dzialania skladnika Anti-Rootkit

AVG Anti-Rootkit to specjalistyczne narzedzie do wykrywania i skutecznego usuwania niebezpiecznych programów typu rootkit, wykorzystujacych technologie, które moga kamuflowac obecnosc innego szkodliwego oprogramowania na komputerze. Skladnik ***AVG Anti-Rootkit*** umozliwia wykrywanie programów typu rootkit na podstawie wstepnie zdefiniowanego zestawu regul. Nalezy zwrócic uwage na fakt, ze wykrywane sa wszystkie programy typu rootkit (*nie tylko te szkodliwe*). Jesli skladnik ***AVG Anti-Rootkit*** wykrywa program typu rootkit, nie znaczy to jeszcze, ze ten program jest szkodliwy. Niekiedy programy typu rootkit sa uzywane jako sterowniki lub jako komponenty innych, pozytecznych aplikacji.

7.3.2. Interfejs skladnika Anti-Rootkit



Interfejs skladnika ***Anti-Rootkit*** zawiera krótki opis jego funkcji, informacje o biezacym stanie (*Skladnik Anti-Rootkit jest aktywny*) oraz date ostatniego uruchomienia testu ***Anti-Rootkit***.

W dolnej czesci okna znajduje sie sekcja ***ustawien skladnika Anti-Rootkit***, w której skonfigurowac mozna podstawowe funkcje skanowania w poszukiwaniu programów typu rootkit. Po pierwsze: nalezy zaznaczyc odpowiednie pola, aby okreslic obiekty, które maja byc skanowane:

- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj sterowniki***

Nastepnie nalezy wybrac tryb skanowania rootkitów:

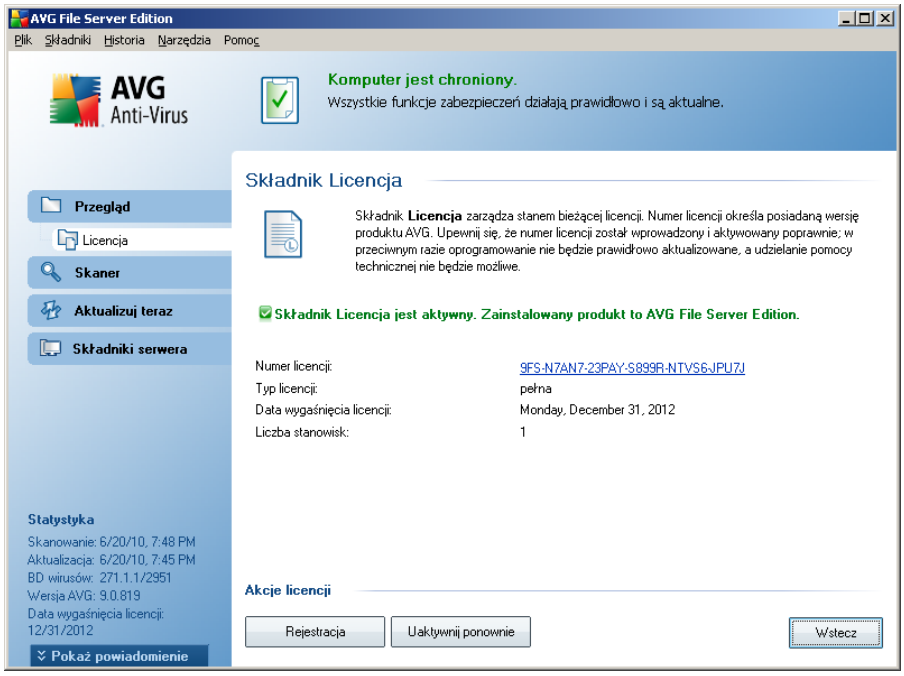
- ***Szybkie skanowanie w poszukiwaniu programów typu rootkit*** - skanowany jest tylko folder systemowy (*zwykle C:\Windows*).
- ***Pelne skanowanie w poszukiwaniu programów typu rootkit*** - skanowane

sa wszystkie dostepne dyski, oprócz A: i B:.

Dostepne sa nastepujace przyciski kontrolne:

- ***Szukaj programów typu rootkit*** - poniewaz skanowanie w poszukiwaniu programów typu rootkit nie jest czescia testu ***Skan calego komputera***, mozna je uruchomic bezposrednio z Interfejsu skladnika ***Anti-Rootkit***, klikajac ten przycisk.
- ***Zapisz zmiany*** - pozwala zapisac wszystkie zmiany wprowadzone w danym oknie i powrócic do domyslnego ***interfejsu uzytkownika AVG*** (przegladu skladników).
- ***Anuluj*** - pozwala powrócic do domyslnego ***interfejsu uzytkownika AVG*** (przegladu skladników) bez zapisywania wprowadzonych zmian.

7.4. Licencja



Okno dialogowe skladnika ***Licencja*** zawiera krótki opis jego funkcji, informacje o jego biezacym stanie (Skladnik Licencja *jest aktywny.*), a takze nastepujace informacje:

- ***Numer licencji*** - dokladny numer licencji. Jezeli kiedykolwiek bedziesz

proszony o podanie swojego numeru licencji, uzyj go w tej samej formie. Dlatego tez zdecydowanie zalecamy korzystanie z metody kopiuj-wklej w przypadku jakiejkolwiek manipulacji numerem licencji.

- ***Typ licencji*** - okresla typ zainstalowanego produktu.
- ***Data wygasniecia licencji*** - data okreslajaca okres waznosci licencji. Aby korzystac z systemu **AVG 9.0 File Server** po tej dacie, nalezy odnowic licencje. Licencje mozna odnowic online za posrednictwem witryny firmy AVG (http://www.avg.com).
- ***Liczba stanowisk*** - liczba stacji roboczych, na których mozna zainstalowac system **AVG 9.0 File Server**.

Przyciski kontrolne

- ***Zarejestruj*** - laczy sie ze strona rejestracji w witrynie internetowej systemu AVG (http://www.avg.com). Nalezy tam podac swoje dane rejestracyjne - jedynie klientom, którzy zarejestrowali swój produkt AVG, przysluguje bezplatna pomoc techniczna.
- ***Uaktywnij ponownie*** - otwiera okno dialogowe ***Aktywacja programu AVG*** zawierajace dane wprowadzone na etapie ***Personalizacji programu AVG*** podczas Instalacji. W oknie tym mozna wprowadzic numer licencji w celu zastapienia numeru sprzedazy (*uzytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przyklad podczas uaktualnienia do nowego produktu AVG*).
- ***Wstecz*** - kliknięcie tego przycisku powoduje powrót do domyslnego Interfejsu uzytkownika systemu AVG (przegladu skladników).

7.5. Ochrona rezydentna

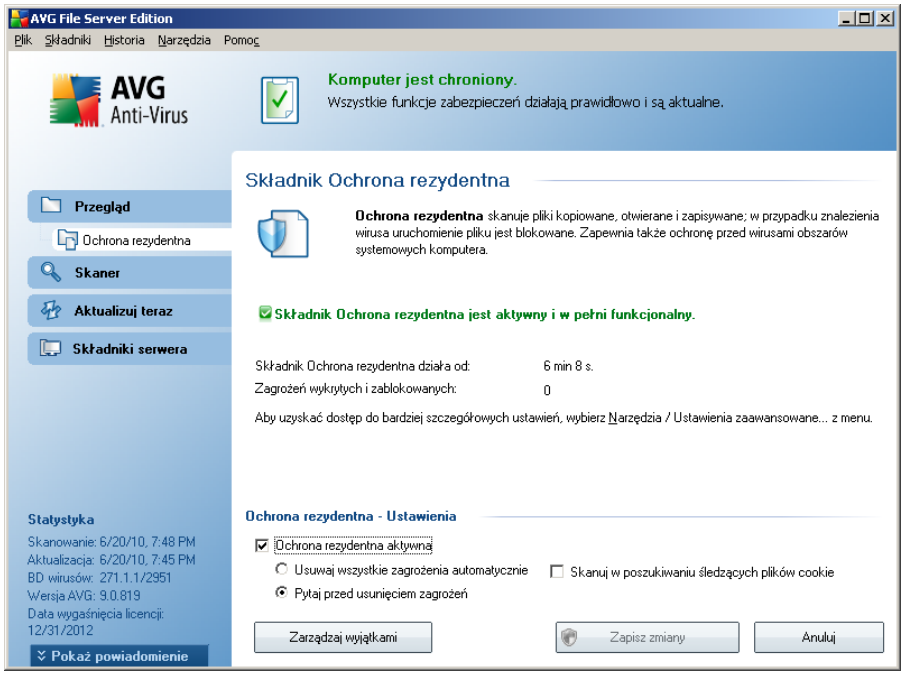
7.5.1. Zasady dzialania skladnika Ochrona rezydentna

Skladnik ***Ochrona rezydentna*** zapewnia stala ochrone komputera. Skladnik ten skanuje kazdy otwierany, zapisywany lub kopiowany plik, oraz chroni obszary systemowe komputera. Po wykryciu wirusa w przetwarzanym pliku, ***Ochrona rezydentna*** zatrzymuje aktualnie wykonywane operacje i uniemozliwia uaktywnienie sie wirusa. Uzytkownik zwykle nie zauwaza dzialania tej ochrony, poniewaz funkcjonuje ona „w tle” i wyswietla powiadomienia tylko w przypadku, gdy wykryje zagrozenie. Domyslna reakcja ***Ochrony rezydentnej*** jest zablokowanie dostepu do

niebezpiecznego pliku. Skladnik ***Ochrona rezydentna*** jest ladowany do pamieci komputera podczas uruchamiania systemu.

Ostrzezenie: Ochrona rezydentna ladowana jest do pamieci komputera podczas uruchamiania systemu i musi pozostac wlaczona przez caly czas!

7.5.2. Interfejs skladnika Ochrona rezydentna



Oprócz przegladu najwazniejszych statystyk oraz informacji na temat stanu skladnika (*skladnik Ochrona rezydentna jest aktywny i w pelni funkcjonalny*), interfejs ***Ochrony rezydentnej*** oferuje takze kilka elementarnych opcji konfiguracyjnych. Wyswietlane sa nastepujace statystyki:

- ***Ochrona rezydenta jest aktywna od*** - okresla czas, jaki uplynal od ostatniego uruchomienia skladnika.

- ***Zagrozenia wykryte i zablokowane*** - liczba wykrytych infekcji, do których uruchomienia/otwarcia nie dopuszczono (*w razie potrzeby ta wartosc moze zostac zresetowana, np. do celów statystycznych - Resetuj wartosc*)

Podstawowa konfiguracja skladnika

W dolnej czesci okna dialogowego znajduje sie sekcja o nazwie ***Ochrona rezydentna - Ustawienia*** , w której mozna edytowac niektóre jej podstawowe funkcje (*szczegółowa konfiguracja, podobnie jak w wypadku innych skladników, dostepna jest za posrednictwem menu Narzedzia/Ustawienia zaawansowane*).

Pole ***Ochrona rezydentna aktywna*** umozliwia latwe wlaczanie/wylaczanie Ochrony rezydentnej. Domyslnie funkcja ta jest wlaczona. Gdy Ochrona rezydentna jest wlaczona, mozna okreslic w jaki sposób ma reagowac na wykryte infekcje:

- automatycznie (***Usuwaj wszystkie zagrozenia automatycznie***)

- lub tylko za zgoda uzytkownika (***Pytaj przed usunieciem zagrozen***).

Wybór te nie ma wplywu na poziom bezpieczenstwa - umozliwia on jedynie podjecie kazdorazowej decyzji o usunieciu lub pozostawieniu wykrytych infekcji.

Dodatkowo mozna okreslic, czy chcesz ***automatycznie usuwac pliki cookie.*** W konkretnych wypadkach mozna wlaczyc te opcje, aby osiagnac najwyzszy poziom ochrony, ale domyslnie jest ona wylaczona. (*pliki cookie to dane tekstowe wysylane przez serwer do przegladarki, która przy nastepnych odwiedzinach na danej stronie udostepni je serwerowi w celach identyfikacyjnych. Pliki cookie sa uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach - np. preferencji dotyczacych wygladu witryny lub zawartosci koszyka w sklepach internetowych*).

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

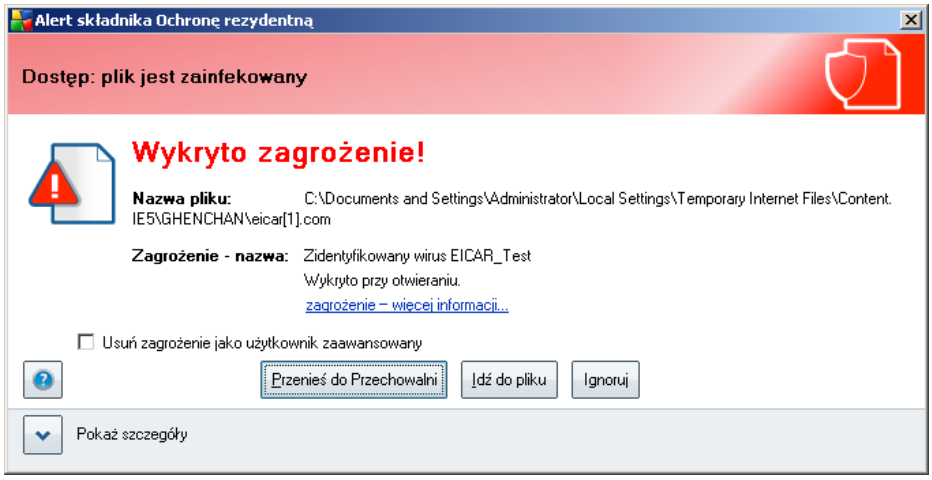
Przyciski kontrolne

W interfejsie skladnika ***Ochrona rezydentna*** dostepne sa nastepujace przyciski kontrolne:

- ***Zarzadzaj wyjatkami*** - otwiera nowe okno dialogowe, w którym mozliwe jest zdefiniowanie folderów/plików, które maja zostac wykluczone ze skanowania skladnika ***Ochrona rezydentna*** (wiecej informacji na ten temat mozna znalezc w rozdzialach ***Wykluczenia katalogów*** i/lub***Wykluczone pliki***).
- ***Zapisz zmiany*** - klikniecie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** - klikniecie tego przycisku powoduje powrót do domyslnego okna ***Interfejsu uzytkownika AVG*** (przegladu skladników).

7.5.3. Zagrozenia wykryte przez Ochrone rezydentna

Ochrona rezydentna to skladnik sluzacy do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrozenia powoduje natychmiastowe wyswietlenie nastepujacego ostrzezenia:



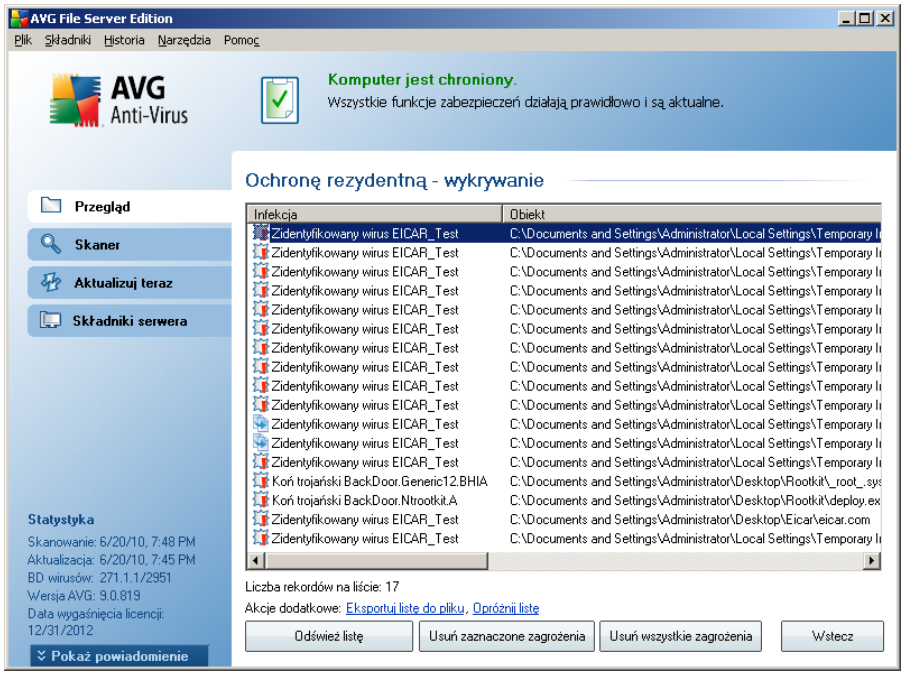
Okno to zawiera informacje dotyczace wykrytej infekcji i pozwala wybrac czynnosc, która ma zostac wykonana:

- ***Wylecz*** - jesli mozliwe jest wyleczenie pliku, system AVG zrobi to automatycznie (opcja zalecana).
- ***Przenies do Przechowalni*** - wirus zostanie przeniesiony do ***Przechowalni wirusów AVG***

- ***Przejdz do pliku*** - pozwala przejsc do lokalizacji podejrzanego obiektu (*w nowym oknie Eksploratora Windows*)

- ***Ignoruj*** - tej opcji NIE nalezy uzywac bez uzasadnionego powodu!

Przeglad wszystkich zagrozen wykrytych przez skladnik ***Ochrona rezydentna*** mozna znalezc w oknie dialogowym ***Zagrozenia wykryte przez Ochrone rezydentna*** dostepnym poprzez menu ***Historia / Zagrozenia wykryte przez Ochrone rezydentna***:



Okno ***Zagrozenia wykryte przez Ochrone rezydentna*** zawiera przeglad obiektów wykrytych i uznanych przez ten skladnik ***za niebezpieczne (które nastepnie wyleczono lub przeniesiono do ***Przechowalni wirusów***). Podawane sa tam nastepujace informacje:

- ***Infekcja***- opis (ewentualnie nazwa) wykrytego zagrozenia.

- ***Obiekt*** - lokalizacja obiektu.

- ***Wynik*** - dzialanie podjete w zwiazku z wykryciem.

- ***Czas wykrycia*** - data i godzina wykrycia obiektu.

- ***Typ obiektu*** - typ wykrytego obiektu.
- ***Proces*** - akcja wykonana w celu wywolania potencjalnie niebezpiecznego obiektu (co umozliwilo jego wykrycie).

U dolu okna znajduja sie informacje na temat lacznej liczby wykrytych infekcji. Ponadto, mozna wyeksportowac cala liste obiektów do pliku, (***Eksportuj liste do pliku***) lub usunac wszystkie jej pozycje (***Opróznij liste***). Przycisk ***Odswiez liste*** pozwala zaktualizowac liste obiektów wykrytych przez ***Ochrone rezydentna***. Przyciski ***Usun zaznaczone zagrozenia*** i ***Usun wszystkie zagrozenia*** pozwalaja przeniesc wybrane zagrozenia (lub wszystkie zagrozenia z listy) do Przechowalni wirusów. Przycisk ***Wstecz*** przelacza z powrotem do domyslnego okna ***Interfejsu uzytkownika systemu AVG*** (przegladu skladników).

7.6. Menedzer aktualizacji

7.6.1. Zasady dzialania Menedzera aktualizacji

Zadne oprogramowanie zabezpieczajace nie moze zapewnic realnej ochrony przed róznymi typami zagrozen bez regularnych aktualizacji! Twórcy wirusów nieustannie szukaja nowych luk w programach i systemach operacyjnych, które mogliby wykorzystac. Nowe wirusy, szkodliwe oprogramowanie i metody ataków pojawiaja sie kazdego dnia. Z tego powodu dostawcy oprogramowania na biezaco wydaja aktualizacje i poprawki zabezpieczen, które maja usuwac wykryte luki.

Regularne aktualizacje systemu AVG sa kluczowe dla Twojego bezpieczenstwa!

Pomaga w tym skladnik ***Menedzer aktualizacji***. Za jego pomoca mozna zaplanowac automatyczne pobieranie aktualizacji (z internetu lub sieci lokalnej). Jesli jest to mozliwe, definicje wirusów nalezy pobierac codziennie. Mniej istotne aktualizacje programu mozna pobierac co tydzien.

Uwaga: *Wiecej informacji na temat typów i poziomów aktualizacji zawiera rozdzial Aktualizacje AVG.*

7.6.2. Interfejs Menedzera aktualizacji

Interfejs skladnika·***Menedzer aktualizacji*** zawiera informacje o jego funkcjach i biezacym stanie (Skladnik *Menedzer aktualizacji jest aktywny.*), a takze istotne statystyki:

- ***Ostatnia aktualizacja*** - data i godzina ostatniej aktualizacji bazy danych.
- ***Wersja bazy danych wirusów*** - numer ostatniej wersji bazy danych wirusów; numer ten jest zwiekszany przy kazdej aktualizacji bazy danych.
- ***Nastepna zaplanowana aktualizacja*** - godzina i data kolejnej zaplanowanej aktualizacji.

Podstawowa konfiguracja skladnika

W dolnej czesci okna dialogowego znajduje sie sekcja ***ustawien Menedzera aktualizacji***, w której mozna wprowadzac zmiany regul uruchamiania procesu aktualizacji. Mozna okreslic tam, czy pliki aktualizacyjne maja byc pobierane automatycznie (***Uruchom aktualizacje automatyczne***), czy tylko na zadanie. Opcja ***Uruchom aktualizacje automatyczne*** jest wlaczona i zaleca sie pozostawienie jej w tym stanie. Regularne pobieranie najnowszych aktualizacji ma kluczowe znaczenie dla

prawidlowego funkcjonowania kazdego oprogramowania zabezpieczajacego!

Ponadto, mozna okreslic, kiedy aktualizacje maja byc uruchamiane:

- ***Okresowo*** - nalezy zdefiniowac interwal aktualizacji.
- ***O okreslonej godzinie*** - nalezy zdefiniowac dokladna date i godzine.

Domyslny interwal aktualizacji to 4 godziny. Stanowczo nie zaleca sie zmiany tych opcji bez uzasadnionej przyczyny!

Uwaga: Dostawca oprogramowania AVG *skonfigurowal wstepnie wszystkie skladniki pod katem optymalnej wydajnosci. Konfiguracje systemu AVG nalezy zmieniac tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Jesli konieczna jest zmiana konfiguracji systemu AVG, nalezy wybrac z menu głównego****Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

Przyciski kontrolne

W interfejsie skladnika ***Menedzer aktualizacji*** dostepne sa nastepujace przyciski kontrolne:

- ***Aktualizuj teraz*** - kliknicie przycisku uruchamia natychmiastowa aktualizacje na zadanie.
- ***Zapisz zmiany*** - kliknicie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** - kliknicie tego przycisku powoduje powrót do domyslnego okna ***Interfejsu uzytkownika AVG*** (przegladu skladników).

8. Skladniki serwera AVG

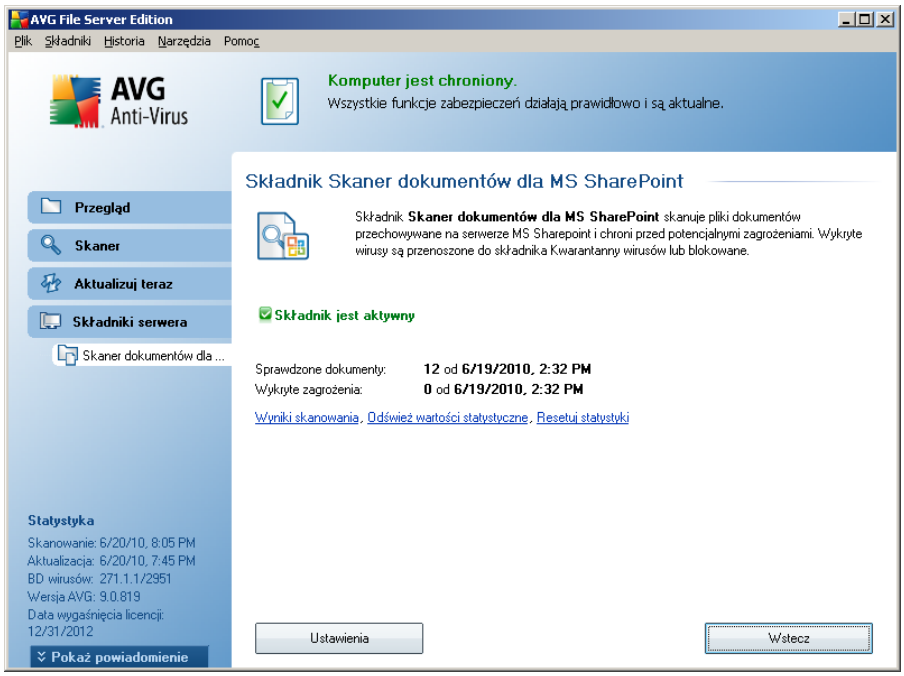
8.1. Skaner dokumentów dla MS SharePoint

8.1.1. Zasady dzialania Skanera dokumentów

Zadaniem skladnika ***Skaner dokumentów dla MS SharePoint*** jest skanowanie dokumentów przechowywanych na serwerze Microsoft SharePoint. Wszystkie wykryte wirusy sa przenoszone do Przechowalni lub usuwane.

Microsoft SharePoint to zbiór produktów obejmujacy m.in. funkcje umozliwiajace współprace poprzez przegladarke Internet Explorer, moduly zarzadzania procesami, moduly wyszukiwania i platforme zarzadzania dokumentami. SharePoint pozwala na hosting witryn WWW korzystajacych ze współdzielonych obszarów roboczych oraz magazynów danych i dokumentów.

8.1.2. Interfejs Skanera dokumentów



Poza przegladem najwazniejszych danych statystycznych i informacji o biezacym stanie skladników (*Skladnik jest aktywny*), interfejs ***Skanera dokumentów dla MS SharePoint*** zawiera krótki przeglad danych statystycznych skladnika :

- ***Sprawdzone dokumenty*** - liczba dokumentów sprawdzonych od okreslonej daty

- ***Wykryte zagrozenia*** - liczba wykrytych infekcji od okreslonej daty

Statystyki te mozna aktualizowac w dowolnym momencie, klikajac link ***Odswiez statystyki***. Nowe dane pojawia sie prawie natychmiast. Aby wyzerowac wszystkie statystyki, kliknij link ***Wyzeruj statystyki***. Link ***Wyniki skanowania*** pozwala otworzyc nowe okno dialogowe z lista wyników skanowania. Dane na liscie mozna sortowac za pomoca przycisków lub kart.

Przyciski kontrolne

W interfejsie ***Skanera poczty e-mail dla MS SharePoint***dostepne sa nastepujace przyciski kontrolne:

- ***Ustawienia*** - otwiera nowe okno dialogowe, w którym mozliwe jest dostosowanie kilku parametrów zwiazanych z wydajnoscia skanowania antywirusowego przez ***Skaner dokumentów dla MS SharePoint*** (wiecej informacji na temat tego okna dialogowego mozna znalezc w rozdzialach ***Ustawienia zaawansowane Skanera dokumentów dla MS SharePoint*** i/lub ***Akcje zwiazane z wykryciem***).

- ***Wstecz*** - ten przycisk umozliwia powrót do domyslnego ***interfejsu skladników serwera***.

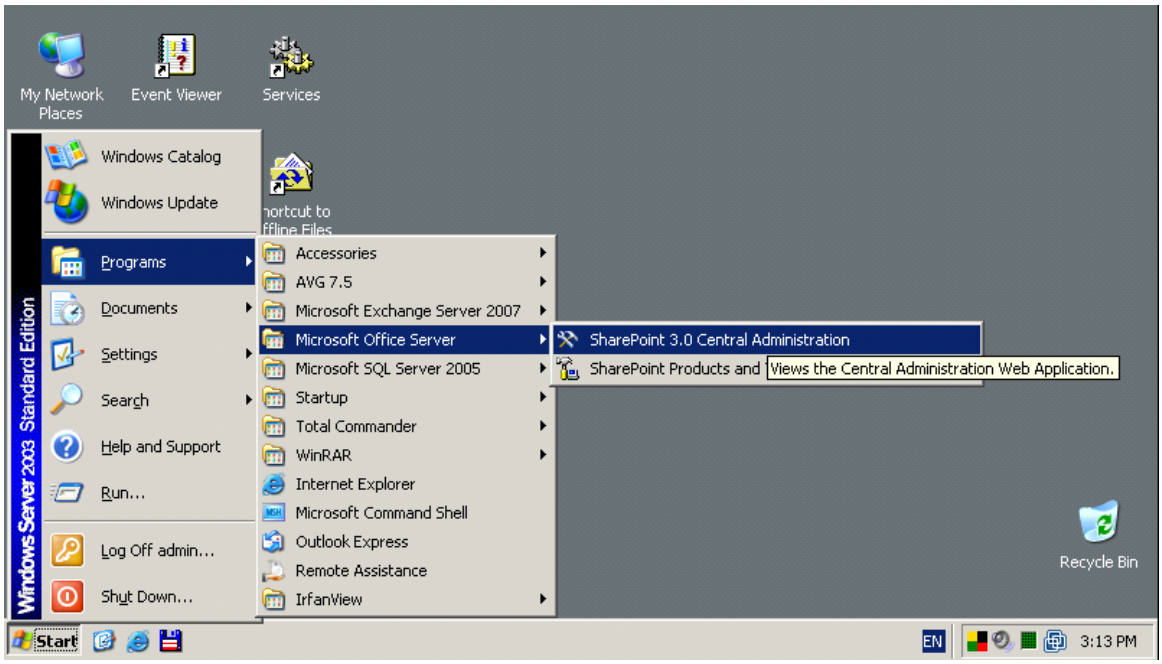
9. AVG dla serwera SharePoint Portal Server

Ten rozdzial zawiera informacje dotyczace obslugi systemu AVG na serwerze***MS SharePoint Portal Server***, który stanowi szczególny typ serwera plików.

9.1. Obsluga programu

Program **AVG dla SharePoint Portal Server** uzywa interfejsu Microsoft SP VSAPI 1.4 do ochrony serwera przed infekcjami wirusowymi. Obiekty na serwerze sa testowane pod katem obecnosci szkodliwego oprogramowania podczas ich pobierania lub wysylania na serwer. Konfiguracja ochrony antywirusowej moze zostac wprowadzona za pomoca ***Centralnej administracji*** serwera SharePoint Portal Server. W ***Centralnej administracji*** mozna równiez zarzadzac plikiem dziennika serwera **AVG dla SharePoint Portal Server**.

Uruchomienie ***Centralnej administracji serwera SharePoint Portal Server*** jest mozliwe po zalogowaniu sie na komputerze, na którym uruchomiony jest serwer. Interfejs administracji jest oparty o witryne WWW (*podobnie jak interfejs uzytkownika serwera SharePoint Portal Server*) i mozna go otworzyc za pomoca opcji ***Centralna administracja serwera SharePoint (3.0)*** z menu Start: ***Programy/Microsoft Office Server*** (***lub SharePoint Portal Server***):



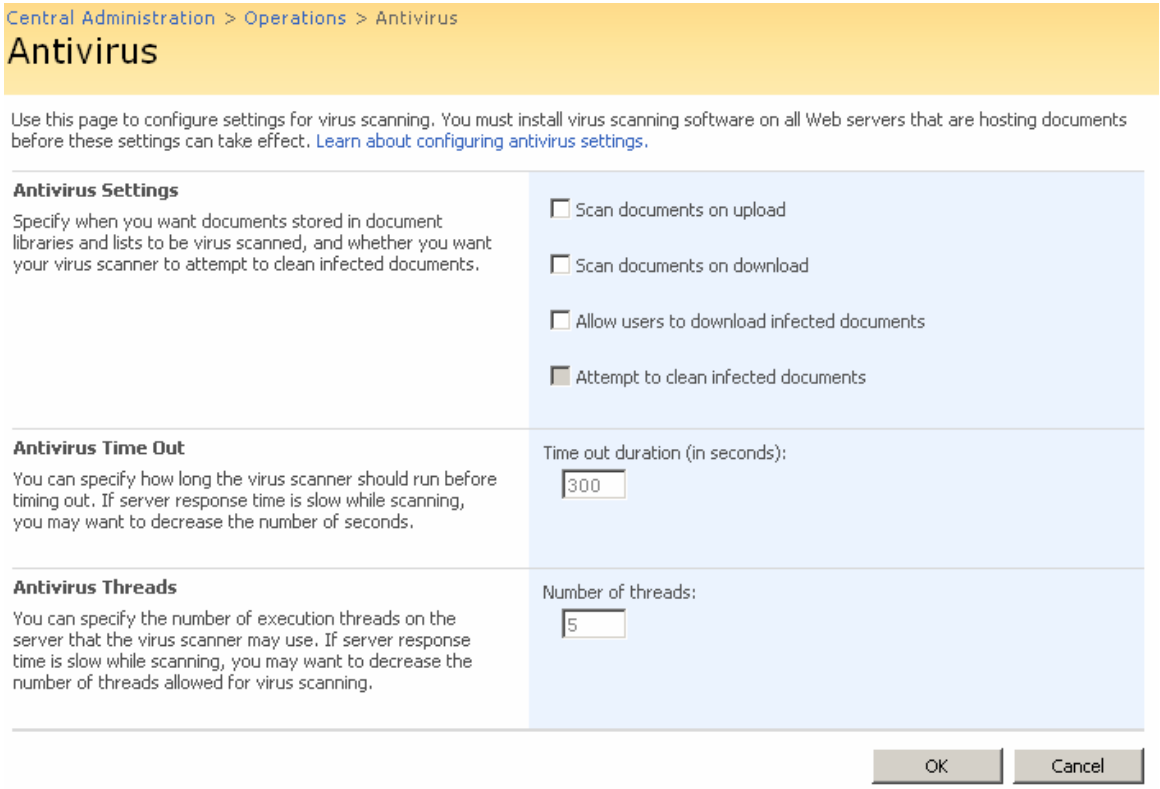
Mozliwe jest równiez zdalne odwiedzenie strony WWW ***Centralna administracja***

serwera SharePoint Portal Server za pomoca odpowiednich uprawnien dostepu i adresu URL.

9.2. Konfiguracja systemu AVG dla SPPS - SharePoint 2007

W interfejsie ***Centralnej administracji serwera SharePoint 3.0*** mozna w latwy sposób skonfigurowac parametry wydajnosci oraz akcje skanera **AVG dla SharePoint Portal Server**. Wybierz opcje ***Operacje*** w sekcji ***Administracja centralna***. Zostanie wyswietlone nowe okno dialogowe. Wybierz pozycje ***Program antywirusowy*** w czesci ***Konfiguracja zabezpieczen***.

Zostanie wyswietlone nastepujace okno:



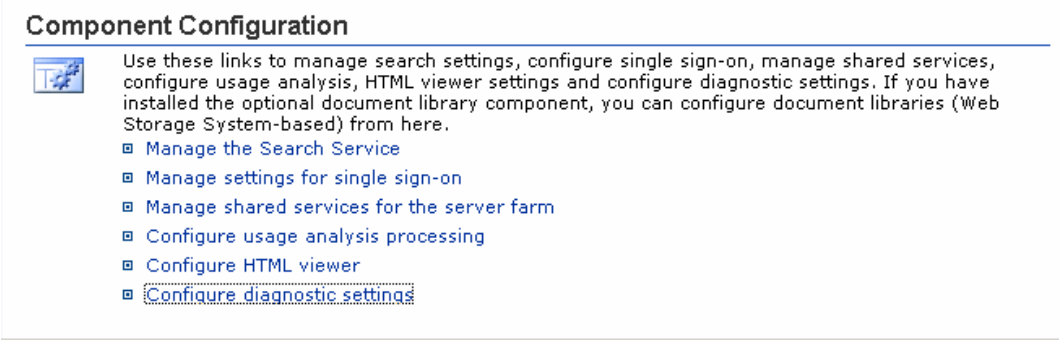
W tym miejscu mozna skonfigurowac rózne akcje skanra antywirusowego programu **AVG dla SharePoint Portal Server**:

- ***Skanuj dokumenty przy ich przesylaniu*** - wlacza/wylacza skanowanie przesylanych dokumentów.
- ***Skanuj dokumenty przy ich pobieraniu*** - wlacza/wylacza skanowanie pobieranych dokumentów.
- ***Pozwól uzytkownikom pobierac zainfekowane dokumenty*** - pozwala/ zabrania uzytkownikom pobierac zainfekowane dokumenty.
- ***Próbuj usuwac zainfekowane dokumenty*** - wlacza/wylacza automatyczne usuwanie zainfekowanych dokumentów.
- ***Limit czasu*** (*w sekundach*) - maksymalna ilosc sekund, przez która moze byc uruchomione pojedyncze skanowanie (wartosc te nalezy zmniejszyc, jesli odpowiedzi serwera podczas skanowania dokumentów sa zbyt wolne).

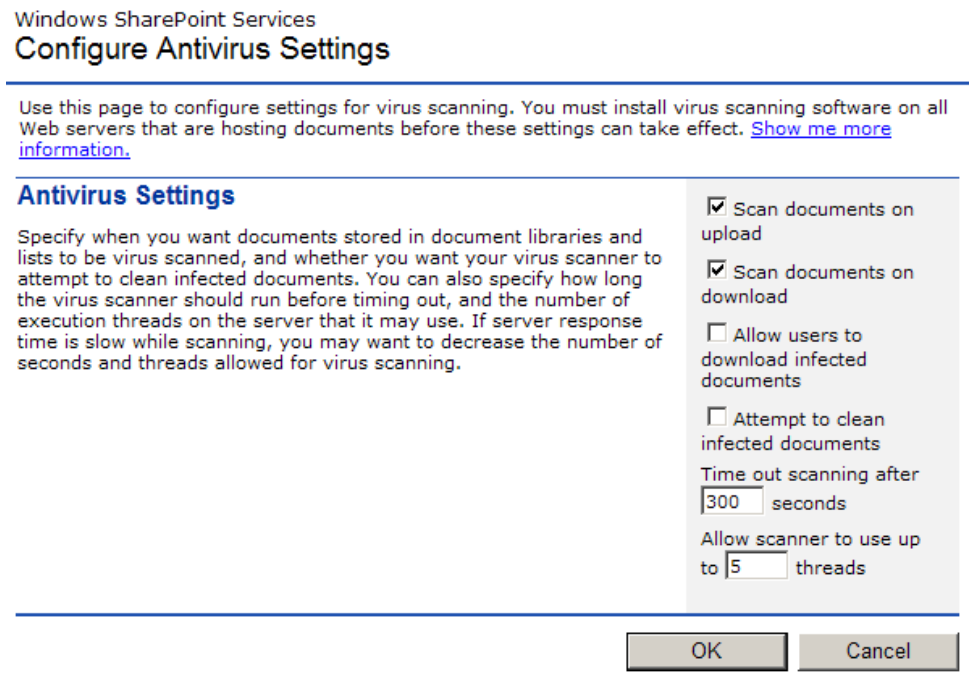
- ***Liczba watków*** - okresla liczbe watków skanera antywirusowego, które moga byc uruchomione jednoczesnie. Zwiekszenie tej liczby moze przyspieszyc skanowanie na maszynach wielordzeniowych, ale moze takze spowodowac zwiekszenie czasu odpowiedzi serwera.

9.3. Konfiguracja systemu AVG dla SPPS - SharePoint 2003

W interfejsie ***Centralnej administracji serwera SharePoint Portal Server*** mozna w latwy sposób skonfigurowac parametry wydajnosci oraz akcje skanera **AVG dla SharePoint Portal Server**. Wybierz opcje ***Konfiguracja akcji programu antywirusowego*** w sekcji ***Konfiguracja zabezpieczen***:



Zostanie wyswietlone nastepujace okno:



W tym miejscu mozna skonfigurowac rózne akcje skanera antywirusowego programu **AVG dla SharePoint Portal Server**:

- ***Skanuj dokumenty przy ich przesylaniu*** - wlacza/wylacza skanowanie przesylanych dokumentów.
- ***Skanuj dokumenty przy ich pobieraniu*** - wlacza/wylacza skanowanie pobieranych dokumentów.
- ***Pozwól uzytkownikom pobierac zainfekowane dokumenty*** - pozwala/ zabrania uzytkownikom pobierac zainfekowane dokumenty.
- ***Próbuj usuwac zainfekowane dokumenty*** - wlacza/wylacza automatyczne usuwanie zainfekowanych dokumentów.
- ***Limit czasu skanowania*** - maksymalna ilosc sekund, przez która moze byc uruchomione pojedyncze skanowanie (*wartosc te nalezy zmniejszyc, jesli odpowiedzi serwera podczas skanowania dokumentów sa zbyt wolne*)
- ***Uzywaj maks. X podprocesów przy skanowaniu dokumentów*** - X okresla liczbe watków skanera antywirusowego, które moga byc uruchomione jednoczesnie. Zwiekszenie tej liczby moze przyspieszyc skanowanie na

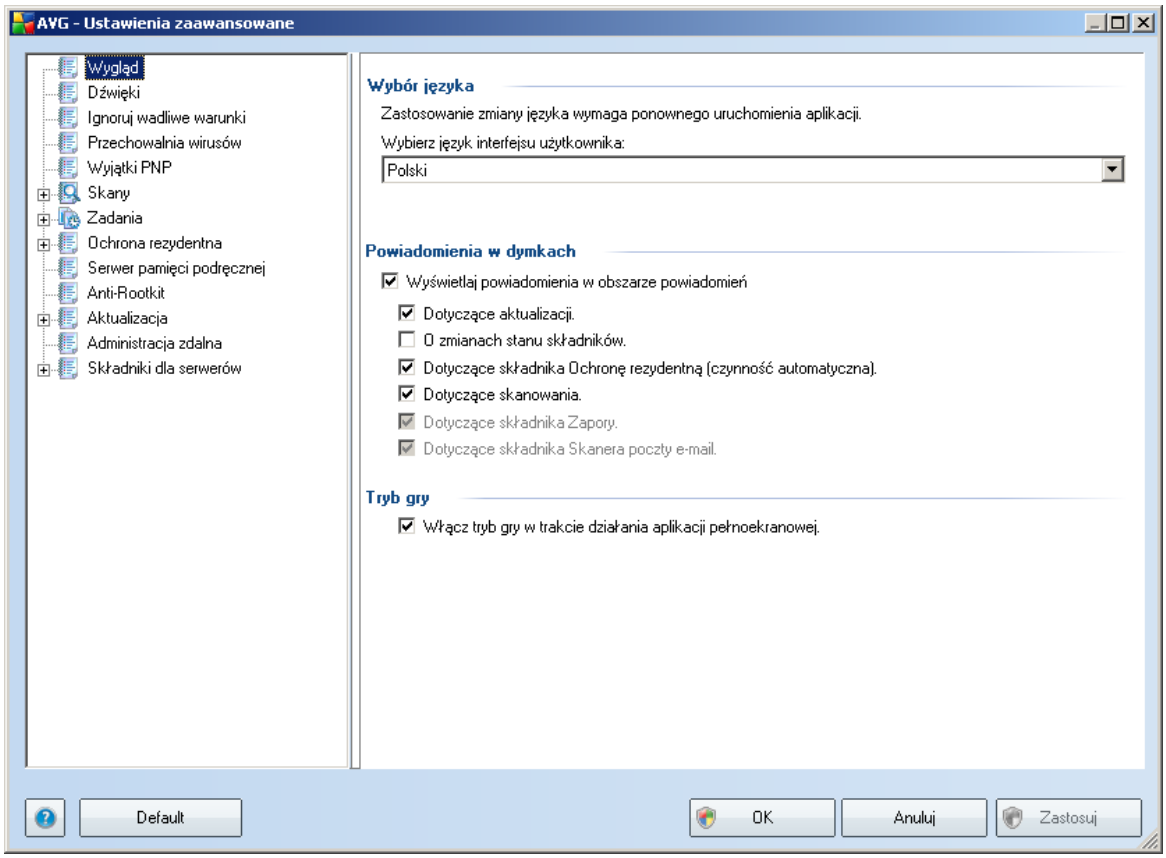
maszynach wielordzeniowych, ale moze takze spowodowac zwiekszenie czasu odpowiedzi serwera.

10. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG 9.0 File Server** zostaja otwarte w nowym oknie o nazwie ***AVG - Ustawienia zaawansowane***. Okno to podzielone jest na dwa obszary: lewy zawiera drzewo nawigacyjne, a prawy - opcje konfiguracji programu. Wybranie skladnika, którego (*lub czesci którego*) konfiguracja ma zostac zmieniona, powoduje przejscie do odpowiedniego okna z prawej strony.

10.1. Wyglad

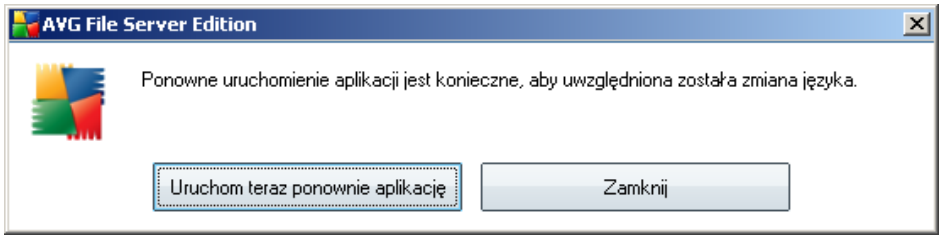
Pierwszy element w drzewie nawigacyjnym, ***Wyglad***, odnosi sie do ogólnych ustawien interfejsu uzytkownika AVG oraz kilku podstawowych opcji sterujacych zachowaniem aplikacji:



Wybór jezyka

W sekcji ***Wybór jezyka*** mozna wybrac zadany jezyk z listy rozwijanej; jezyk ten bedzie uzywany w calym interfejsie uzytkownika AVG. Menu rozwijane zawiera tylko jezyki wybrane podczas instalacji (zobacz rozdzial Instalacja niestandardowa - Wybieranie skladników). Przelaczenie aplikacji na inny jezyk wymaga ponownego uruchomienia interfejsu uzytkownika. W tym celu nalezy wykonac nastepujace kroki:

- Wybierz zadany jezyk aplikacji i potwierdz wybór, klikajac przycisk ***Zastosuj*** (widoczny w prawym dolnym rogu).
- Wcisnij przycisk ***OK***, aby potwierdzic.
- W nowym oknie dialogowym pojawi sie informacja, ze zmiana jezyka interfejsu systemu AVG wymaga ponownego uruchomienia programu:



Powiadomienia w dymkach

W tym obszarze mozna wylaczyc wyswietlane w dymkach powiadomienia dotyczace stanu aplikacji. Domyslnie wszystkie powiadomienia sa wyswietlane i nie zaleca sie zmiany tych ustawien. Zwykle informuja one o zmianach stanu skladników AVG i w zadnym wypadku nie wolno ich ignorowac!

Jesli jednak z jakiegos powodu powiadomienia te nie maja byc wcale wyswietlane lub maja dotyczyc tylko okreslonych skladników AVG, mozna zdefiniowac wlasne preferencje, zaznaczajac lub usuwajac zaznaczenie odpowiednich opcji:

- ***Wyswietlaj powiadomienia w obszarze powiadomien*** - pole jest domyslnie zaznaczone (*opcja wlaczona*), a powiadomienia sa wyswietlane. Usuniecie zaznaczenia opcji powoduje calkowite wylaczenie wyswietlania powiadomien w dymkach. Po wlaczeniu tej opcji mozna bardziej szczegółowo okreslic, jakie powiadomienia maja byc wyswietlane:
    - ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace aktualizacji*** - nalezy okreslic, czy maja byc wyswietlane informacje dotyczace rozpoczecia, postepu i zakonczenia aktualizacji systemu AVG;

- ***Wyswietlaj powiadomienia o zmianach stanu skladników*** - nalezy okreslic, czy maja byc wyswietlane informacje dotyczace aktywnosci lub nieaktywnosci skladników badz mozliwych problemów ich dotyczacych. W przypadku zglaszania stanu bledu skladnika, opcja ta pelni funkcje informacyjna w ten sam sposób co ikona na pasku zadan, która wskazuje na problemy z którymś ze skladników systemu AVG *(opcja ta jako jedyna jest domyslnie wylaczona)*;

- ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace skladnika Ochrona rezydentna*** - nalezy okreslic, czy informacje dotyczace zapisywania, kopiowania i otwierania plików maja byc wyswietlane, czy pomijane;

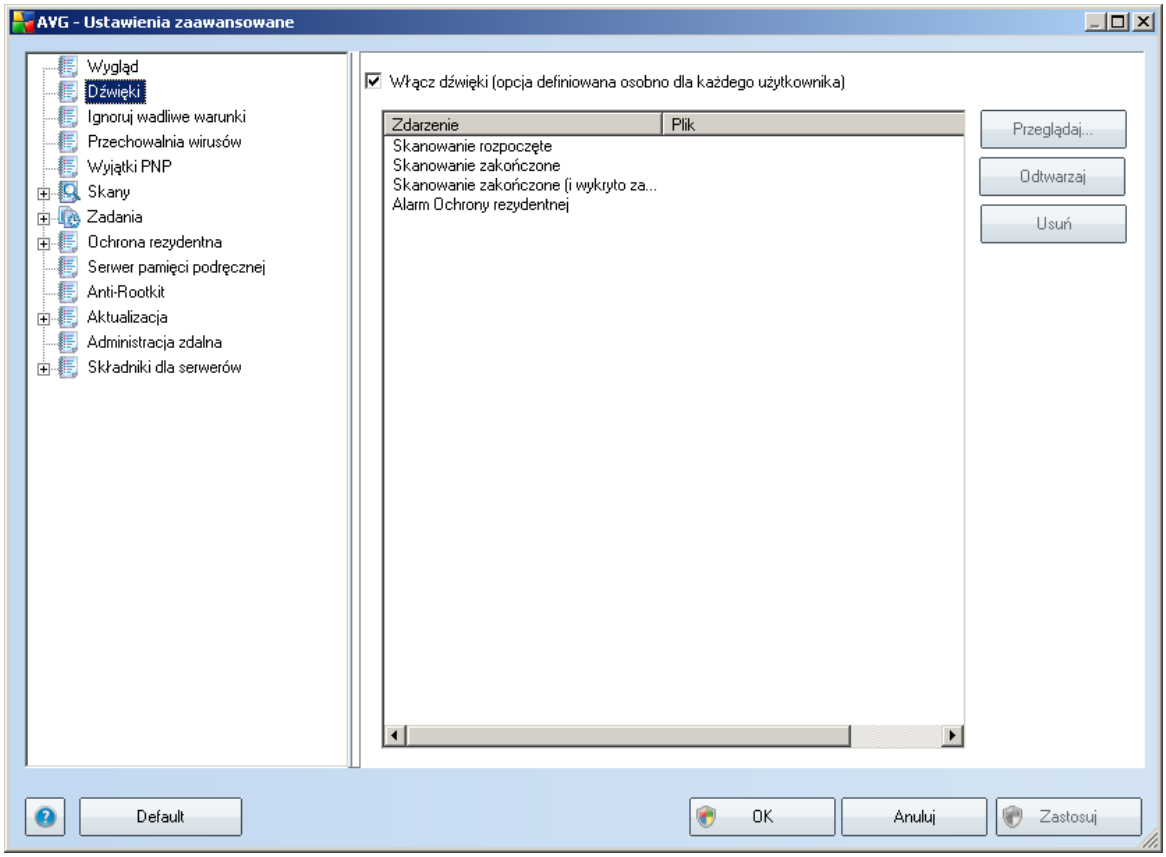
- ***Wyswietlaj w obszarze powiadomien komunikaty dotyczace skanowania*** - nalezy okreslic, czy maja byc wyswietlane informacje dotyczace automatycznego rozpoczecia, postepu i zakonczenia zaplanowanego skanowania.

Tryb gry

Ta funkcja jest przeznaczona dla aplikacji pelnoekranowych, w dzialaniu których mogłyby przeszkadzac (*np. minimalizowac lub zaklócac wyswietlanie grafiki*) powiadomienia systemu AVG (*wyswietlane np. w chwili uruchomienia zaplanowanego skanowania*). Aby tego uniknac, nalezy pozostawic pole wyboru ***Wlacz tryb gry w trakcie dzialania aplikacji pelnoekranowej*** zaznaczone (*ustawienie domyslne*).

10.2. Dzwieki

W oknie dialogowym ***Dzwieki*** mozna okreslic, czy system AVG ma informowac o okreslonych czynnosciach za pomoca dzwieków. Jesli tak, nalezy zaznaczyc pole wyboru ***Wlacz efekty dzwiekowe*** (*domyslnie wylaczone*), aby wlaczyc liste czynnosci systemu AVG:

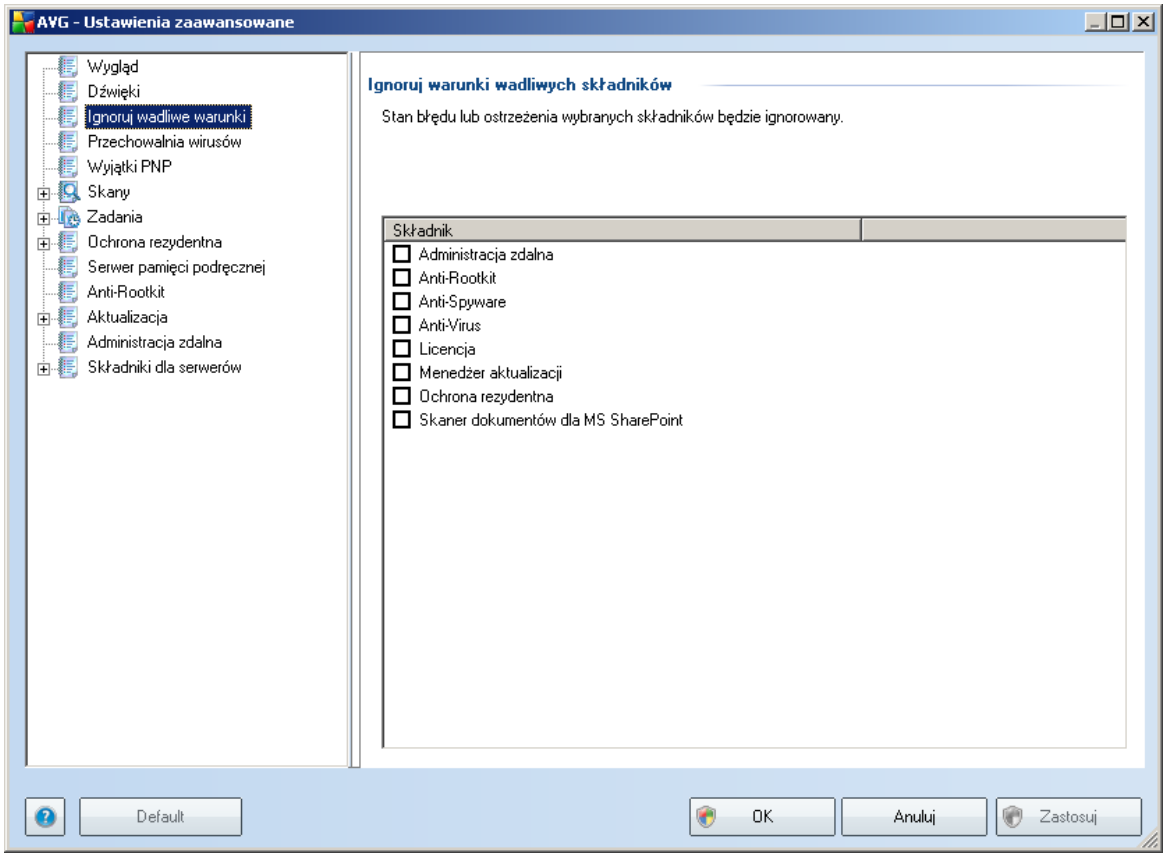


Nastepnie nalezy wybrac odpowiednie zdarzenie z listy i wskazac plik dzwiekowy, który ma zostac do niego przypisany (***Przegladaj***). Aby odtworzyc wybrany dzwiek, nalezy zaznaczyc go na liscie i nacisnac przycisk ***Odtwórz***. Aby usunac dzwiek przypisany do okreslonego zdarzenia, nalezy uzyc przycisku ***Usun***.

Uwaga: *Obslugiwane sa tylko pliki *.wav!*

10.3. Ignoruj bledny stan skladników

W oknie dialogowym ***Ignoruj wadliwy stan skladników*** mozna wskazac skladniki, które maja byc pomijane w powiadomieniach o stanie:



Domyslnie zaden skladnik nie jest zaznaczony. Oznacza to, ze jesli dowolny skladnik znajdzie sie w stanie bledu, natychmiast wygenerowane zostanie powiadomienie:

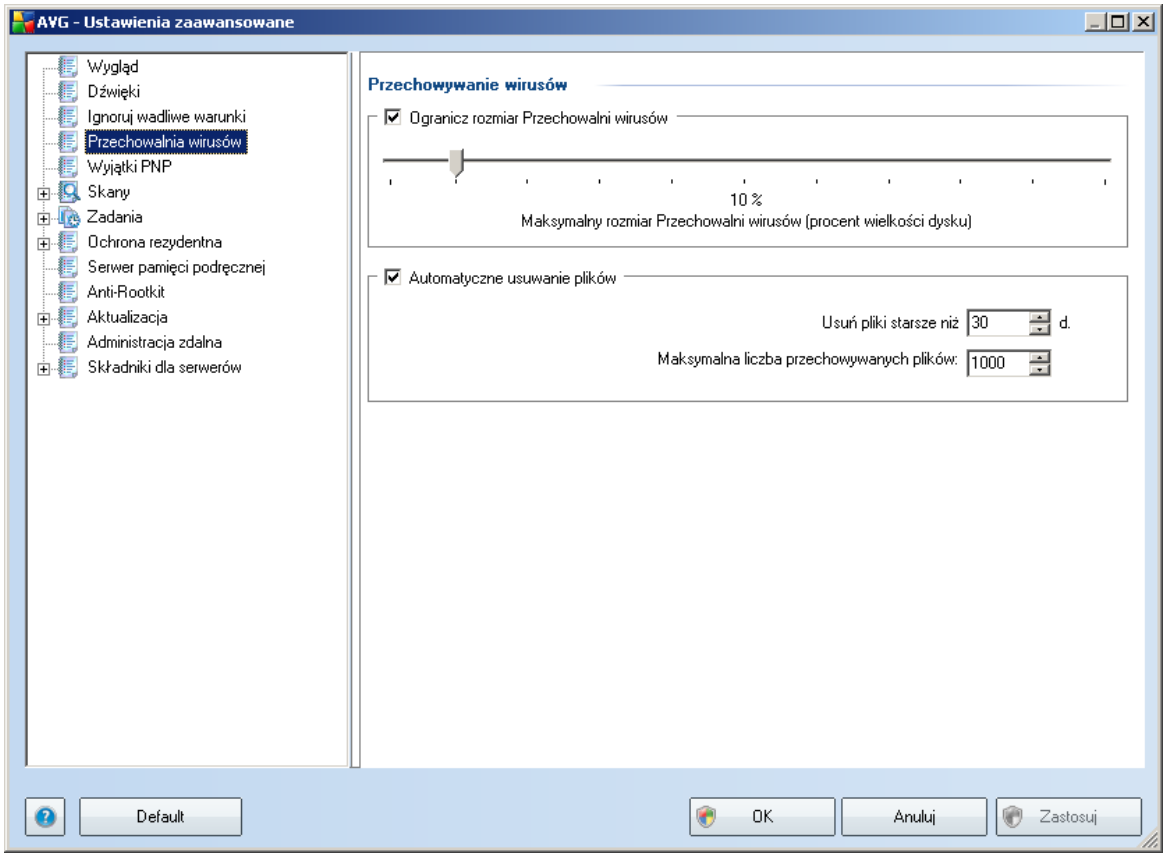
- ***ikona na pasku zadan*** - gdy wszystkie skladniki systemu AVG dzialaja prawidlowo, wyswietlana jest standardowa ikona AVG; w przypadku bledu wyswietlany jest zólty wykrzyknik,
- tekstowy opis problemu jest widoczny w sekcji ***Informacje o stanie bezpieczenstwa*** okna glównego AVG

Moze wystapic sytuacja, w której skladnik powinien zostac tymczasowo wylaczony (*nie jest to zalecane; wszystkie skladniki powinny byc zawsze wlaczone i dzialac w*

trybie domyslnym, ale niekiedy moze byc wymagane odstepstwo od tej reguly). W takim przypadku ikona na pasku zadan automatycznie informuje o stanie bledu skladnika. W takiej sytuacji nie ma jednak faktycznego bledu, poniewaz wylaczenie skladnika bylo celowe, a ryzyko z tym zwiazane jest znane. Ponadto, gdy obok ikony wyswietlany jest wykrzyknik, nie moze ona juz informowac o ewentualnych realnych bledach.

W takim przypadku nalezy w powyzszym oknie dialogowym zaznaczyc skladniki, które moga byc w stanie bledu (*lub wylaczone*) bez wyswietlania odpowiednich powiadomien. Opcja ***ignorowania stanu skladnika*** jest takze dostepna dla okreslonych skladników bezposrednio w sekcji przegladu skladników okna glównego AVG.

10.4. Przechowalnia wirusów



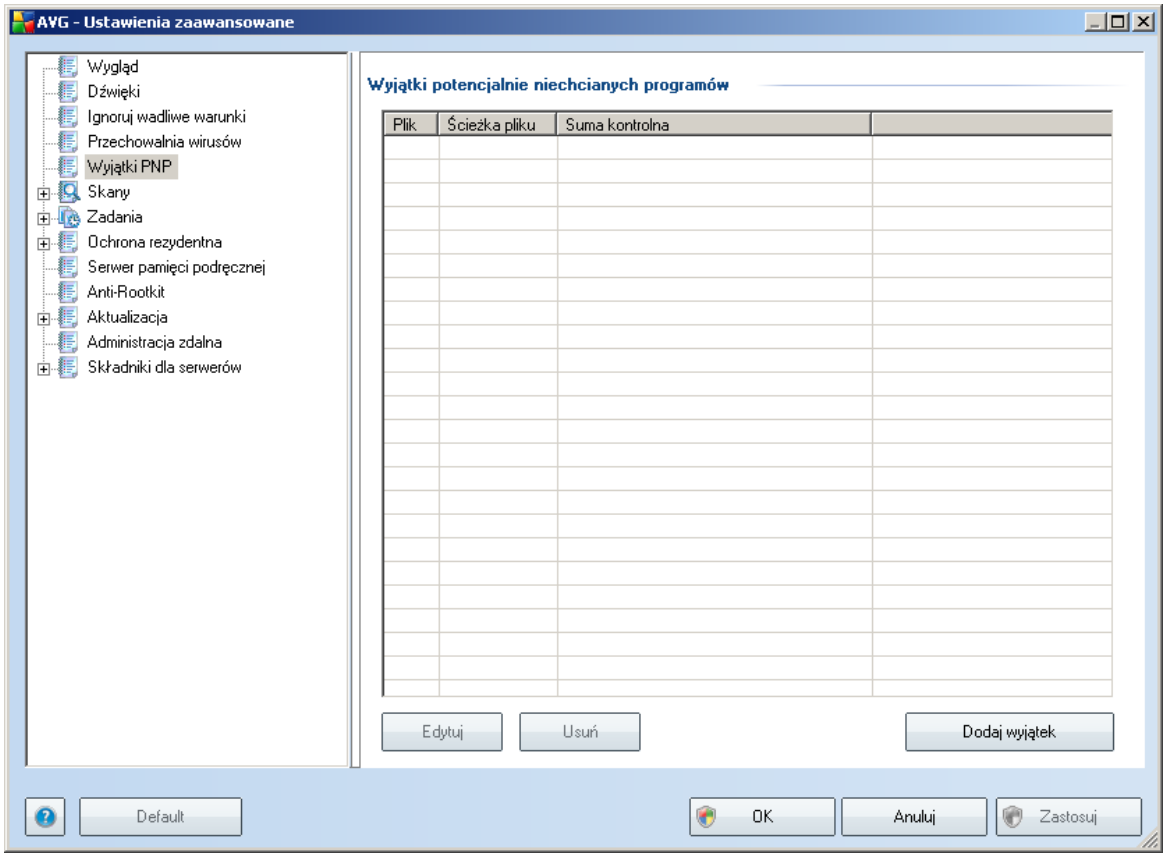
W oknie ***Przechowalnia wirusów*** mozna zdefiniowac kilka parametrów dotyczacych administrowania obiektami znajdujacymi sie w ***Przechowalni***:

- ***Ogranicz rozmiar Przechowalni wirusów*** - za pomoca suwaka nalezy okreslic maksymalny rozmiar ***Przechowalni wirusów***. Rozmiar jest okreslany w stosunku do rozmiaru dysku lokalnego.

- ***Automatyczne usuwanie plików*** - w tym obszarze mozna zdefiniowac maksymalny okres przetrzymywania obiektów w ***Przechowalni wirusów*** (***Usun pliki starsze niz ... dni***) oraz maksymalna liczbe plików, które moga znajdowac sie w ***Przechowalni*** (***Maksymalna liczba przechowywanych plików***).

10.5. Wyjatki PNP

System **AVG 9.0 File Server** potrafi analizowac i wykrywac pliki wykonywalne i biblioteki DLL, których obecnosc w systemie operacyjnym moze byc niepozadana. W niektórych przypadkach uzytkownik moze chciec zachowac na komputerze okreslone potencjalnie niechciane programy (*jesli zostaly zainstalowane celowo*). Niektóre aplikacje, zwlaszcza bezplatne, zawieraja oprogramowanie reklamowe. Moze ono zostac wykryte i zgloszone przez system AVG jako ***potencjalnie niechciany program***. Jesli chcesz zachowac taki program na komputerze, mozesz zdefiniowac go jako wyjatek potencjalnie niechcianych programów:

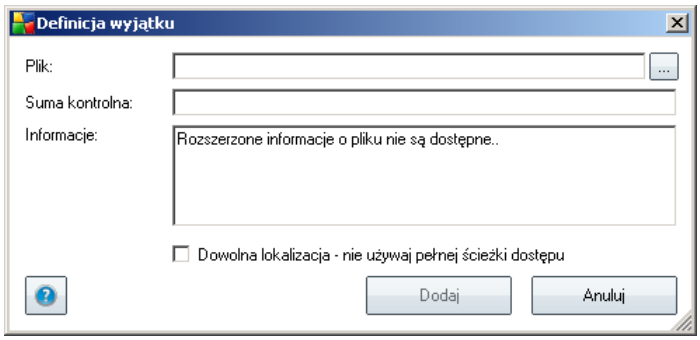


Okno ***Wyjatki potencjalnie niechcianych programów*** zawiera liste juz zdefiniowanych i aktualnie obowiazujacych wyjatków potencjalnie niechcianych programów. Liste te mozna edytowac, usuwac istniejace pozycje lub dodawac nowe wyjatki. Dla kazdego wyjatku na liscie dostepne sa nastepujace informacje:

- ***Plik*** - zawiera nazwe odpowiedniej aplikacji.
- ***Sciezka pliku*** - wyswietla sciezke dostepu do aplikacji.
- ***Suma kontrolna*** - wyswietla unikatowa „sygnature” wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odrózniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu pliku.

Przyciski kontrolne

- ***Edytuj*** - otwiera okno edycji (*identyczne jak okno definiowania nowego wyjatku (patrz nizej*), w którym mozna zmienic parametry istniejacego wyjatku.
- ***Usun*** - usuwa wybrany element z listy wyjatków.
- ***Dodaj wyjatek*** - otwiera okno edycji, w którym mozna zdefiniowac parametry nowego wyjatku:



  - ***Plik*** - nalezy podac pelna sciezke do pliku, który ma byc oznaczony jako wyjatek.
  - ***Suma kontrolna*** - wyswietla unikatowa „sygnature" wybranego pliku. Suma ta jest generowanym automatycznie ciagiem znaków, który pozwala programowi AVG jednoznacznie odrózniac wybrany plik od innych. Jest ona generowana i wyswietlana po pomyslnym dodaniu pliku.
  - ***Informacje o pliku*** - wyswietla wszelkie dodatkowe dostepne informacje na temat pliku (*licencja/wersja itp.*).
  - ***Dowolna lokalizacja - nie uzywaj pelnej sciezki dostepu*** - jesli plik ma byc zdefiniowany jako wyjatek jedynie dla konkretnej lokalizacji, wówczas nalezy pozostawic to pole niezaznaczone.

10.6. Skany

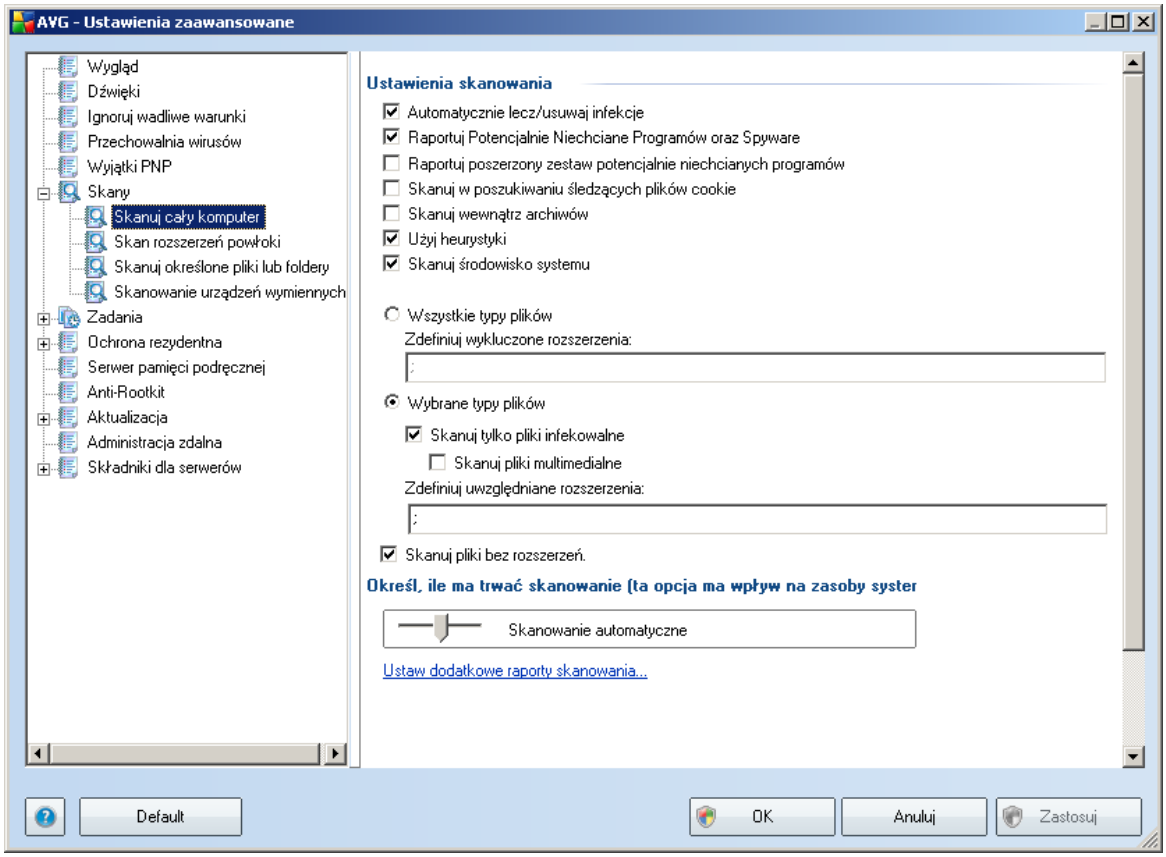
Zaawansowane ustawienia skanowania sa podzielone na cztery kategorie odnoszace sie do okreslonych typów testów:

- ***Skan calego komputera*** - standardowe, wstepnie zdefiniowane skanowanie calego komputera.
- ***Skan rozszerzenia powloki*** - skanowanie wybranych obiektów bezposrednio z interfejsu Eksploratora Windows.

- ***Skan okreslonych plików lub folderów*** - standardowe, wstepnie zdefiniowane skanowanie okreslonych obszarów komputera.
- ***Skan urzadzen wymiennych*** - skanowanie urzadzen wymiennych podlaczonych do komputera.

10.6.1. Skan calego komputera

Opcja ***Skanuj caly komputer*** umozliwia edycje parametrów jednego ze wstepnie zdefiniowanych testów: ***Skan calego komputera***:



Ustawienia skanowania

Sekcja ***Ustawienia skanowania*** zawiera liste parametrów silnika skanujacego:

- ***Automatycznie lecz/usuwaj infekcje*** - jezeli podczas skanowania wykryty

zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jesli zainfekowanego pliku nie mozna wyleczyc, lub jesli opcja ta zostanie wylaczona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcje. Zalecana metoda jest przeniesienie zainfekowanego pliku do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujace*** - parametr ten kontroluje funkcje skladnika ***Anti-Virus***, które pozwalaja wykrywac potencjalnie niechciane programy (*pliki wykonywalne mogace dzialac jak oprogramowanie szpiegujace lub reklamowe*), a nastepnie blokowac je lub usuwac.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - to pole nalezy zaznaczyc, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona;

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** - ten parametr skladnika Anti-Spyware okresla, ze skanowanie ma wykrywac pliki cookie (*pliki cookie sa w protokole HTTP uzywane do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach, na przyklad preferencji wygladu witryny czy zawartosci koszyków w sklepach internetowych*).

- ***Skanuj wewnatrz archiwów*** - parametr ten okresla, czy skanowanie ma obejmowac wszystkie pliki - nawet te znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.

- ***Uzyj heurystyki*** - analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny*) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.

- ***Skanuj srodowisko systemu*** - skanowanie obejmie takze obszary systemowe komputera.

Nastepnie nalezy zdecydowac, czy skanowane maja byc

- ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

- ***Wybrane typy plików*** - skanowane bede tylko pliki infekowalne (*pliki, które*

nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne), z uwzglednieniem plików multimedialnych (*plików wideo i audio - jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

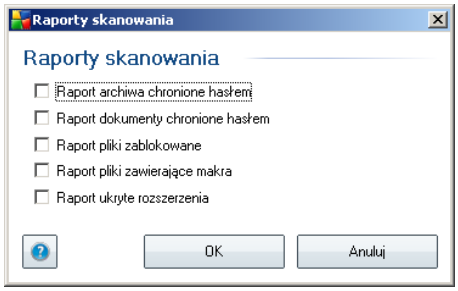
- Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** - ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

Priorytet procesu skanowania

W sekcji ***Priorytet procesu skanowania*** mozna szczególowo okreslic zadana predkosc skanowania, w zaleznosci od wykorzystania zasobów systemowych. Domyslnie wartosc tej opcji jest na srednim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jesli skanowanie ma przebiegac szybciej, poziom wykorzystania zasobów wzrosnie, co moze spowolnic dzialanie innych procesów i aplikacji (*opcji mozna smialo uzywac wtedy, gdy komputer jest wlaczony, ale nikt na nim nie pracuje*). Mozna takze obnizyc wykorzystanie zasobów, co przedluzy jednoczesnie czas skanowania.

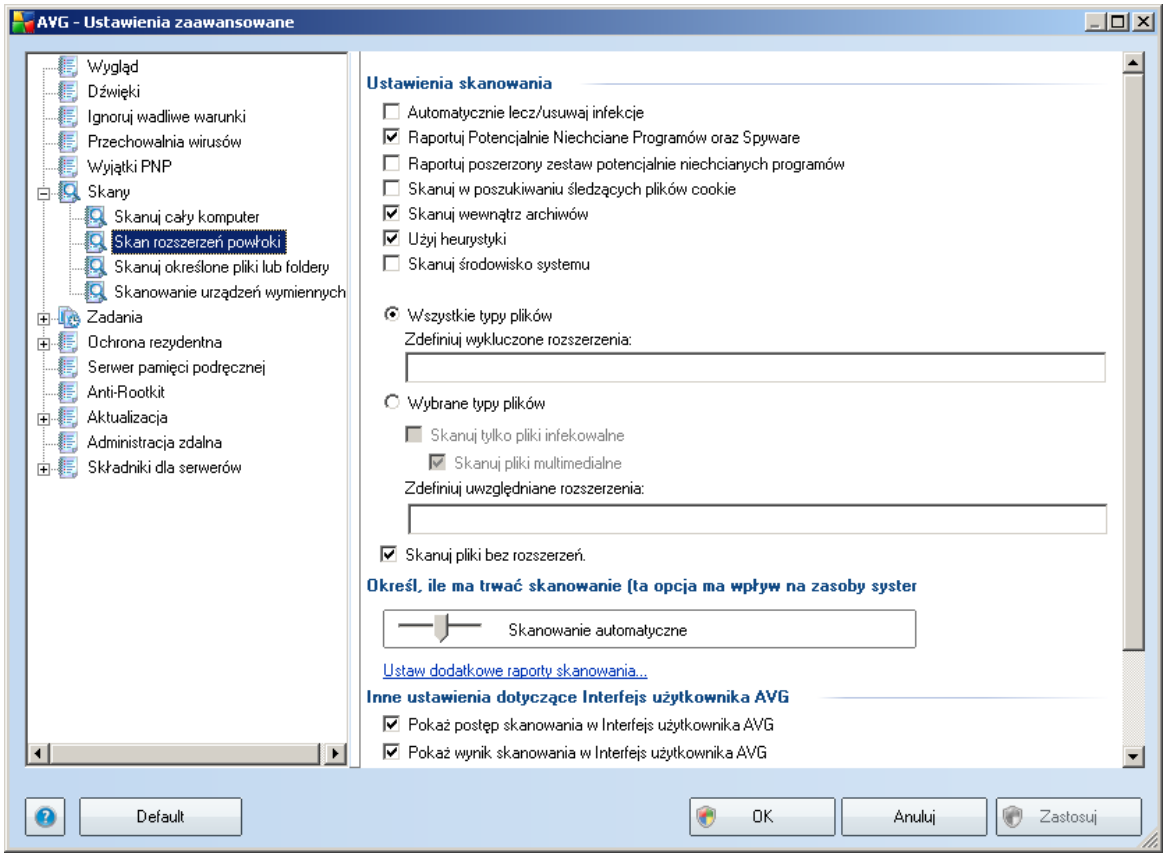
Ustaw dodatkowe raporty skanowania...

Klikniecie linku ***Ustaw dodatkowe raporty skanowania...*** powoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym mozna okreslic szczególowosc raportów, zaznaczajac zadane elementy:



10.6.2. Skan rozszerzenia powloki

Analogicznie do ***Skanu calego komputera***, test ***Skan rozszerzenia powloki*** takze oferuje szereg opcji silnika skanujacego, zdefiniowanych wstepnie przez dostawce oprogramowania AVG. W tym przypadku konfiguracja odnosi sie do skanowania okreslonych obiektów bezposrednio z interfejsu Eksploratora Windows (*rozszerzenie powloki*); zobacz rozdzial ***Skanowanie z poziomu Eksploratora Windows***:



Lista parametrów jest identyczna jak dla testu ***Skan calego komputera***. Ustawienia domyslne sa jednak inne: wiekszosc opcji ***skanu calego komputera*** jest aktywna, natomiast w przypadku ***skanu rozszerzenia powloki*** (***Skanowanie z poziomu Eksploratora Windows***) wybrane sa tylko najistotniejsze parametry.

Uwaga: *Opis poszczególnych parametrów mozna znalezc w rozdziale* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

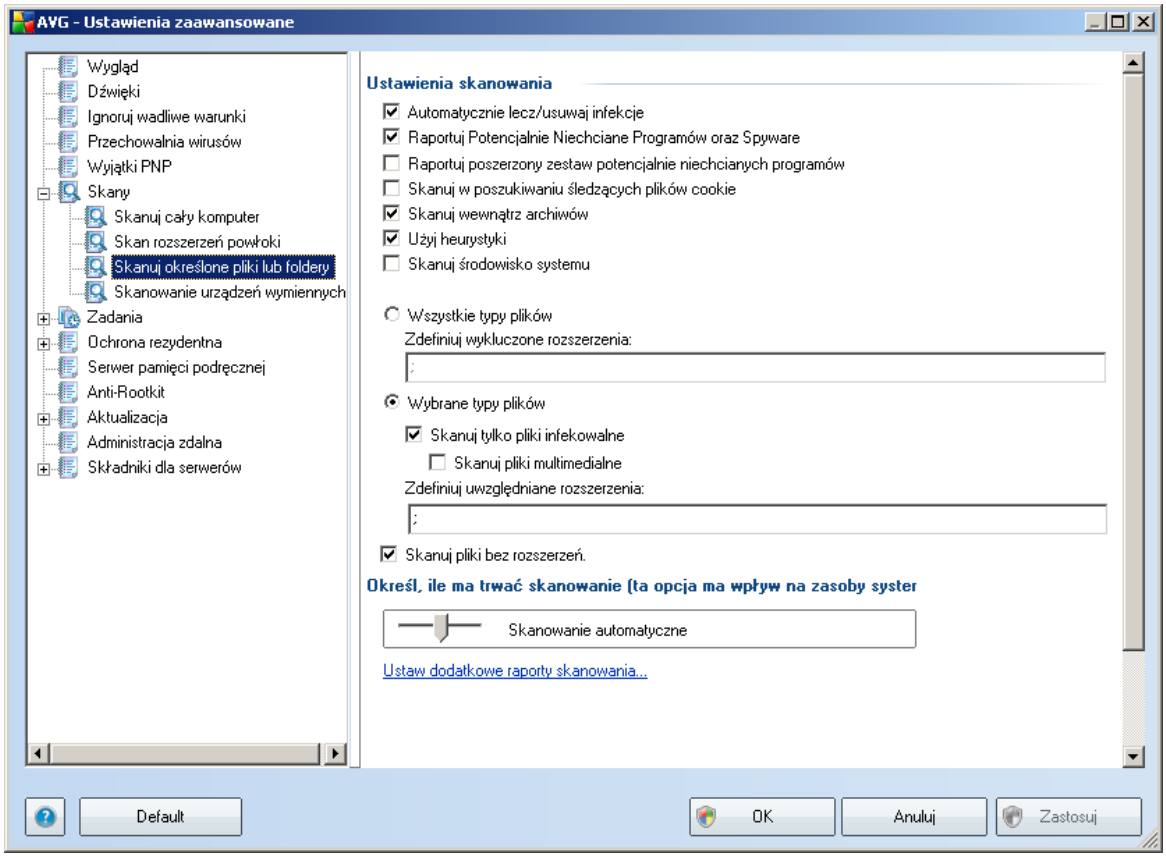
Jest jednak kilka parametrów, które sa dostepne tylko dla skanu rozszerzenia powloki.

Mozna je znalezc w sekcji **Inne ustawienia dotyczace Interfejsu uzytkownika AVG** :

- ***Pokaz postep skanowania w Interfejsie uzytkownika AVG*** - jesli to pole jest zaznaczone, uzytkownik bedzie powiadamiany o kazdym rozpoczeciu/ zakonczeniu skanu rozszerzenia powloki (dymek z odpowiednia informacja wyswietlany bedzie w prawym dolnym rogu ekranu).
- ***Pokaz wyniki skanowania w Interfejsie uzytkownika AVG*** - jesli to pole jest zaznaczone, za kazdym razem gdy skan rozszerzenia powloki zostanie zakonczony, nastapi otwarcie Interfejsu uzytkownika systemu AVG i wyswietlenie standardowego okna dialogowego ***Szczegóły wyników skanowania*** (liczba kart bedzie zalezec od wyniku skanowania).
  - ***Tylko jesli wyniki skanowania zawieraja zagrozenia*** - to pole jest aktywne jedynie, jesli poprzednie pole zostalo zaznaczone. Zaznaczenie tej opcji powoduje wyswietlenie okna dialogowego ***Szczegóły wyników skanowania*** tylko w sytuacji, gdy podczas skanu rozszerzenia powloki zostana wykryte zagrozenia.

10.6.3. Skan okreslonych plików lub folderów

Interfejs edycji testu ***Skan okreslonych plików lub folderów*** jest identyczny jak w przypadku ***Skanu calego komputera***. Wszystkie opcje konfiguracyjne sa takie same, jednak ustawienia domyslne dla ***skanu calego komputera*** sa bardziej rygorystyczne:

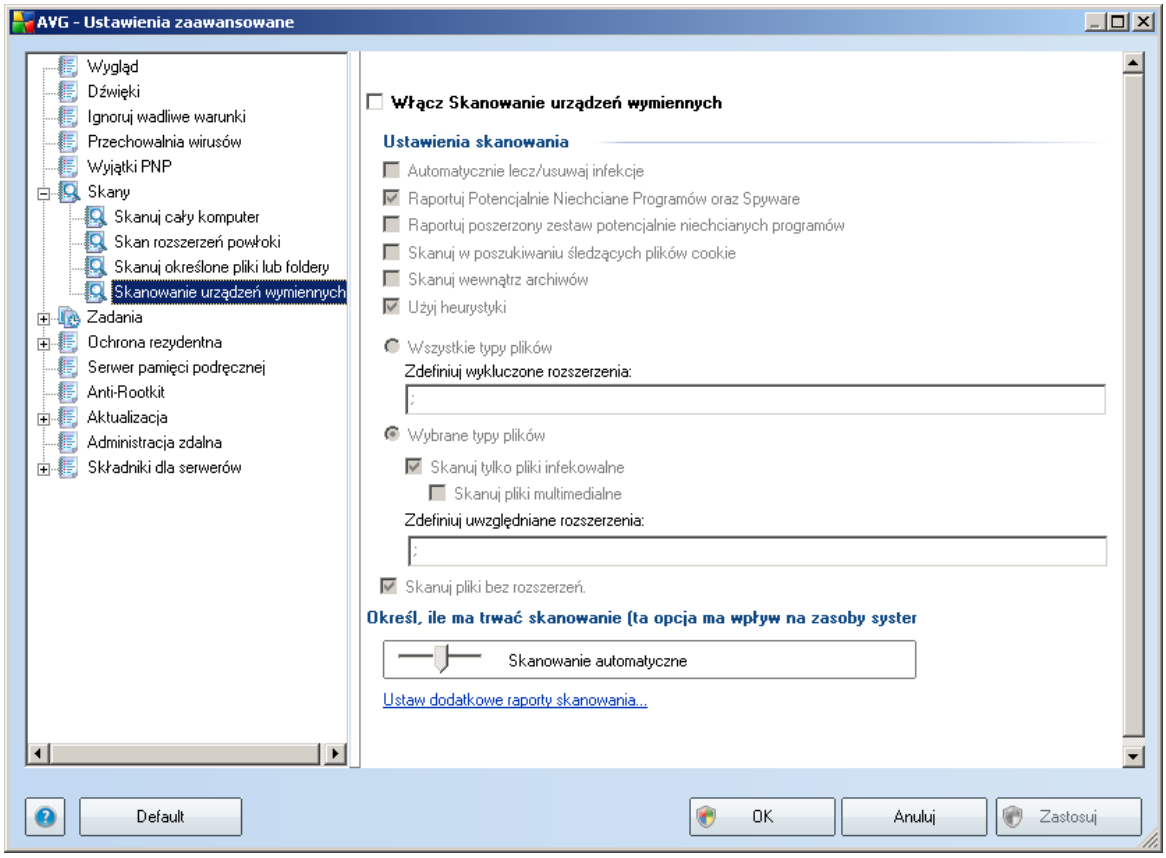


Wszystkie parametry ustawiane w tym oknie dialogowym odnosza sie tylko do obszarów wybranych do ***skanowania okreslonych plików lub folderów***!

Uwaga: *Opis poszczególnych parametrów mozna znalezc w rozdziale* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

10.6.4. Skan urzadzen wymiennych

Okno z opcjami ***Skanu urzadzen wymiennych*** jest takze bardzo podobne do okna ***Skan calego komputera***:



Skan urzadzen wymiennych jest uruchamiany automatycznie po podlaczeniu do komputera dowolnego urzadzenia wymiennego. Domyslnie jest on wylaczony. Skanowanie urzadzen wymiennych w poszukiwaniu potencjalnych zagrozen jest jednak bardzo wazne, poniewaz sa one czestym zródlem infekcji. Jesli skan ma byc uruchamiany automatycznie, nalezy zaznaczyc opcje ***Wlacz skanowanie urzadzen wymiennych***.

Uwaga: *Opis poszczególnych parametrów mozna znalezc w rozdziale* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

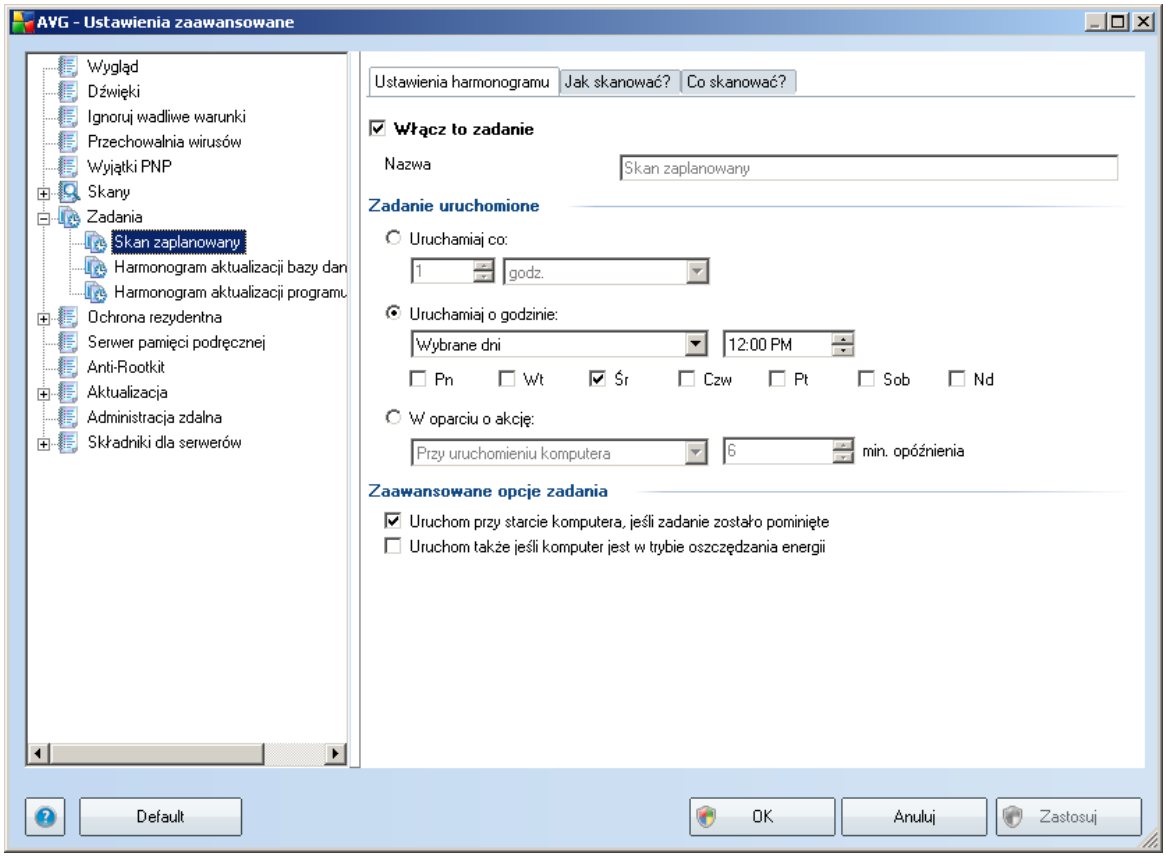
10.7. Zaplanowane zadania

W oknie ***Zadania*** mozna edytowac domyslne ustawienia nastepujacych pozycji:

- Skan zaplanowany
- Harmonogram aktualizacji bazy wirusów
- Harmonogram aktualizacji programu

10.7.1. Skan zaplanowany

Parametry skanowania zaplanowanego mozna edytowac (*albo utworzyc nowy harmonogram*) na trzech kartach:



Na karcie ***Ustawienia harmonogramu*** mozna zaznaczyc/odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowany test lub wlaczyc go ponownie, gdy zajdzie taka potrzeba.

W polu tekstowym ***Nazwa*** (*wylaczone dla harmonogramów domyslnych*) wyswietlana jest nazwa przypisana do danego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (*aby dodac harmonogram, nalezy kliknac prawym przyciskiem myszy element* ***Skan zaplanowany*** *w drzewie nawigacji po lewej*) mozna okreslic wlasna nazwe, a wspomniane pole tekstowe jest edytowalne. Nalezy uzywac krótkich, opisowych nazw, aby ulatwic rozpoznawanie ich przez innych uzytkowników w przyszlosci.

Przyklad: *Nazwy takie jak „Nowy skan" lub „Mój skan" nie sa odpowiednie, poniewaz nie informuja o tym, co jest przedmiotem skanowania. Przykladem dobrej, opisowej nazwy jest „Skan obszarów systemowych". Ponadto, nie ma potrzeby okreslac w nazwie skanowania, czy skanowany jest caly komputer, czy tylko jego wybrane obszary - wlasne testy uzytkownika sa zawsze specyficznym skanowaniem okreslonych plików lub folderów.*

W tym samym oknie mozna szczególowo okreslic nastepujace parametry skanowania:

Zadanie uruchomione

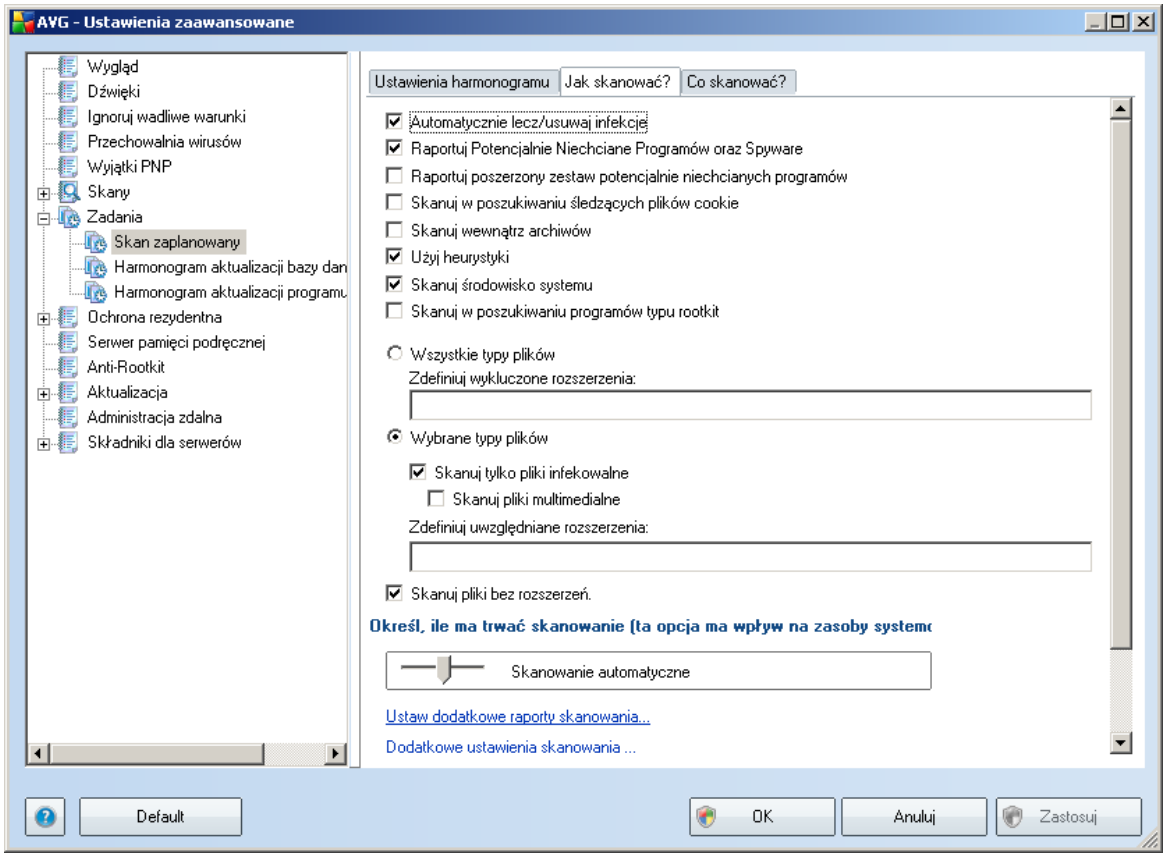
W tym miejscu mozna okreslic, jak czesto ma byc uruchamiane nowe skanowanie. Uruchamianie skanowania moze byc powtarzane w okreslonych odstepach czasu (***Uruchamiaj co***) lub w zadanych momentach (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia okreslonego zdarzenia (***akcja powiazana z uruchomieniem komputera***).

Zaawansowane opcje harmonogramu

Ta sekcja umozliwia zdefiniowanie warunków uruchamiania skanowania w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

Po rozpoczeciu zaplanowanego skanu, nad ikona AVG na pasku zadan wyswietlone zostanie odpowiednie powiadomienie:

Nastepnie pojawi sie tam nowa ikona AVG (*kolorowa, z biala strzalka - jak powyzej*), która informuje o uruchomieniu skanowania.



Karta ***Jak skanowac?*** zawiera liste parametrów testu, które mozna wlaczyc lub wylaczyc. Domyslnie wiekszosc funkcji jest wlaczona, a odpowiadajace im ustawienia sa stosowane podczas skanowania. Ustawienia te nalezy zmieniac tylko w uzasadnionych przypadkach, w pozostalych zachowujac wstepnie zdefiniowana konfiguracje:

- ***Automatycznie lecz/usuwaj infekcje*** - (*domyslnie wlaczona*) jezeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jesli zainfekowanego pliku nie mozna wyleczyc, lub jesli opcja ta zostanie wylaczona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcje. Zalecana czynnoscia jest przeniesienie zainfekowanego pliku do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujace*** - (*domyslnie wlaczona*) parametr ten kontroluje funkcje skladnika Anti-Virus, które pozwalaja wykrywac potencjalnie niechciane programy (*pliki wykonywalne mogace dzialac jak oprogramowanie szpiegujace lub reklamowe*), a nastepnie blokowac je lub usuwac.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - (*domyslnie wylaczone*): ten parametr pozwala wykrywac wieksza ilosc oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona;

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** - (*domyslnie wylaczona*) ten parametr skladnika Anti-Spyware okresla, czy wykrywane maja byc pliki cookie (*uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach - np. preferencji wygladu witryny i zawartosc koszyków w sklepach internetowych*).

- ***Skanuj wewnatrz archiwów*** - (*domyslnie wylaczona*) parametr okresla, ze skanowanie ma obejmowac wszystkie pliki, nawet te znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.

- ***Uzyj heurystyki*** - (*domyslnie wlaczona*) analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny*) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.

- ***Skanuj srodowisko systemu*** - (*domyslnie wlaczona*) skanowanie obejmie takze obszary systemowe komputera.

- ***Skanuj w poszukiwaniu programów typu rootkit*** - zaznaczenie tej pozycji pozwala dolaczyc wykrywanie programów typu rootkit do operacji skanowania calego komputera. Test Anti-Rootkit mozna takze uruchomic niezaleznie, dzieki interfejsowi skladnika ***Anti-Rootkit***

Nastepnie nalezy zdecydowac, czy skanowane maja byc

- ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

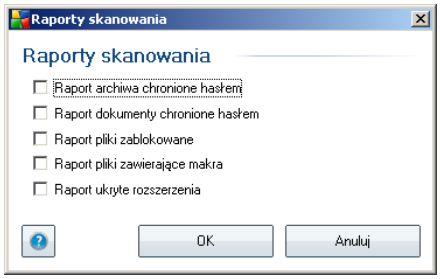
- ***Wybrane typy plików*** - skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio - jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

- Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** - ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

Priorytet procesu skanowania

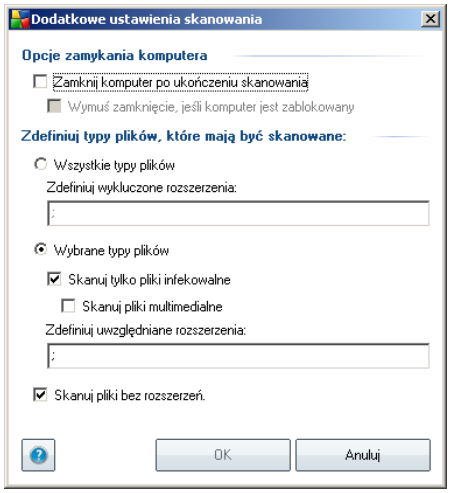
W sekcji ***Priorytet procesu skanowania*** mozna szczególowo okreslic zadana predkosc skanowania, w zaleznosci od wykorzystania zasobów systemowych. Domyslnie wartosc tej opcji jest na srednim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jesli skanowanie ma przebiegac szybciej, poziom wykorzystania zasobów wzrosnie, co moze spowolnic dzialanie innych procesów i aplikacji (*opcji mozna smialo uzywac wtedy, gdy komputer jest wlaczony, ale nikt na nim nie pracuje*). Mozna takze obnizyc wykorzystanie zasobów, co przedluzy jednoczesnie czas skanowania.

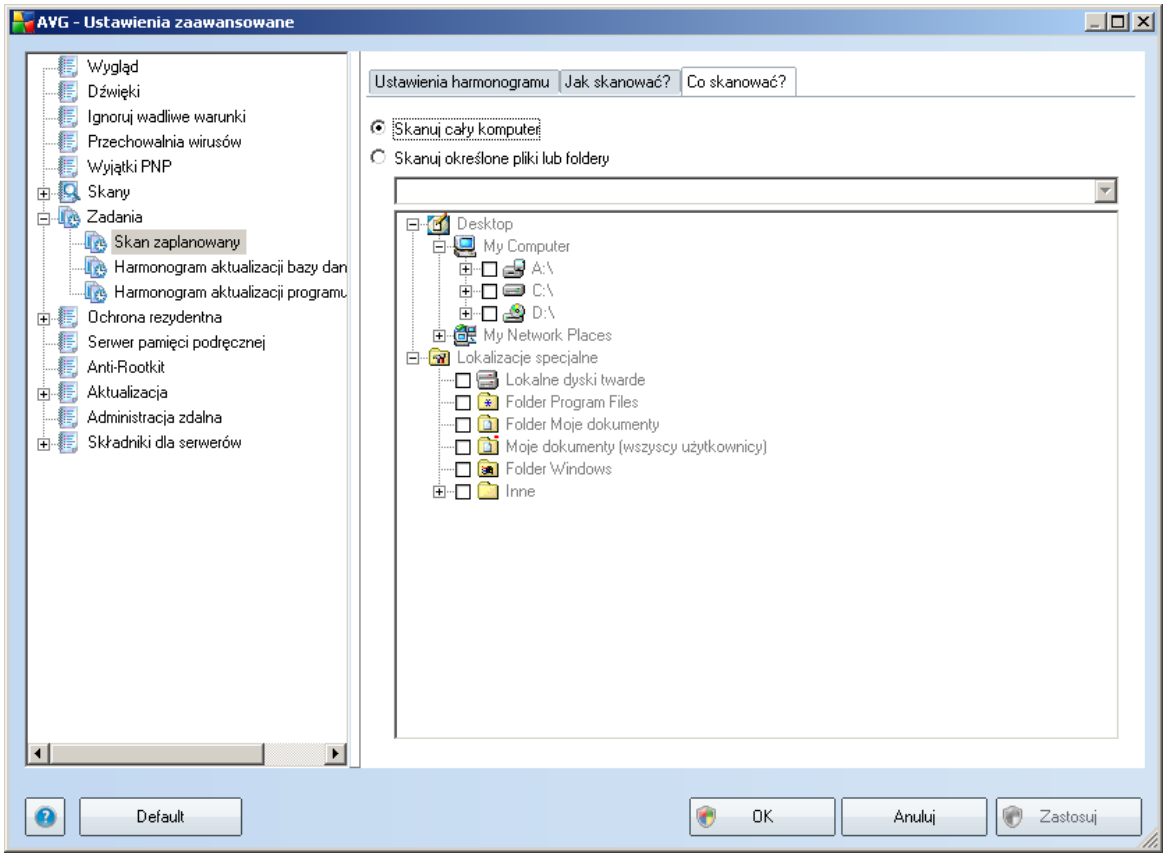
Klikniecie linku ***Ustaw dodatkowe raporty skanowania...*** powoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym mozna okreslic szczególowosc raportów, zaznaczajac zadane elementy:



Dodatkowe ustawienia skanowania - link ten pozwala otworzyc nowe okno dialogowe ***Opcje zamykania komputera***, w którym mozna okreslic, czy komputer ma byc zamykany automatycznie po zakonczeniu procesu skanowania. Wybranie tej opcji

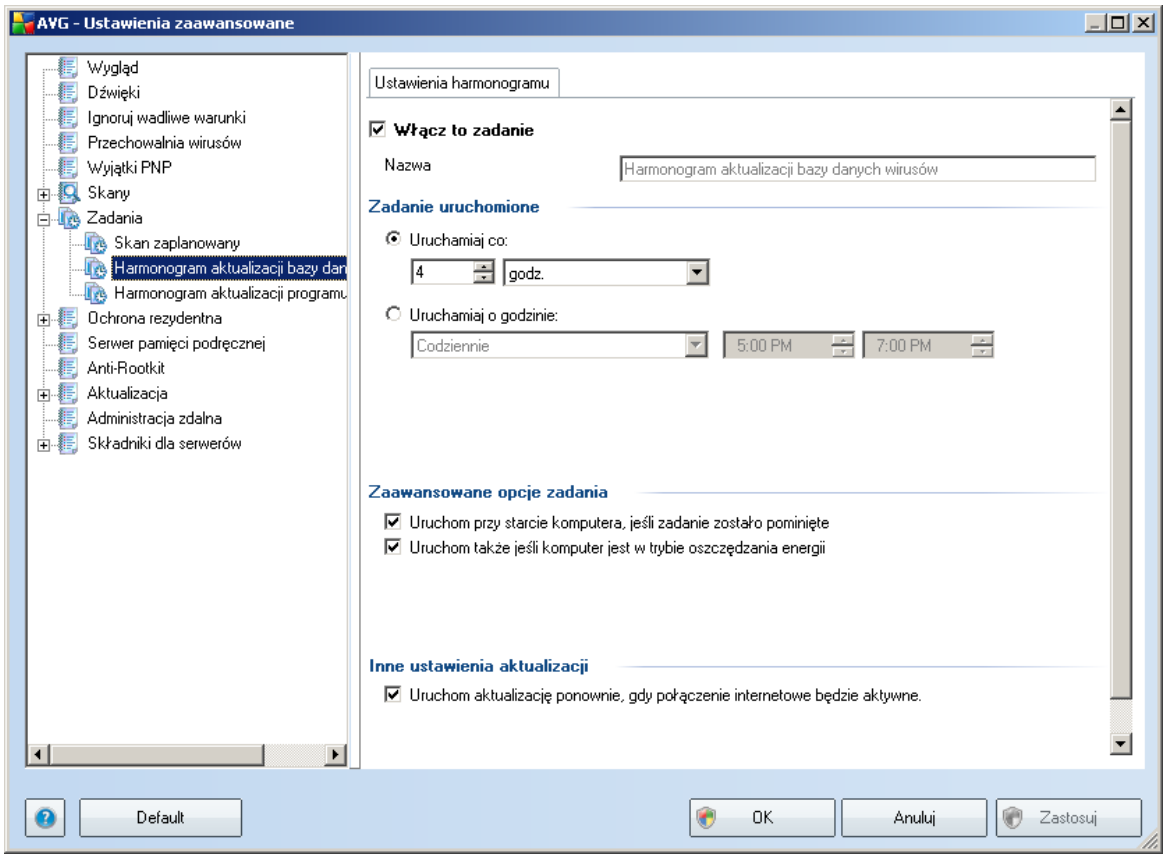
(***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).





Na karcie ***Co skanowac?*** mozna okreslic, czy planowane jest skanowanie calego komputera, czy skanowanie okreslonych plików lub folderów. W przypadku skanowania okreslonych plików lub folderów, w dolnej czesci okna dialogowego aktywowane jest drzewo katalogów, w którym mozna wybrac obiekty do przeskanowania.

10.7.2. Harmonogram aktualizacji bazy wirusów



Na karcie ***Ustawienia harmonogramu*** mozna odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana aktualizacje bazy wirusów i wlaczyc ja ponownie dopiero gdy zajdzie taka potrzeba.

Podstawowe opcje harmonogramu aktualizacji bazy wirusów dostepne sa w skladniku ***Menedzer aktualizacji***. W niniejszym oknie mozna ustawic szczególowe parametry harmonogramu:

W polu tekstowym ***Nazwa*** (*nieaktywne dla harmonogramów domyslnych*) jest wyswietlana nazwa przypisana do tego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (*aby dodac harmonogram, nalezy kliknac prawym przyciskiem myszy element* ***Harmonogram aktualizacji bazy wirusów*** *w drzewie nawigacji po lewej*) mozna okreslic wlasna nazwe, a wspomniane pole tekstowe jest edytowalne. Warto uzywac jak najkrótszych, opisowych nazw harmonogramów, aby potem móc je latwo identyfikowac.

Zadanie uruchomione

W tej sekcji nalezy okreslic interwal dla planowanych aktualizacji bazy danych wirusów. Aktualizacja moze byc powtarzana w okreslonych odstepach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia zdefiniowanego zdarzenia (***W oparciu o akcje, np. uruchomienie komputera***).

Zaawansowane opcje harmonogramu

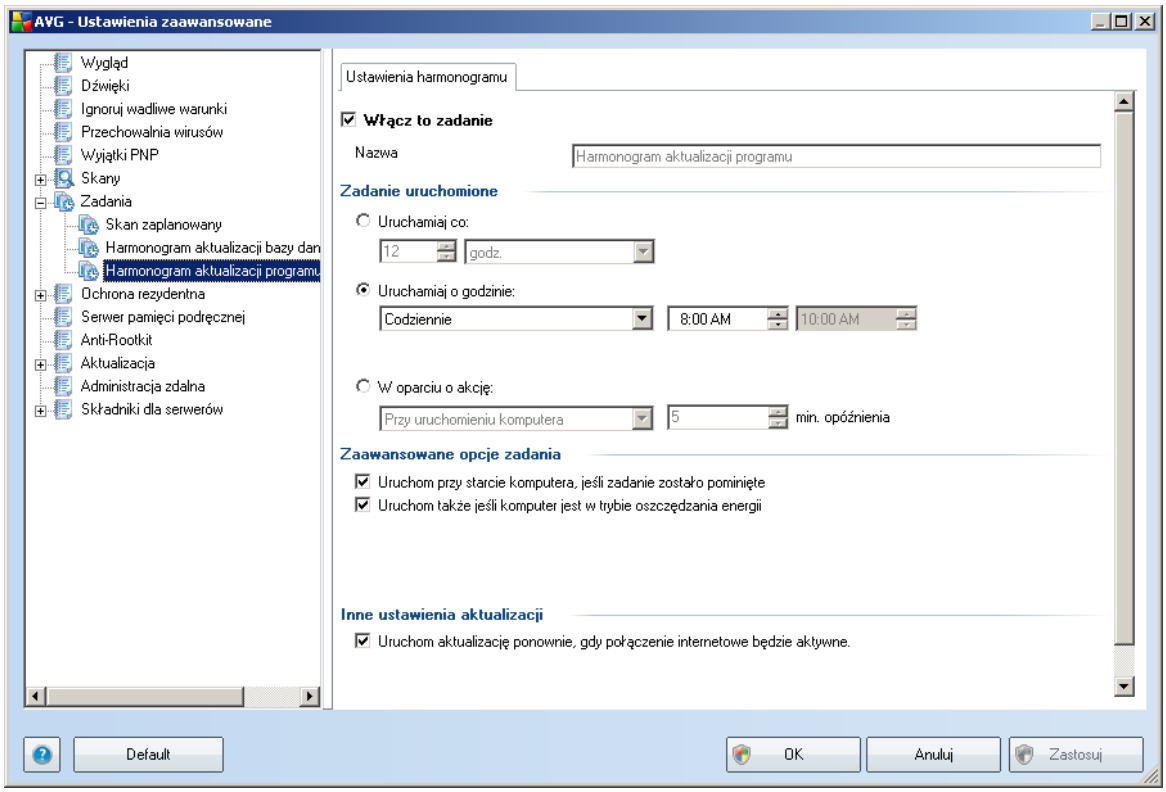
Ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

Inne ustawienia aktualizacji

Zaznacz opcje ***Uruchom aktualizacje ponownie po nawiazaniu polaczenia z internetem***, aby upewnic sie, ze jesli polaczenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie sie, po ponownym polaczeniu z internetem aktualizacja zostanie rozpoczeta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o okreslonej godzinie, nad ikona AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji* ***Ustawienia zaawansowane/Wyglad***).

10.7.3. Harmonogram aktualizacji programu



Na karcie ***Ustawienia harmonogramu*** mozna odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana aktualizacje programu i wlaczyc ja ponownie dopiero gdy zajdzie taka potrzeba.

W polu tekstowym ***Nazwa*** (*nieaktywne dla harmonogramów domyslnych*) jest wyswietlana nazwa przypisana do tego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (*aby dodac harmonogram, nalezy kliknac prawym przyciskiem myszy element* ***Harmonogram aktualizacji programu*** *w drzewie nawigacji po lewej*) mozna okreslic wlasna nazwe, a wspomniane pole tekstowe jest edytowalne. Warto uzywac jak najkrótszych, opisowych nazw harmonogramów, aby potem móc je latwo identyfikowac.

Zadanie uruchomione

W tym miejscu nalezy okreslic interwal dla nowo zaplanowanych aktualizacji programu. Uruchamianie aktualizacji moze byc powtarzane w okreslonych odstepach czasu (

Uruchamiaj co) lub w zadanych momentach (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia okreslonego zdarzenia (***akcja powiazana z uruchomieniem komputera***).

Zaawansowane opcje harmonogramu

Ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

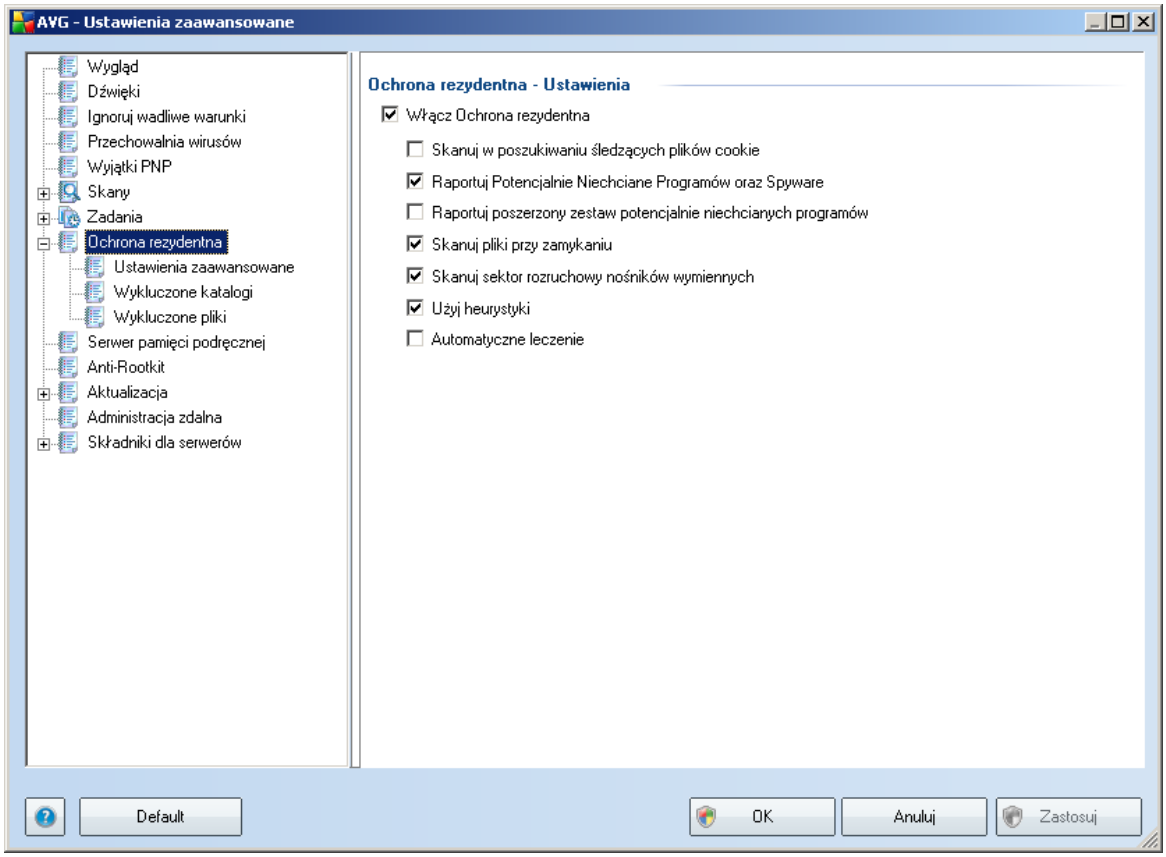
Inne ustawienia aktualizacji

Zaznacz opcje ***Uruchom aktualizacje ponownie po nawiazaniu polaczenia z internetem***, aby upewnic sie, ze jesli polaczenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie sie, po ponownym polaczeniu z internetem aktualizacja zostanie rozpoczeta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o okreslonej godzinie, nad ikona AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wyglad**)*.

10.8. Ochrona rezydentna

Skladnik ***Ochrona Rezydentna*** zapewnia aktywna ochrone plików i folderów przed wirusami, oprogramowaniem szpiegujacym i innymi zagrozeniami.



W oknie ***Ustawienia Ochrony rezydentnej*** mozna calkowicie wlaczyc lub wylaczyc ***Ochrone Rezydentna***, zaznaczajac lub odznaczajac pole ***Wlacz Ochrone Rezydentna*** (*opcja ta jest domyslnie wlaczona*). Ponadto, mozna aktywowac tylko wybrane funkcje ***Ochrony Rezydentnej***:

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** - parametr ten okresla, czy w czasie skanowania maja byc wykrywane pliki cookie. (*Pliki cookie w protokole HTTP sa uzywane do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach - np. preferencje dotyczace wygladu witryny lub zawartosc koszyka w sklepach internetowych.*)
- ***Raportuj potencjalnie niechciane programy i oprogramowanie***

szpiegujace- (*domyslnie wlaczone*) skanowanie w poszukiwaniu potencjalnie niechcianych programów (*plików wykonywalnych, które moga byc oprogramowaniem szpiegujacym lub reklamowym*).

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - (*domyslnie wylaczone*) wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona;

- ***Skanuj pliki przy zamykaniu*** - oznacza, ze system AVG skanuje aktywne obiekty (np. aplikacje, dokumenty itp.) nie tylko przy ich otwieraniu, ale takze przy zamykaniu. Funkcja ta pomaga chronic komputer przed pewnymi typami bardziej skomplikowanych wirusów.

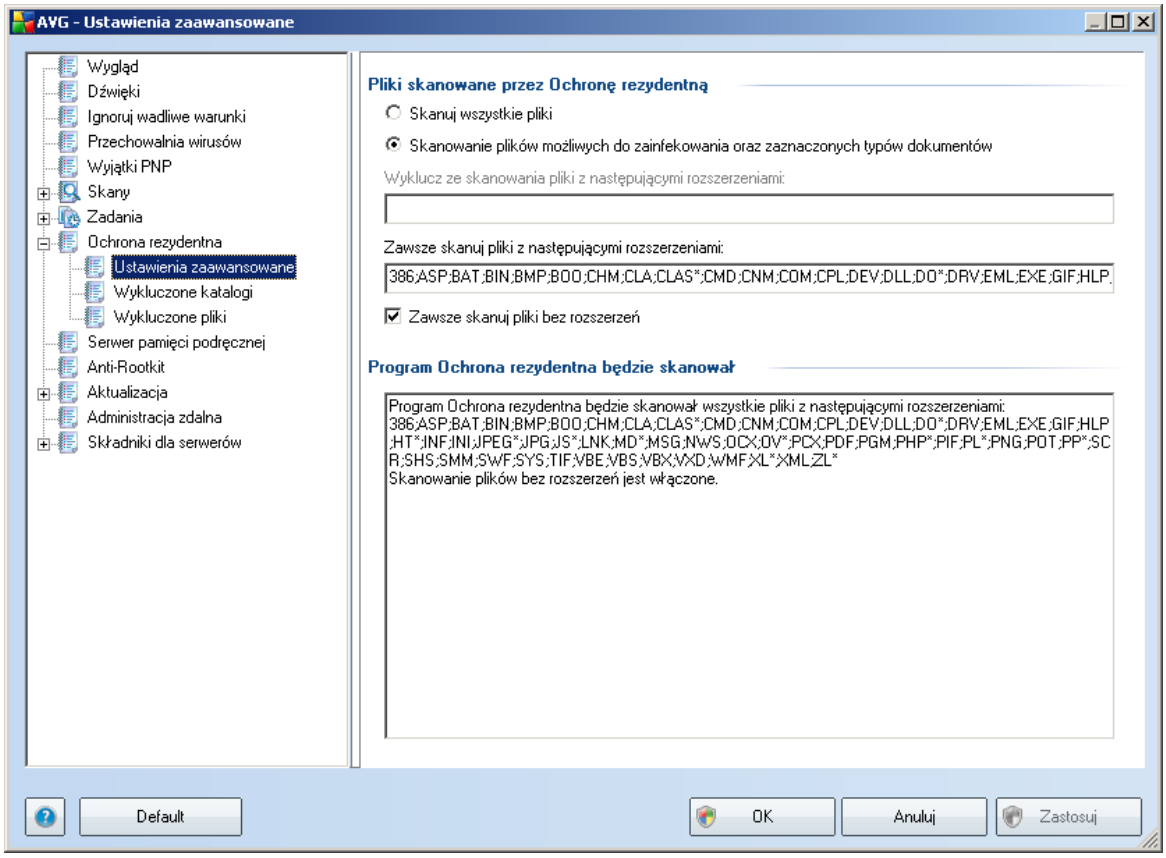
- ***Skanuj sektor rozruchowy nosników wymiennych*** - (*domyslnie wlaczona*)

- ***Uzyj heurystyki*** - (*domyslnie wlaczona*) do wykrywania bedzie uzywana heurystyka (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku maszyny wirtualnej*).

- ***Automatyczne leczenie*** - kazda wykryta infekcja bedzie automatycznie leczona (o ile jest to mozliwe).

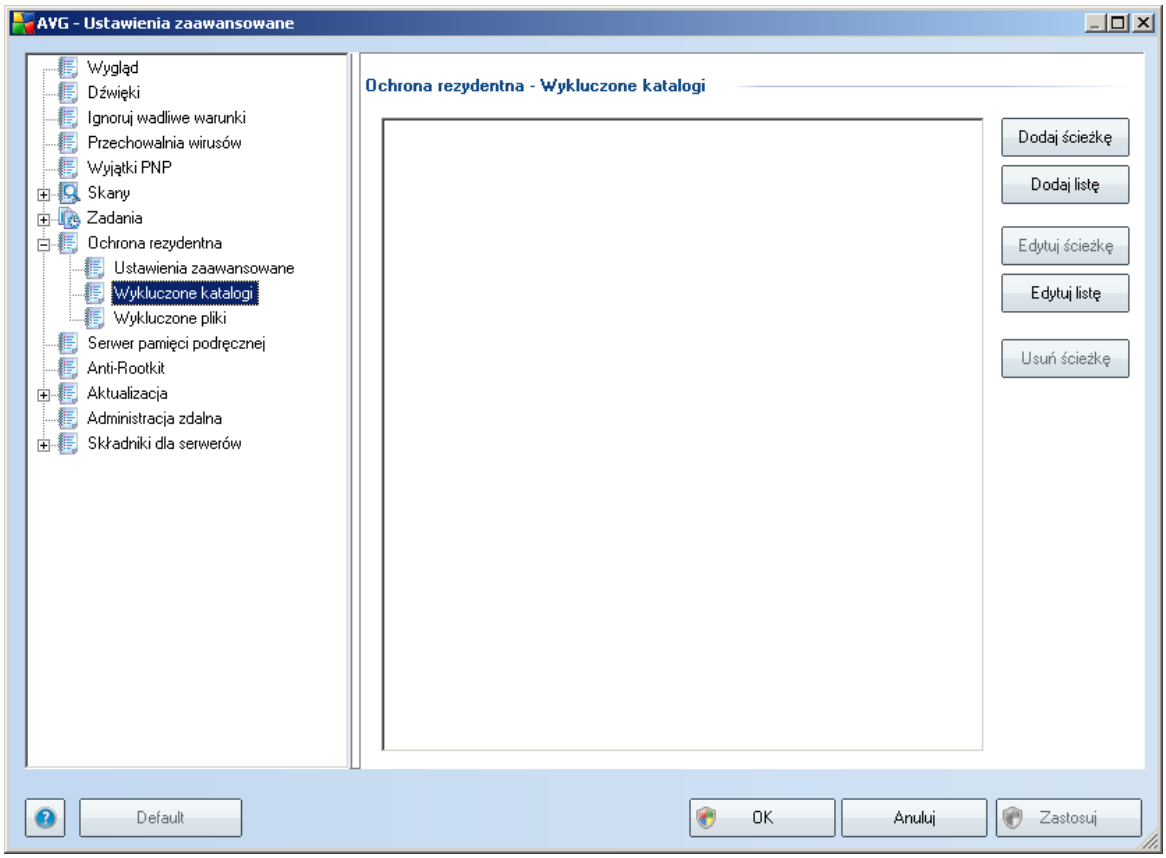
10.8.1. Ustawienia zaawansowane

W oknie ***Pliki skanowane przez Ochrone Rezydentna*** mozna okreslic, które pliki maja byc skanowane (*wedlug ich rozszerzen*):



Zdecyduj, czy chcesz skanowac tylko pliki infekowalne - jesli tak, bedziesz mógl okreslic liste rozszerzen plików, które maja byc wykluczone ze skanowania, oraz liste tych, które maja byc zawsze skanowane.

10.8.2. Wykluczenia katalogów



Okno ***Ochrona rezydentna - Wykluczone katalogi*** pozwala definiowac foldery, które maja byc wykluczone ze skanowania przez ***Ochrone Rezydentna.***

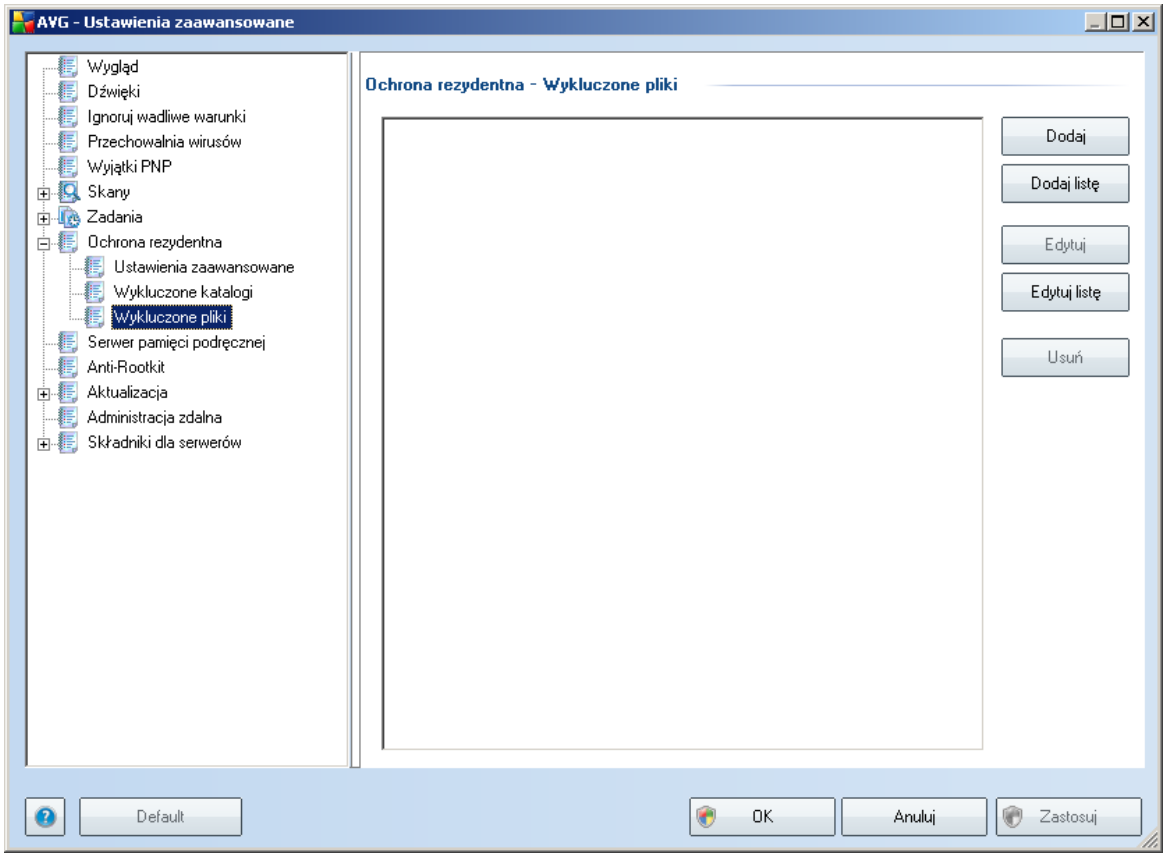
Jesli nie jest to koniecznie, zdecydowanie zalecamy nie wykluczac zadnych katalogów ze skanowania!

W biezacym oknie dostepne sa nastepujace przyciski kontrolne:

- ***Dodaj sciezke***- umozliwia okreslenie folderów, które maja zostac wykluczone ze skanowania, przez wybranie ich kolejno w drzewie obrazujacym strukture katalogów.
- ***Dodaj liste***- umozliwia podanie listy katalogów, które zostana wykluczone ze skanowania przez ***Ochrone Rezydentna***.

- ***Edytuj sciezke***- umozliwia edycje sciezki do wybranego folderu.
- ***Edytuj liste***- umozliwia edycje listy folderów.
- ***Usun sciezke***- umozliwia usuniecie z listy wybranego folderu.

10.8.3. Wykluczone pliki



Okno dialogowe ***Ochrona rezydentna - wykluczone pliki*** zachowuje sie w taki sam sposób co poprzednio opisane okno ***Ochrona rezydentna - wykluczone katalogi***, ale zamiast folderów mozna w nim okreslic pliki, które maja zostac wykluczone ze skanowania przez ***Ochrone rezydentna.***

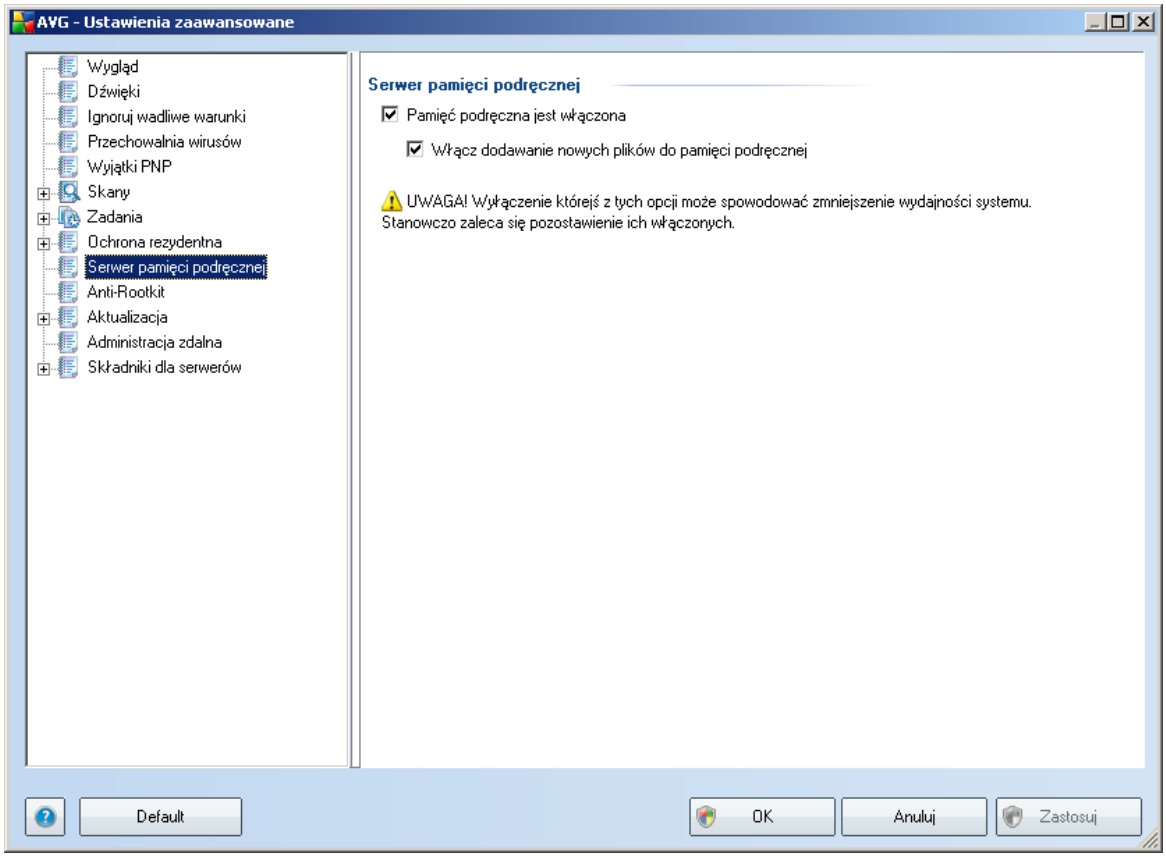
Jesli nie jest to koniecznie, zdecydowanie zalecamy nie wylaczac zadnych katalogów ze skanowania!

W biezacym oknie dostepne sa nastepujace przyciski kontrolne:

- ***Dodaj***- umozliwia okreslenie katalogów, które maja zostac wykluczone ze skanowania, przez wybranie ich kolejno w drzewie nawigacyjnym dysku lokalnego.
- ***Dodaj liste***- umozliwia podanie listy plików, które zostana wylaczone ze skanowania przez skladnik ***Ochrona rezydentna***.
- ***Edytuj*** - umozliwia edycje sciezki dostepu do wybranego pliku.
- ***Edytuj liste*** - umozliwia edycje listy plików.
- ***Usun***- umozliwia usuniecie z listy wybranej sciezki do pliku.

10.9. Serwer pamieci podrecznej

Funkcja ***Serwer pamieci podrecznej*** to tak naprawde proces majacy na celu przyspieszenie skanowania (*skanowania na zadanie, zaplanowanego skanowania calego komputera oraz skanowania skladnika Ochrona rezydentna*). Zbiera on i zachowuje informacje na temat bezpiecznych plików (*takich jak pliki systemowe z podpisem cyfrowym itp.*) - pliki te sa wówczas uwazane za bezpieczne i pomijane podczas skanowania.



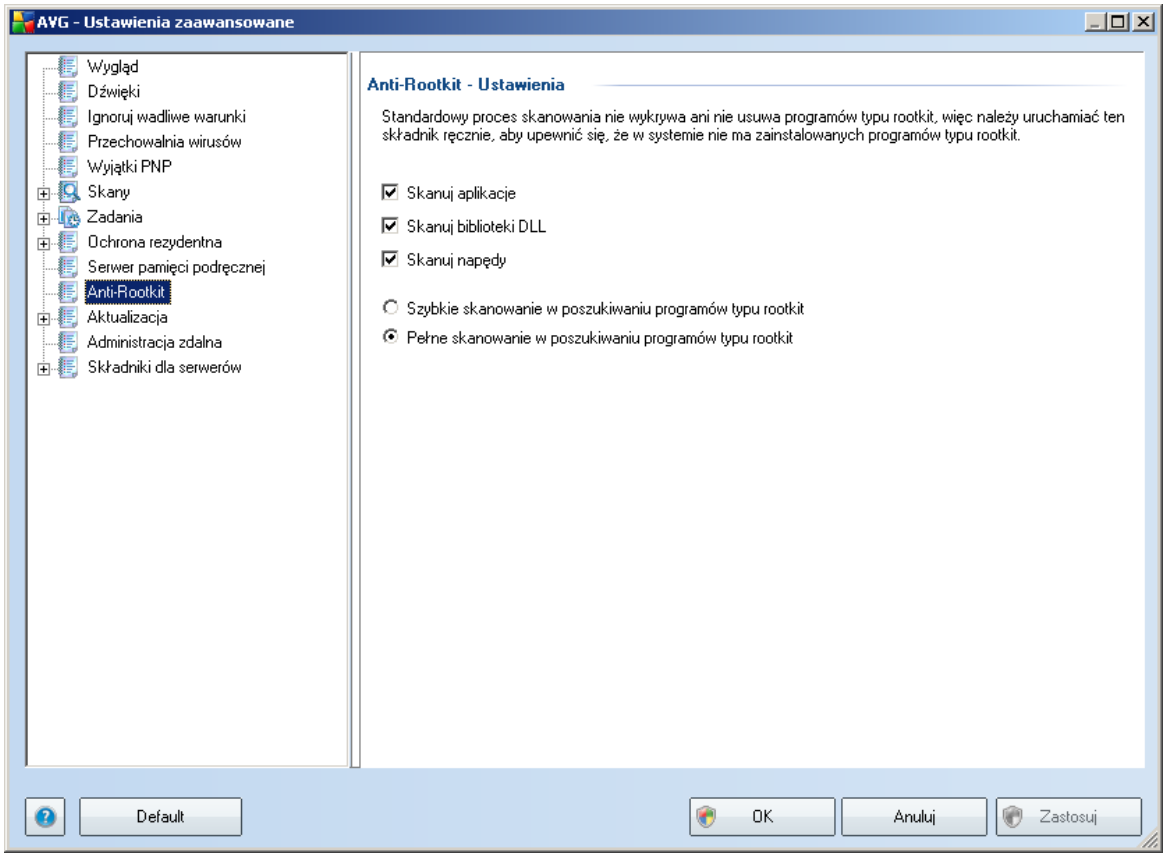
Okno dialogowe ustawien zawiera dwie opcje:

- ***Wlaczona pamiec podreczna*** (*opcja domyslnie wlaczona*) - odznaczenie tego pola powoduje wylaczenie funkcji ***Serwer pamieci podrecznej*** i opróznienie pamieci podrecznej. Nalezy pamietac, ze skanowanie moze spowolnic dzialanie komputera i zmniejszyc jego ogólna wydajnosc, poniewaz kazdy uzywany plik bedzie skanowany w poszukiwaniu wirusów i oprogramowania szpiegujacego.

- ***Wlacz dodawanie nowych plików do pamieci podrecznej*** (*opcja domyslnie wlaczona*) - odznaczenie tego pola umozliwia wylaczenie funkcji dodawania kolejnych plików do pamieci podrecznej. Wszystkie pliki zapisane w pamieci podrecznej sa w niej przechowywane dopóki funkcja nie zostanie zupelnie wylaczona lub do czasu kolejnej aktualizacji bazy wirusów.

10.10. Anti-Rootkit

W tym oknie dialogowym mozna edytowac konfiguracje skladnika ***Anti-Rootkit***:



Wszystkie funkcje skladnika ***Anti-Rootkit***dostepne w tym oknie dialogowym mozna takze edytowac bezposrednio w ***interfejsie skladnika Anti-Rootkit***.

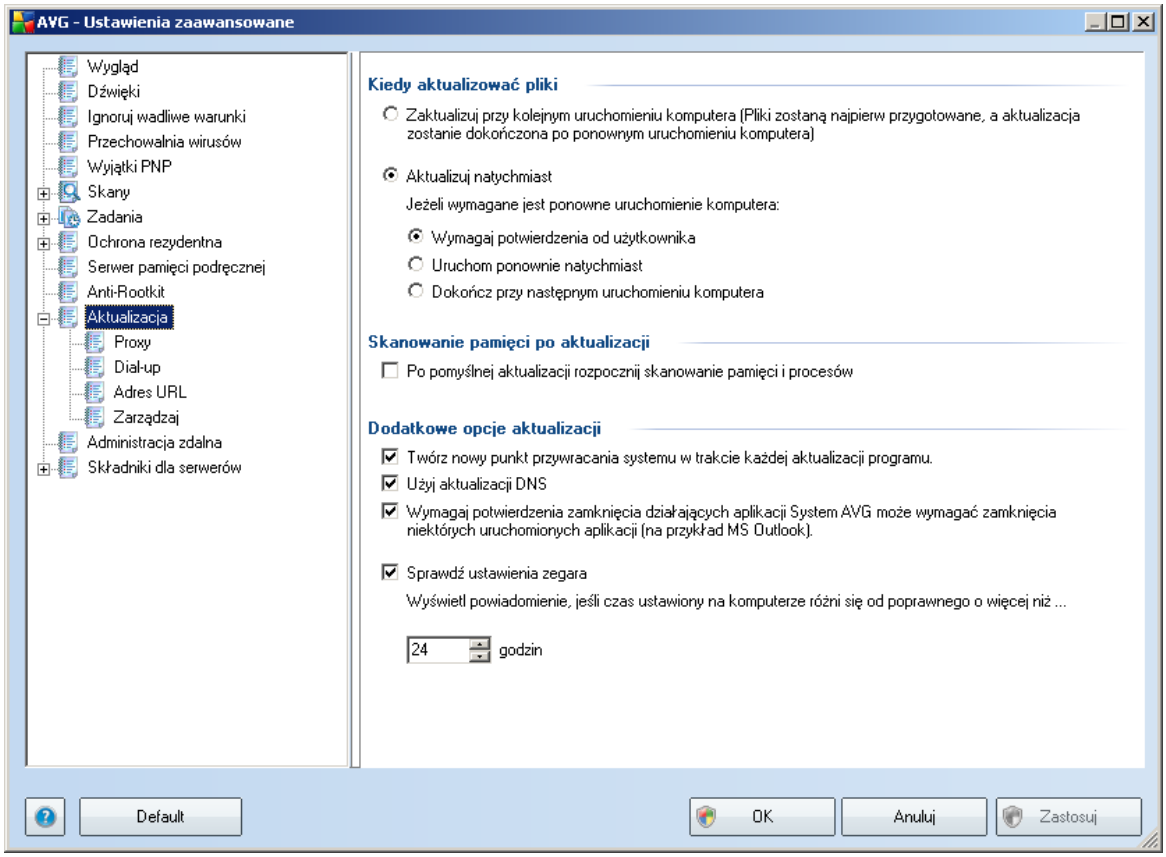
Zaznacz odpowiednie pola wyboru, aby okreslic obiekty, które maja byc skanowane:

- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj sterowniki***

Nastepnie nalezy wybrac tryb skanowania rootkitów:

- ***Szybkie skanowanie w poszukiwaniu programów typu rootkit*** - skanowany jest tylko folder systemowy (*zwykle C:\Windows*).
- ***Pelne skanowanie w poszukiwaniu programów typu rootkit*** - skanowane sa wszystkie dostepne dyski, oprócz A: i B:.

10.11. Aktualizacja



Kliknięcie pozycji ***Aktualizacja*** otwiera nowe okno dialogowe, w którym mozna okreslic ogólne parametry aktualizacji AVG:

Kiedy aktualizowac pliki

W tej sekcji mozna wybrac jedna z dwóch metod: zaplanowanie aktualizacji na najblizszy restart komputera lub uruchomienie aktualizacji natychmiast. Domyslnie

wybrana jest opcja natychmiastowa, poniewaz zapewnia ona maksymalny poziom bezpieczenstwa. Zaplanowanie aktualizacji na kolejne uruchomienie komputera zaleca sie tylko w przypadku, gdy komputer jest regularnie restartowany (co najmniej raz dziennie).

Przy pozostawienia konfiguracji domyslnej (natychmiastowe uruchomienie), mozna okreslic warunki ewentualnego restartu komputera:

- ***Wymagaj potwierdzenia od uzytkownika*** - przed zakonczeniem aktualizacji system zapyta uzytkownika o pozwolenie na restart komputera.
- ***Uruchom ponownie natychmiast*** - komputer zostanie automatycznie zrestartowany zaraz po zakonczeniu procesu aktualizacji - potwierdzenie ze strony uzytkownika nie jest wymagane.
- ***Dokoncz przy nastepnym uruchomieniu komputera*** - zakonczenie aktualizacji zostanie odlozone do najblizszego restartu komputera. Nalezy pamietac, ze opcja ta jest zalecana tylko w przypadku, gdy komputer jest regularnie uruchamiany (co najmniej raz dziennie).

Skanowanie pamieci po aktualizacji

Pole to nalezy zaznaczyc, jesli po kazdej pomyslnej aktualizacji system ma uruchamiac skanowanie pamieci. Pobrana aktualizacja mogla zawierac nowe definicje wirusów, które moga zostac zastosowane podczas takiego skanowania.

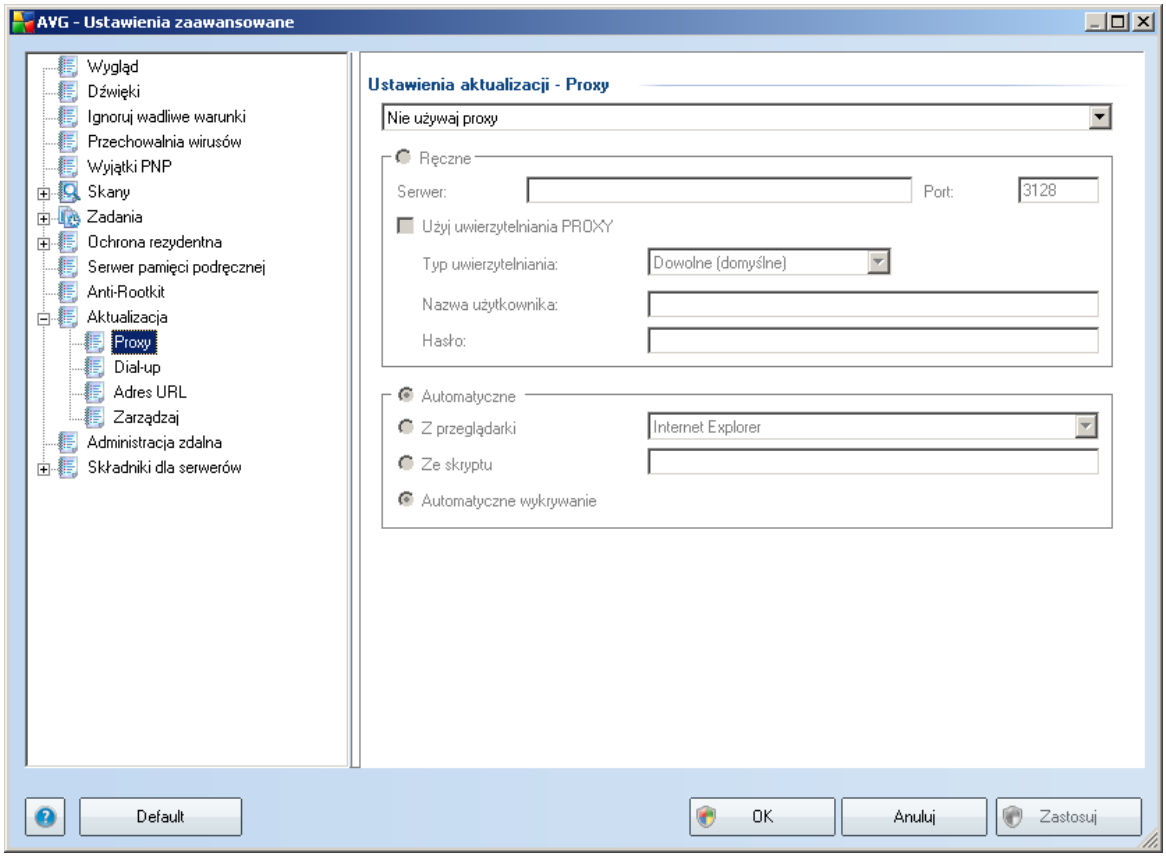
Dodatkowe opcje aktualizacji

- ***Twórz nowy punkt przywracania systemu po kazdej aktualizacji programu*** - przed kazdym uruchomieniem aktualizacji systemu AVG tworzony bedzie punkt przywracania systemu. Przy jego uzyciu mozliwe bedzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Aby przywrócic system, nalezy wybrac kolejno: Start / Wszystkie programy / Akcesoria / Narzedzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoswiadczonym uzytkownikom! Aby korzystac z tej funkcji, pole wyboru musi pozostac zaznaczone.
- ***Uzyj aktualizacji DNS*** - zaznacz to pole, aby potwierdzic, ze chcesz uzywac metody wykrywania nowych aktualizacji, która ogranicza ilosc danych przesylanych miedzy serwerem aktualizacyjnym a klientem AVG.

- ***Wymagaj potwierdzenia zamkniecia dzialajacych aplikacji*** (*domyslnie wlaczona*) - daje pewnosc, ze zadne dzialajace aplikacje nie zostana zamkniete bez potwierdzenia ze strony uzytkownika, jesli do zakonczenia aktualizacji bedzie wymagane ponowne uruchomienie komputera.

- ***Sprawdz ustawienia zegara*** - zaznacz to pole jesli chcesz, aby program AVG wyswietlil powiadomienie, gdy róznica miedzy wlasciwym a lokalnym czasem komputera przekroczy okreslona wartosc.

10.11.1. Proxy



Serwer proxy jest samodzielnym serwerem lub uruchomiona na komputerze usluga gwarantujaca bezpieczniejsze polaczenie internetowe. Zgodnie z okreslonymi w Twojej sieci zasadami, polaczenie internetowe moze odbywac sie bezposrednio lub poprzez serwer proxy. Mozna takze zezwolic na korzystanie z obu opcji jednoczesnie. Dlatego tez w oknie ***Ustawienia aktualizacji - Proxy*** nalezy najpierw wybrac jedna z dostepnych opcji:

- ***Uzywaj proxy***
- ***Nie uzywaj serwera proxy*** - ustawienia domyslne
- ***Spróbuj polaczyc przy uzyciu proxy, a w razie niepowodzenia polacz bezposrednio***

W przypadku wybrania opcji uzycia serwera proxy nalezy podac dalsze informacje. Ustawienia serwera moga zostac skonfigurowane recznie lub automatycznie.

Konfiguracja reczna

W przypadku wybrania konfiguracji recznej (zaznaczenie *opcji* ***Recznie*** *aktywuje odpowiednia sekcje*) nalezy podac nastepujace informacje:

- ***Serwer*** - okresl adres IP lub nazwe serwera
- ***Port*** - okresl numer portu umozliwiajacego dostep do internetu (*domyslnie jest to port 3128, ale moze byc ustawiony inaczej; w przypadku watpliwosci nalezy skontaktowac sie z administratorem sieci*).

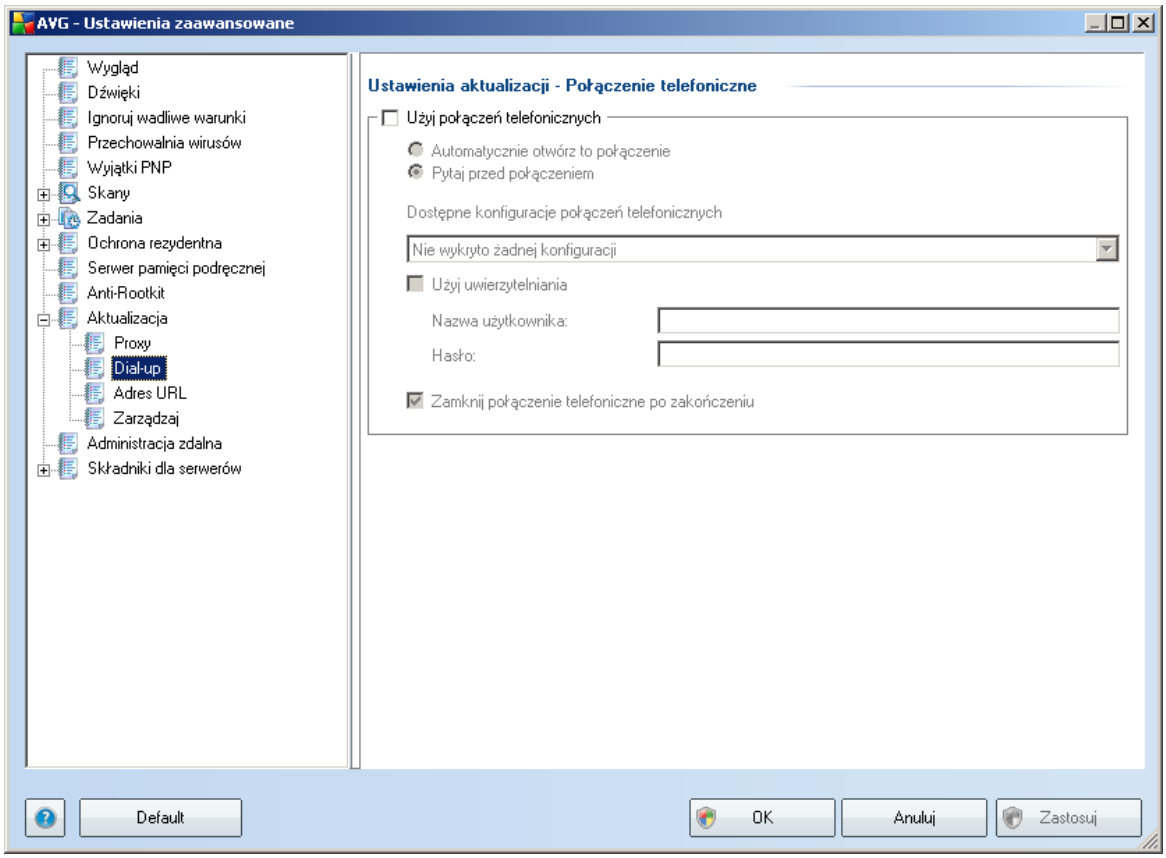
Zdarza sie, ze na serwerze proxy dla kazdego uzytkownika skonfigurowane sa odrebne reguly. Jesli serwer proxy jest skonfigurowany w ten sposób, nalezy zaznaczyc opcje ***Uzyj uwierzytelniania PROXY***, aby serwer weryfikowal nazwe uzytkownika i haslo przed nawiazaniem polaczenia.

Konfiguracja automatyczna

W przypadku wybrania konfiguracji automatycznej (*zaznaczenie opcji* ***Automatycznie*** *aktywuje odpowiedni obszar okna dialogowego*) nalezy wskazac, skad ma zostac pobrana konfiguracja proxy:

- ***Z przegladarki*** - konfiguracja zostanie odczytana z domyslnej przegladarki internetowej.
- ***Ze skryptu*** - konfiguracja zostanie odczytana z pobranego skryptu zawierajacego funkcje zwracajaca adres serwera proxy.
- ***Automatyczne wykrywanie*** - konfiguracja zostanie wykryta automatycznie bezposrednio na serwerze proxy.

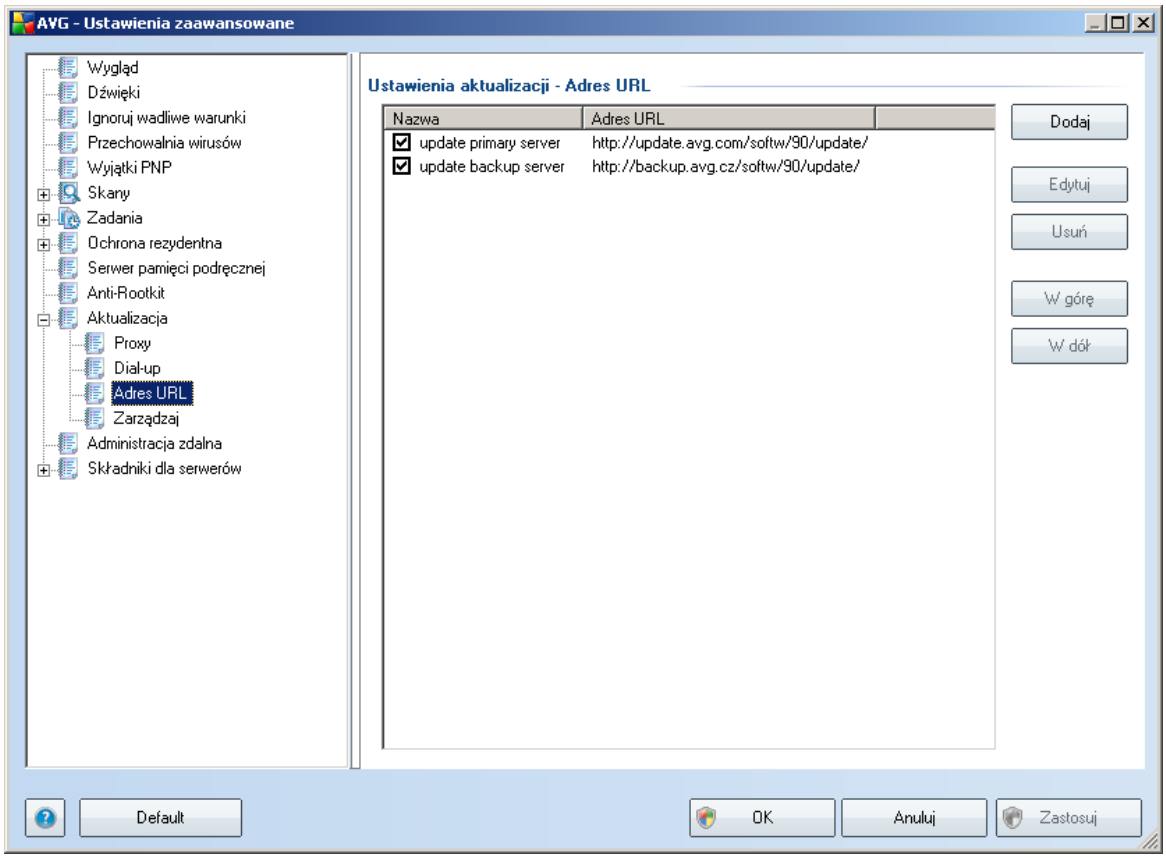
10.11.2. Polaczenie telefoniczne



Wszystkie opcjonalne parametry podawane w oknie ***Ustawienia aktualizacji - Polaczenie telefoniczne*** odnosza sie do polaczenia dial-up z internetem. Pola tego okna pozostaja nieaktywne az do zaznaczenia opcji ***Uzyj polaczen telefonicznych.***

Nalezy okreslic, czy polaczenie z internetem zostanie nawiazane automatycznie (***Automatycznie otwórz to polaczenie***), czy tez realizacje polaczenia nalezy zawsze potwierdzac recznie (***Pytaj przed polaczeniem***). W przypadku laczenia automatycznego nalezy takze okreslic, czy polaczenie ma byc zamykane natychmiast po zakonczeniu aktualizacji (***Zamknij polaczenie telefoniczne po zakonczeniu***).

10.11.3. URL



W oknie ***URL*** znajduje sie lista adresów internetowych, z których mozna pobierac pliki aktualizacyjne. Liste i jej elementy mozna modyfikowac za pomoca nastepujacych przycisków kontrolnych:

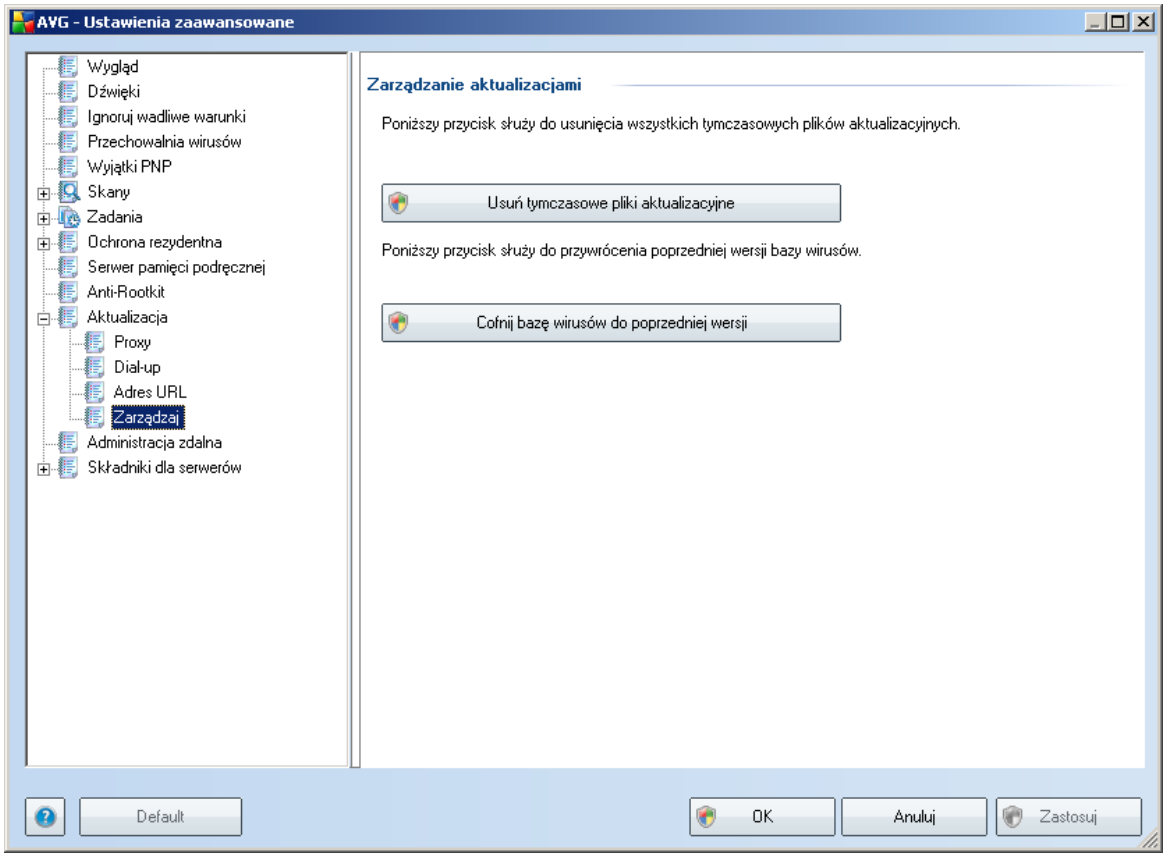
- ***Dodaj***- powoduje otwarcie okna dialogowego umozliwiajacego okreslenie nowego adresu URL, który zostanie dodany do listy.
- ***Edytuj*** - powoduje otwarcie okna dialogowego umozliwiajacego edycje parametrów wybranego adresu URL.
- ***Usun***- powoduje usuniecie wybranego adresu z listy.
- ***Do góry/W dól*** - te dwa przyciski pelnia wazna role. Pierwszy serwer na liscie jest zawsze uzywany jako pierwszy przy próbie pobrania aktualizacji. Dlatego tez przesuwanie serwerów na tej liscie w góre lub w dól stanowi w

rzeczywistosci okreslanie ich priorytetu. Przycisk ***Do góry*** przesuwa wybrany adres URL na liscie o jedna pozycje w góre, podczas gdy przycisk ***W dól*** - o jedna pozycje w dól.

Usuniecie zaznaczenia pola obok nazwy serwera tymczasowo wylacza go (bez potrzeby calkowitego usuwania go z listy).

10.11.4. Zarzadzaj

Okno dialogowe ***Zarzadzaj*** zawiera dwa przyciski:

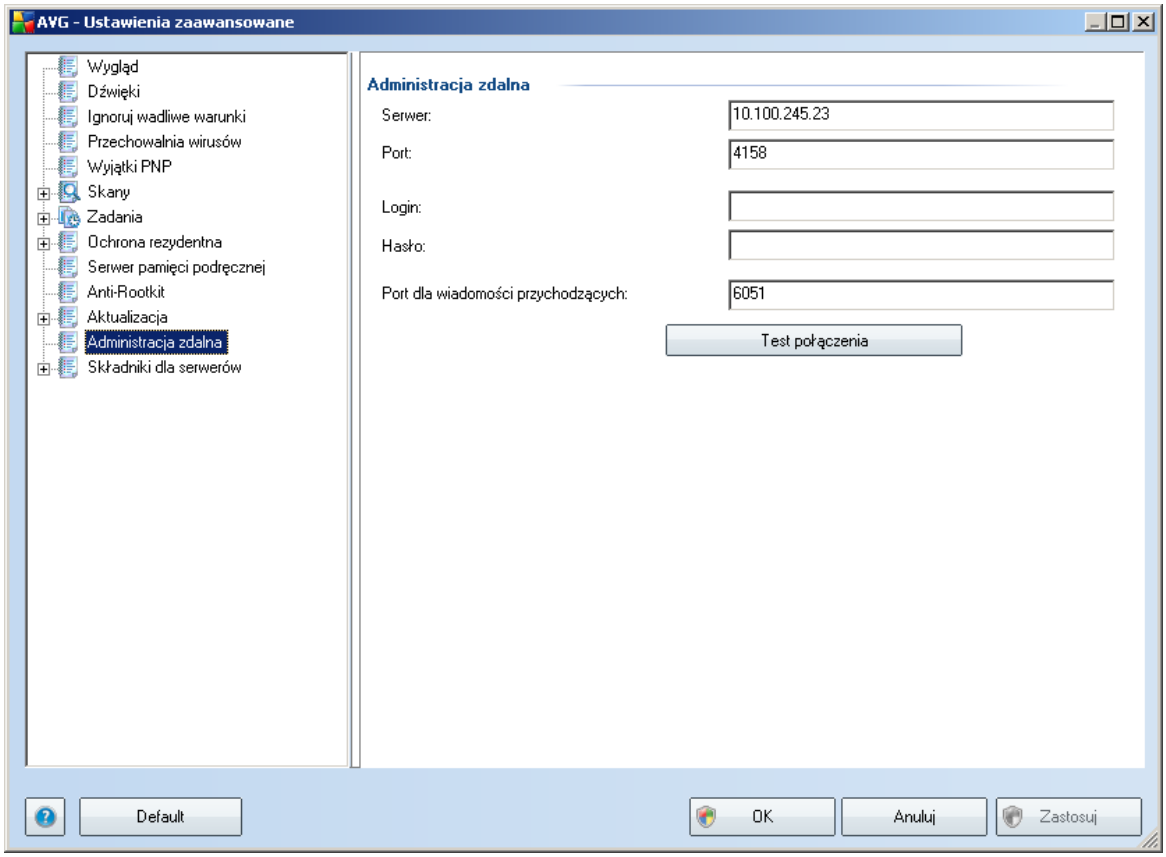


- ***Usun tymczasowe pliki aktualizacyjne*** - pozwala usunac z dysku twardego wszystkie zbedne pliki aktualizacyjne (*sa one domyslnie przechowywane przez 30 dni*)
- ***Cofnij baze wirusów do poprzedniej wersji*** - pozwala usunac z dysku twardego ostatnia wersje bazy wirusów i przywrócic ja do poprzedniego stanu

(*nowa baza bedzie czescia najblizszej aktualizacji*)

10.12. Administracja zdalna

Pozycja ***Administracja zdalna*** jest wyswietlana w przegladzie ***ustawien zaawansowanych*** tylko, jesli wczesniej wybrano jej instalacje, tj. gdy podczas procesu instalacji zaznaczono te opcje w oknie dialogowym ***Wybór skladników***:



Ustawienia ***Administracji zdalnej*** okreslaja sposób laczenia sie stacji roboczej AVG z systemem administracji zdalnej. Jesli dana stacja ma laczyc sie ze zdalnym serwerem administracyjnym, nalezy okreslic nastepujace parametry:

- ***Serwer*** - nazwa (lub adres IP) serwera, na którym zainstalowano oprogramowanie AVG Admin Server.
- ***Port*** - numer portu, przez który klient AVG komunikuje sie z serwerem AVG Admin Server (*za domyslny uwazany jest port 4158 - jesli ma byc uzywany,*

nie trzeba go wprowadzac).

- ***Login*** - jesli uzywana jest opcja bezpiecznej komunikacji miedzy klientem AVG i oprogramowaniem AVG Admin Server, nalezy podac nazwe uzytkownika.
- ***Haslo*** - wymagane, jesli podano login.
- ***Port dla wiadomosci przychodzacych*** - numer portu, na którym klient AVG odbiera wiadomosci od serwera AVG Admin Server.

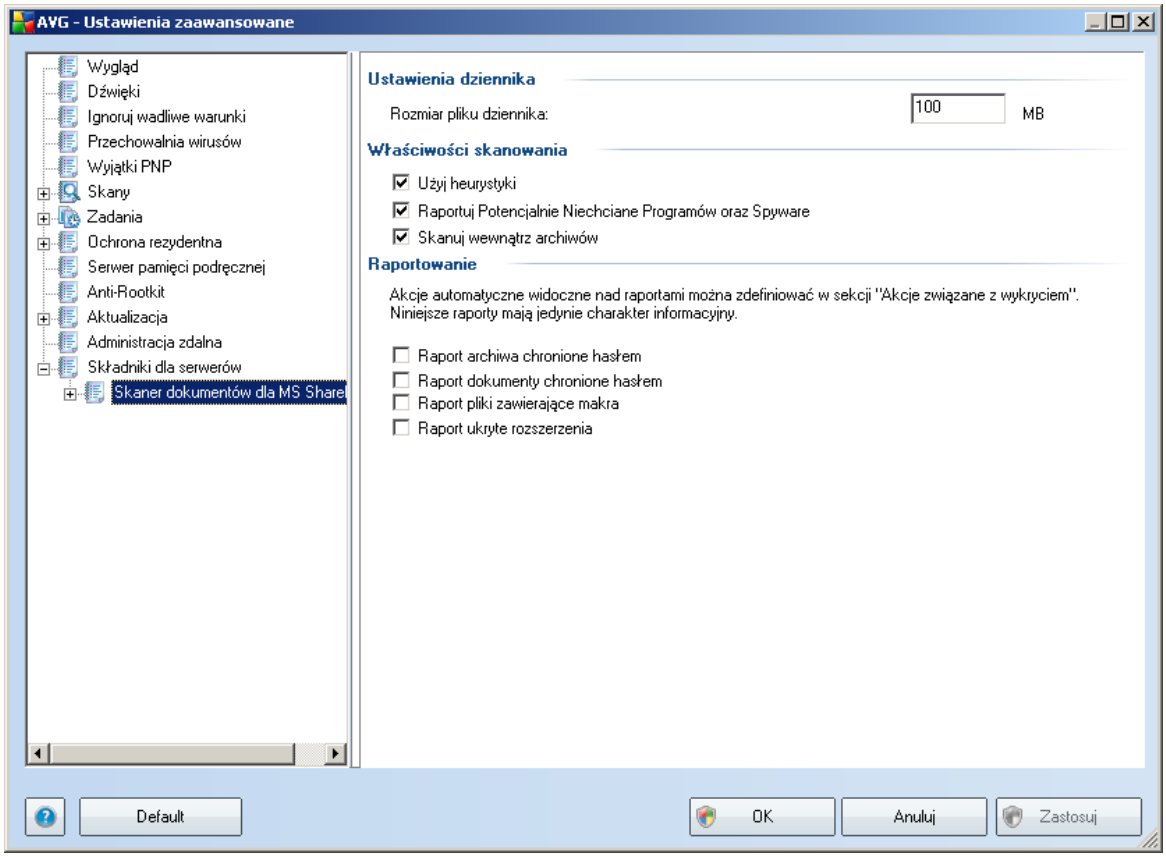
Przycisk·***Testuj polaczenie*** pozwala sprawdzic, czy wszystkie powyzsze dane sa prawidlowe i zapewnia pomyslne polaczenie z baza danych DataCenter.

Uwaga: *Szczególowy opis funkcji administracji zdalnej zawiera dokumentacja programu AVG Business Edition.*

10.13. Skladniki serwera

10.13.1. Skaner dokumentów dla MS SharePoint

To okno dialogowe zawiera kilka wstepnie ustawionych opcji dotyczacych wydajnosci ***Skanera dokumentów dla MS SharePoint*** podczas wyszukiwania wirusów w dokumentach. Okno dialogowe podzielone jest na kilka·obszarów:



Ustawienia dziennika

Rozmiar pliku dziennika - plik dziennika zawiera zapisy zdarzen powiazanych ze skladnikiem ***Skaner dokumentów dla MS SharePoint***, np. uwagi dotyczace ladowania bibliotek, odnalezienia wirusów, ostrzezen itp. To pole pozwala okreslic maksymalny rozmiar pliku dziennika.

Wlasciwosci skanowania

- ***Uzyj analizy heurystycznej*** - zaznaczenie tego pola umozliwia korzystanie z analizy heurystycznej podczas skanowania dokumentów. Gdy ta opcja jest wlaczona, mozliwe jest filtrowanie dokumentów·nie tylko wedlug ich rozszerzenia, ale równiez na podstawie ich wlasciwej zawartosci.

- ***Raportuj potencjalnie niechciane programy i oprogramowanie***

szpiegujace - zaznaczenie tego pola umozliwia korzystanie z silnika Anti-Spyware, tj. zglaszanie podejrzanych i potencjalnie niechcianych programów w czasie skanowania dokumentów.

- ***Skanuj wewnatrz archiwów*** - zaznaczenie tego pola umozliwi skanowanie zawartosci archiwów.

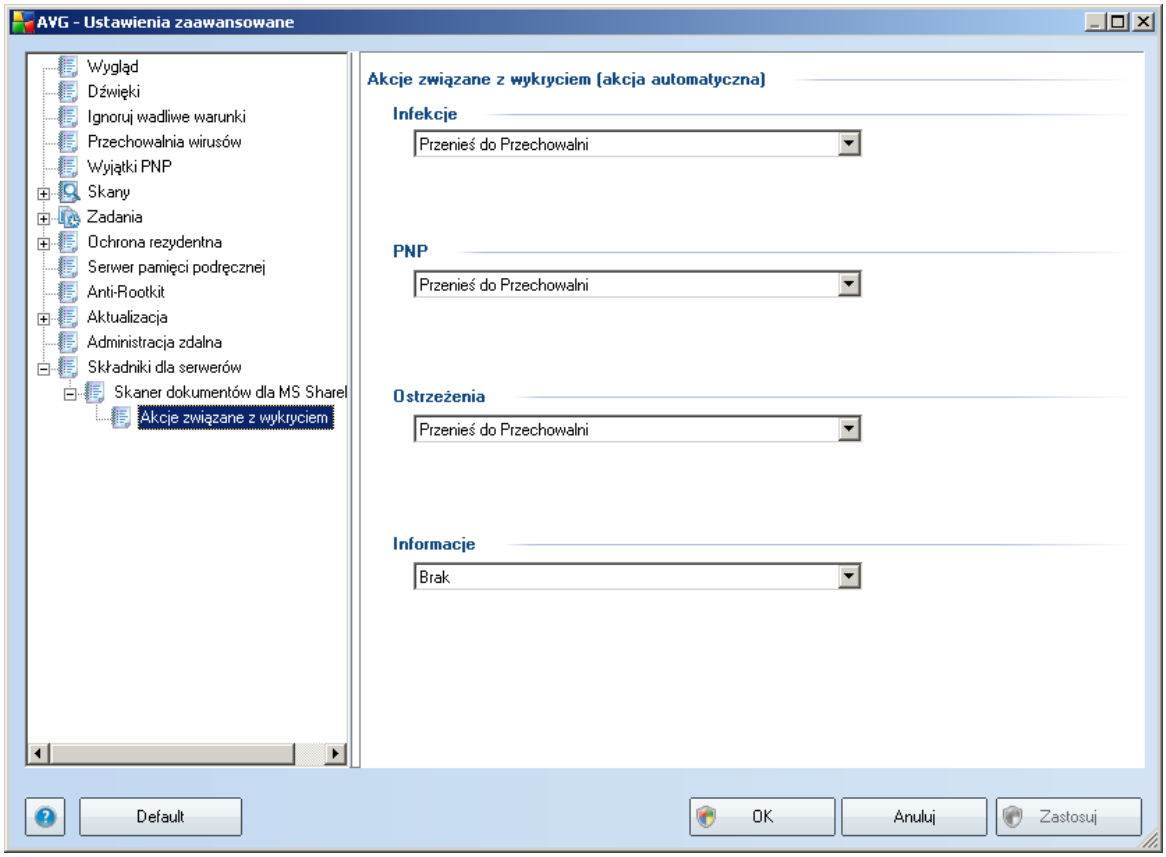
Raportowanie

- ***Raportuj archiwa chronione haslem*** - archiwów (ZIP, RAR itp.) chronionych haslem nie mozna skanowac w poszukiwaniu wirusów. Nalezy zaznaczyc to pole wyboru, aby system AVG zglaszal je jako potencjalnie niebezpieczne.

- ***Raportuj dokumenty chronione haslem*** - dokumentów chronionych haslem nie mozna skanowac w poszukiwaniu wirusów. Nalezy zaznaczyc to pole wyboru, aby system AVG zglaszal je jako potencjalnie niebezpieczne.

- ***Raportuj pliki zawierajace makra*** - makro to predefiniowana sekwencja kroków majaca ulatwiac wykonywanie okreslonych czynnosci (szeroko znane sa np. makra programu MS Word). Makra moga byc potencjalnie niebezpieczne - warto zaznaczyc to pole, aby miec pewnosc, ze pliki zawierajace makra beda raportowane jako podejrzane.

- ***Raportuj ukryte rozszerzenia*** - ukryte rozszerzenia moga maskowac podejrzane pliki wykonywalne (np. plik.txt.exe) jako niegrozne pliki tekstowe (np. plik.txt). Nalezy zaznaczyc to pole wyboru, aby zglaszac je jako potencjalnie niebezpieczne.



W tym oknie dialogowym mozna skonfigurowac sposób dzialania ***Skanera dokumentów dla MS SharePoint*** po wykryciu zagrozenia. Zagrozenia dziela sie na kilka kategorii:

- ***Infekcje*** - szkodliwy kod, który sam sie powiela, czesto pozostaje niezauwazony do czasu, gdy wyrzadzi szkody.
- PNP (potencjalnie niechciane programy) - takie programy moga stanowic powazne zagrozenie komputera, lub jedynie potencjalne ryzyko naruszenia prywatnosci.
- ***Ostrzezenia*** - dotycza obiektów, których nie mozna przeskanowac.
- ***Informacje*** - wszystkie wykryte potencjalne zagrozenia, których nie mozna przypisac do kategorii wymienionych powyzej.

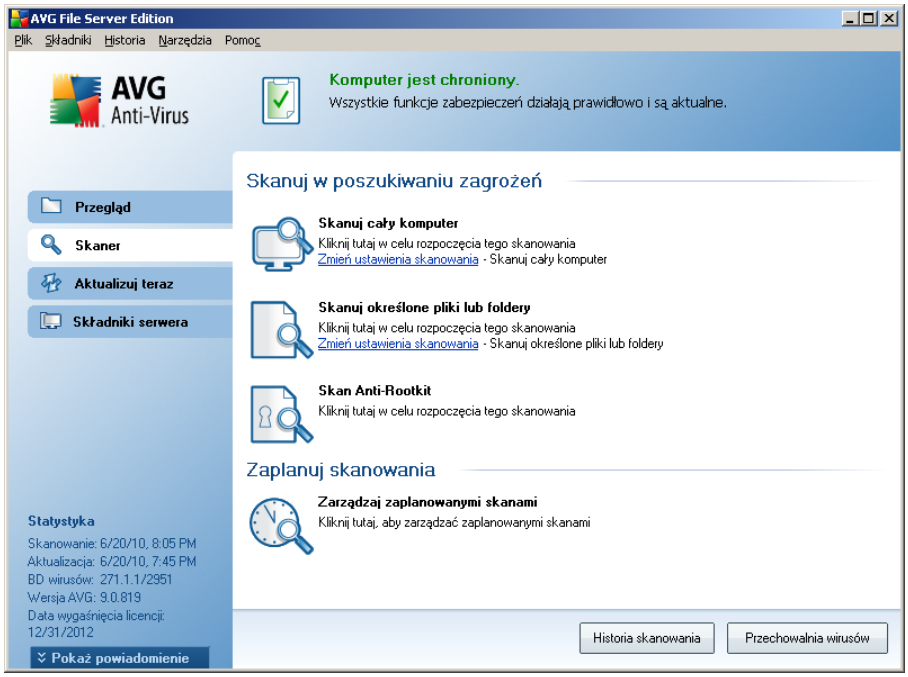
Akcje automatyczna dla kazdej kategorii mozna wybrac za pomoca menu rozwijanych:

- ***Brak*** - dokument zawierajacy takie zagrozenie nie bedzie przetwarzany.
- ***Przenies do Przechowalni****** - kazdy zainfekowany dokument zostanie przeniesiony do Przechowalni wirusów.
- ***Usun*** - dokument zawierajacy wirus zostanie usuniety.

11. Skanowanie AVG

Skanowanie jest podstawowym elementem funkcjonowania systemu **AVG 9.0 File Server**. Mozliwe jest uruchamianie testów na zadanie lub planowanie ich okresowego przeprowadzania o odpowiednich porach.

11.1. Interfejs skanowania



Interfejs skanera AVG dostepny jest za posrednictwem linku ***Skaner***. Kliknieciе go otwiera okno ***Skanuj w poszukiwaniu zagrozen***. Okno to zawiera nastepujace elementy:

- przeglad wstepnie zdefiniowanych testów - trzy·typy testów (zdefiniowane przez dostawce oprogramowania) sa gotowe do uzycia na zadanie lub wedlug utworzonego harmonogramu:
    - ***Skan calego komputera***
    - ***Skan okreslonych plików lub folderów***
    - ***Skan Anti-rootkit***

- Planowanie testów - w tym obszarze mozna definiowac nowe testy i tworzyc nowe harmonogramy w zaleznosci od potrzeb.

Przyciski kontrolne

Interfejs skanera zawiera nastepujace przyciski kontrolne:

- ***Historia skanowania*** - wyswietla okno dialogowe Przeglad wyników skanowania, które zawiera pelna historie testów.
- ***Przechowalnia wirusów*** - otwiera nowe okno z zawartoscia Przechowalni wirusów, w której izolowane sa wykryte infekcje.

11.2. Wstepnie zdefiniowane testy

Jedna z glównych funkcji systemu **AVG 9.0 File Server** jest skanowanie na zadanie. Testy na zadanie sluza do skanowania konkretnych obszarów komputera, gdy uzytkownik podejrzewa obecnosc wirusa. Stanowczo zaleca sie jednak wykonywanie tych testów regularnie, nawet w przypadku, gdy nie ma takich podejrzen.

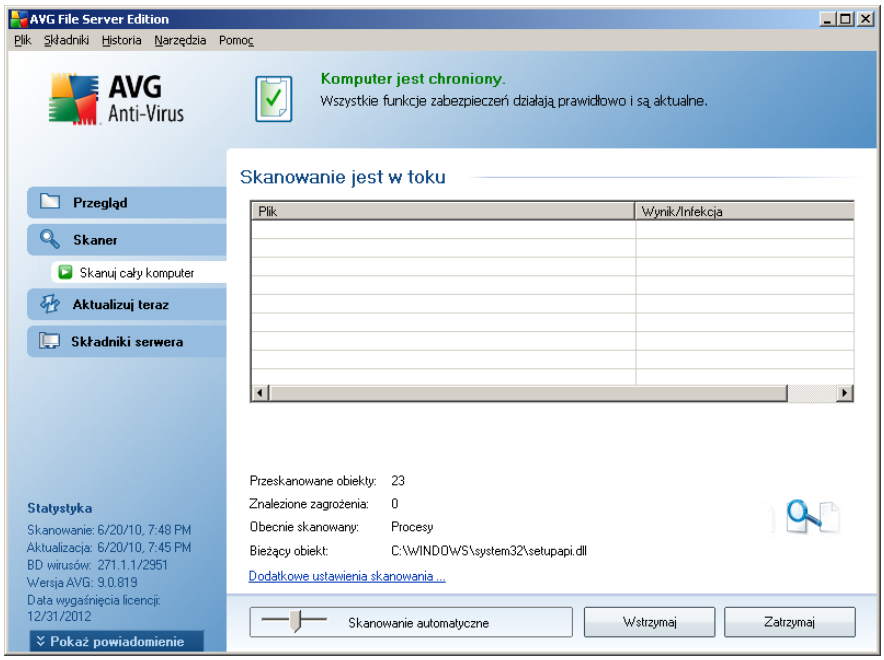
W systemie **AVG 9.0 File Server** dostepne sa nastepujace typy skanowania zdefiniowane wstepnie przez producenta:

11.2.1. Skan calego komputera

Skanuj caly komputer - skanuje caly komputer w poszukiwaniu mozliwych infekcji i/ lub potencjalnie niechcianych programów. Test ten obejmuje wszystkie dyski twarde komputera. Wykryte infekcje sa leczone lub przenoszone do ***Przechowalni wirusów***. Skanowanie calego komputera powinno byc regularnie przeprowadzane co najmniej raz na tydzien.

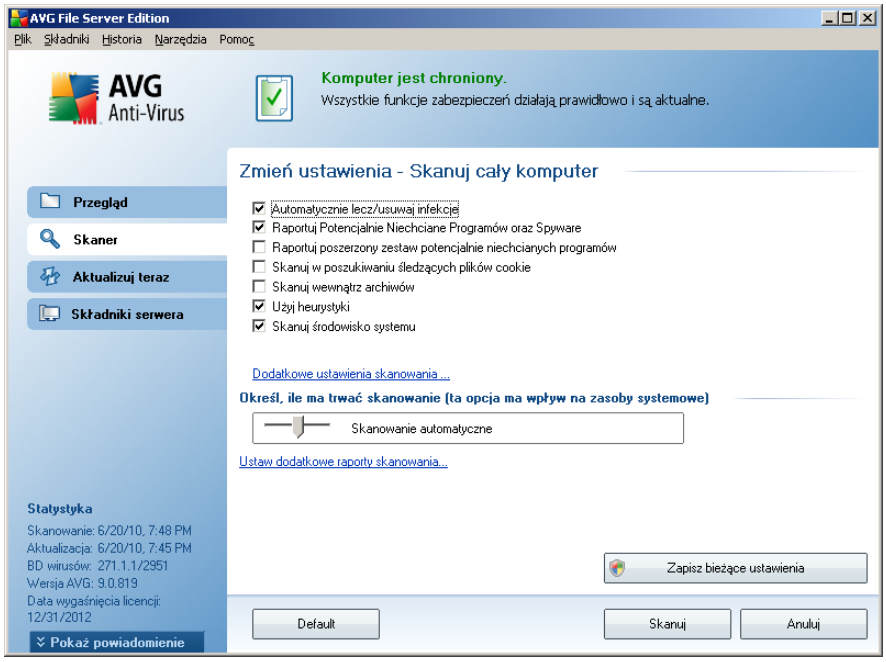
Uruchamianie skanowania

Skanowanie calego komputera mozna uruchomic bezposrednio z poziomu interfejsu skanera, klikajac ikone odpowiedniego testu. Dla tego skanowania nie mozna okreslac dalszych ustawien; jest ono uruchamiane natychmiast w oknie dialogowym ***Skanowanie w toku***. (*patrz ilustracja*). W razie potrzeby skanowanie mozna tymczasowo przerwac (***Wstrzymaj***) lub anulowac (***Zatrzymaj***).



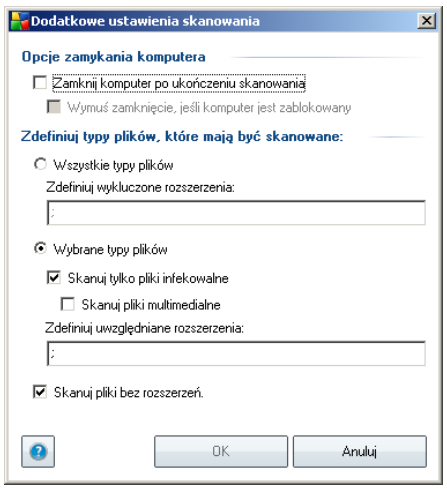
Edycja konfiguracji skanowania

Wstepne, domyslne ustawienia testu ***Skan calego komputera*** mozna latwo edytowac. Kliknięcie linku ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***Zmien ustawienia skanu calego komputera. Zaleca sie nie zmieniac ustawien domyslnych, jesli nie jest to konieczne!***



- ***Parametry skanowania*** - na liscie parametrów skanowania mozna wlaczyc/ wylaczyc okreslone parametry w zaleznosci od potrzeb. Wiekszosc parametrów jest domyslnie wlaczona i automatycznie uzywana podczas skanowania.

- ***Dodatkowe ustawienia skanowania*** - link do okna dialogowo ***Dodatkowe ustawienia skanowania***, w którym mozna okreslic nastepujace parametry:



- **_Opcje wylaczania komputera_** - okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (**_Zamknij komputer po ukonczeniu skanowania_**) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (**_Wymus zamkniecie, jesli komputer jest zablokowany_**).

- **_Zdefiniuj typy plików do skanowania_** - nalezy zdecydowac, które z ponizszych elementów maja byc skanowane:

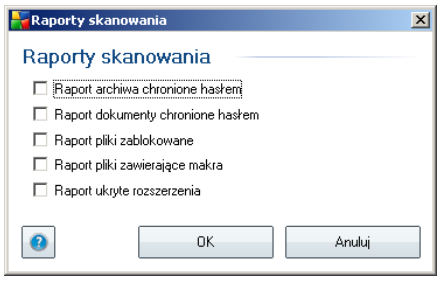
  - **_Wszystkie typy plików_** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

  - **_Wybrane typy plików_** - skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio - jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

  - Opcjonalnie mozna zdecydowac o **_skanowaniu plików bez rozszerzenia_** - ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- **_Priorytet procesu skanowania_** - za pomoca suwaka mozna zmienic priorytet procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- **_Ustaw dodatkowe raporty skanowania_** - link ten pozwala otworzyc nowe okno dialogowe **_Raporty skanowania_**, w którym mozna okreslic elementy lub zdarzenia, które maja byc zglaszane:



Ostrzezenie: *Ustawienia te sa identyczne jak domyslne parametry nowo utworzonych testów - zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanowac****. Jesli jednak domyslna konfiguracja testu* ***Skan calego komputera*** *zostanie zmieniona, nowe ustawienia mozna zapisac jako konfiguracje domyslna, aby byly uzywane we wszystkich przyszlych skanach calego komputera.*

11.2.2. Skan okreslonych plików lub folderów

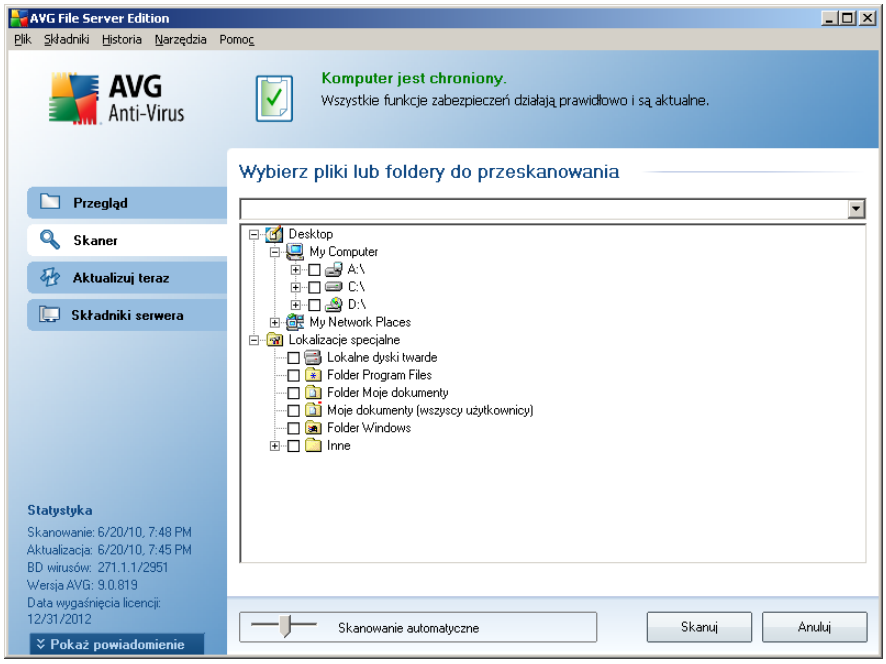
Skan okreslonych plików lub folderów - skanowane sa tylko wskazane obszary komputera (wybrane foldery, a takze dyski twarde, pamieci flash, CD itd).). Postepowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu calego komputera: kazdy znaleziony wirus jest leczony lub przenoszony do ***Przechowalni***. Skanowanie okreslonych plików lub folderów moze posluzyc do utworzenia wlasnych testów i planowania ich zgodnie z konkretnymi potrzebami.

Uruchamianie skanowania

Skanowanie okreslonych plików lub folderów mozna uruchomic bezposrednio z poziomu interfejsu skanera, klikajac ikone testu. Wyswietlone zostanie nowe okno dialogowe ***Wybierz pliki lub foldery do przeskanowania***. W drzewie katalogów nalezy wybrac te, które maja zostac przeskanowane. Sciezki do wszystkich wybranych folderów zostana wygenerowane automatycznie i wyswietlone w polu tekstowym w górnej czesci okna dialogowego.

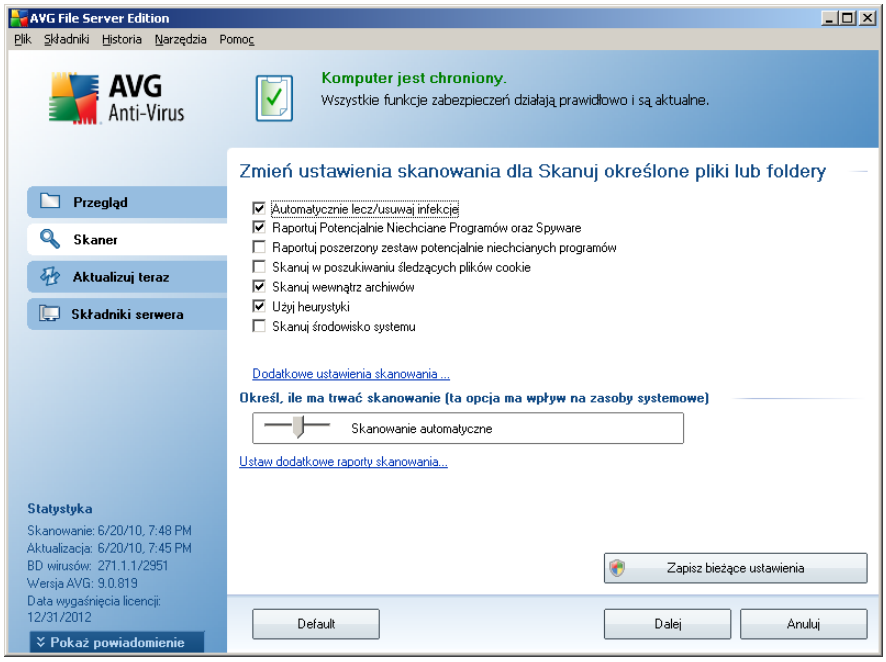
Mozna takze przeskanowac wybrany folder, wykluczajac jednoczesnie ze skanowania wszystkie jego podfoldery; w tym celu nalezy dodac znak minus "**-**" przed jego nazwa w automatycznie wygenerowanej sciezce. Aby wykluczyc caly folder ze skanowania, nalezy uzyc parametru „!”.

Na koniec, aby uruchomic skanowanie, nalezy nacisnac przycisk ***Rozpocznij skanowanie***; proces skanowania jest w zasadzie taki sam jak skanowanie calego komputera.



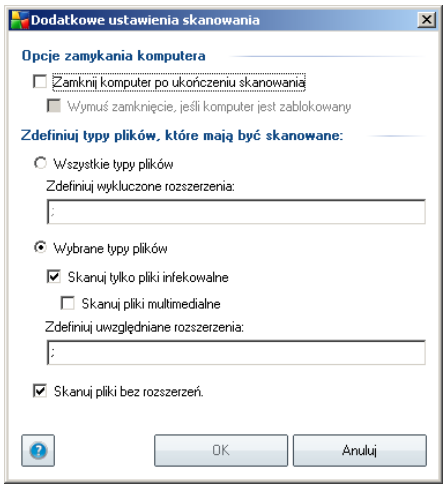
Edycja konfiguracji skanowania

Wstepne, domyslne ustawienia testu ***Skan okreslonych plików lub folderów*** mozna latwo edytowac. Kliknięcie linku ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***zmiany ustawien dla skanowania okreslonych plików lub folderów***. ***Zaleca sie nie zmieniac ustawien domyslnych, jesli nie jest to konieczne!***



- ***Parametry skanowania*** - na liscie parametrów skanowania mozna wlaczac/wylaczac okreslone parametry w zaleznosci od potrzeb *(szczególowy opis tych ustawien zawiera rozdzial Zaawansowane ustawienia AVG / Skany / Skanowanie okreslonych plików lub folderów)*.

- ***Dodatkowe ustawienia skanowania*** - link do okna dialogowo Dodatkowe ustawienia skanowania, w którym mozna okreslic nastepujace parametry:



- ***Opcje wylaczania komputera*** - okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie pierwszej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet wtedy, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** - nastepnie nalezy zdecydowac, czy skanowane maja byc:

  - ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

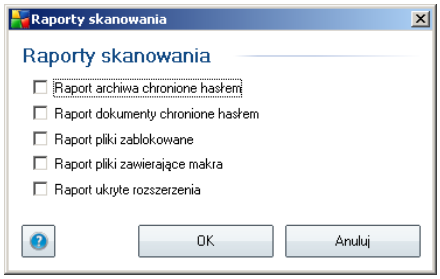
  - ***Wybrane typy plików*** - skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio - jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

  - Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** - ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- ***Priorytet procesu skanowania*** - za pomoca suwaka mozna zmienic priorytet

procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Ustaw dodatkowe raporty skanowania*** - link ten pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic elementy lub zdarzenia, które maja byc zglaszane:



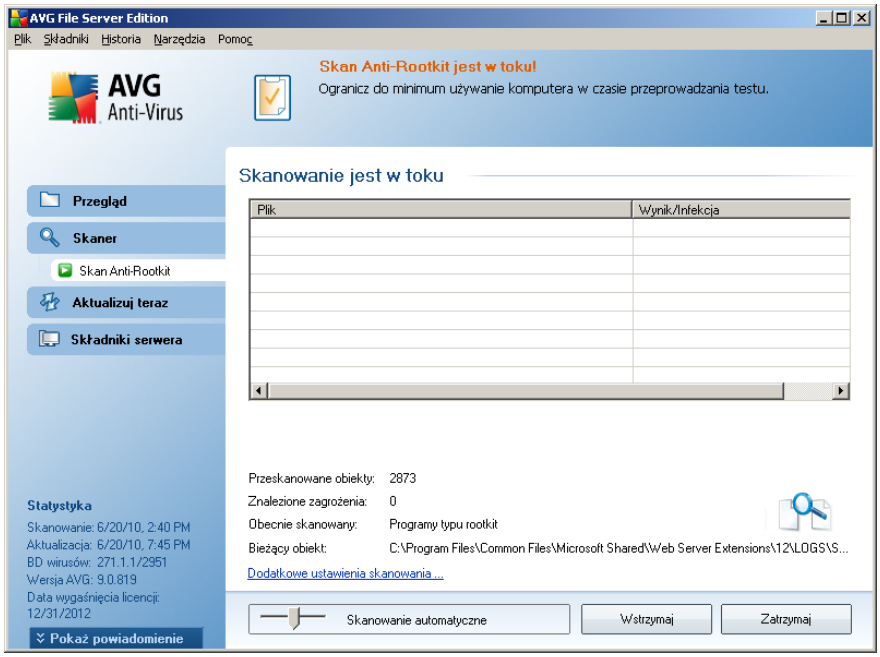
Ostrzezenie: *Ustawienia te sa identyczne jak domyslne parametry nowo utworzonych testów - zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanowac****. Jesli jednak domyslna konfiguracja testu* ***Skan okreslonych plików lub folderów*** *zostanie zmieniona, nowe ustawienia bedzie mozna zapisac jako konfiguracje domyslna, która bedzie uzywana we wszystkich zdefiniowanych w przyszlosci Skanach okreslonych plików lub folderów. Stanie sie ona równiez szablonem dla wszystkich nowych skanów zaplanowanych (wszystkie testy uzytkownika oparte sa na biezacej konfiguracji Skanu okreslonych plików lub folderów).*

11.2.3. Skan Anti-Rootkit

Skan Anti-Rootkit przeszukuje komputer w poszukiwaniu obecnych na nim programów typu rootkit (*aplikacji oraz technologii, które moga maskowac dzialanie szkodliwego oprogramowania na tym komputerze*). Wykrycie programu typu rootkit nie jest równoznaczne z tym, ze komputer jest zainfekowany. W niektórych przypadkach pewne sterowniki lub elementy zwyklych aplikacji moga omylkowo zostac zaklasyfikowane jako programy typu rootkit.

Uruchamianie skanowania

Skan Anti-Rootkit moze zostac uruchomiony bezposrednio z poziomu interfejsu skanera poprzez klikniecie ikony skanowania. Dla tego skanowania nie mozna okreslac dalszych ustawien; jest ono uruchamiane od razu w oknie dialogowym ***Skanowanie w toku***. (*patrz ilustracja*). W razie potrzeby skanowanie mozna tymczasowo przerwac (***Wstrzymaj***) lub anulowac (***Zatrzymaj***).

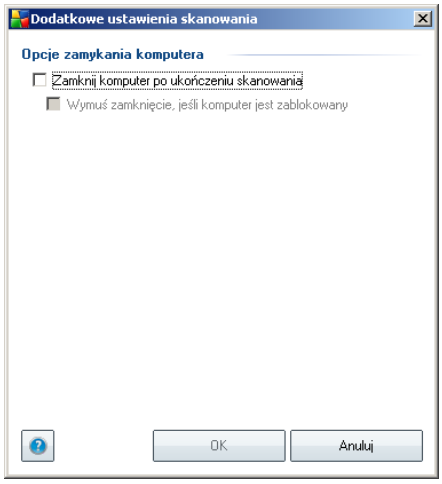


Edycja konfiguracji skanowania

Skan Anti-Rootkit jest zawsze uruchamiany z ustawieniami domyslnymi, a edycja parametrów skanowania jest dostepna tylko w oknie dialogowym ***Zaawansowane ustawienia systemu AVG / skladnik Anti-Rootkit***. Z poziomu interfejsu skanera dostepne sa tylko nastepujace opcje konfiguracji:

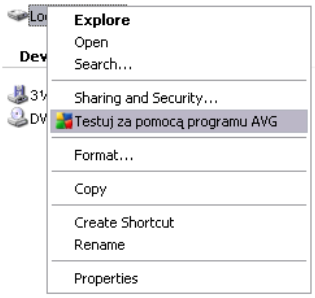
- ***Skanowanie automatyczne*** - za pomoca suwaka mozna zmienic priorytet procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Dodatkowe ustawienia skanowania*** - link ten umozliwia otwarcie nowego okna dialogowego ***dodatkowych ustawien skanowania***, w którym dostepne sa opcje ***Zamknij komputer po zakonczeniu skanowania*** *oraz* ***Wymus zamkniecie, jesli komputer jest zablokowany***:



11.3. Skan z poziomu eksploratora systemu Windows

Oprócz wstepnie zdefiniowanych skanów obejmujacych caly komputer lub wybrane obszary, system **AVG 9.0 File Server** oferuje takze mozliwosc skanowania okreslonych obiektów bezposrednio z interfejsu Eksploratora Windows. Jesli nie ma pewnosci co do zawartosci pliku, który ma zostac otwarty, mozna przeskanowac go „na zadanie”. W tym celu nalezy wykonac nastepujace kroki:



- W Eksploratorze Windows zaznacz plik (lub folder), który chcesz sprawdzic.
- Kliknij go prawym przyciskiem myszy, aby wyswietlic menu kontekstowe.
- Wybierz polecenie ***Testuj za pomoca programu AVG***, aby system AVG

przeskanowal obiekt.

11.4. Skan z poziomu wiersza polecen

System **AVG 9.0 File Server** posiada opcje uruchamiania skanowania z poziomu wiersza polecen. Opcji tej mozna uzywac na przyklad na serwerach lub w czasie tworzenia skryptu wsadowego, który ma byc uruchamiany po restarcie komputera. Uruchamiajac skanowanie z wiersza polecen, mozna uzywac wiekszosci parametrów dostepnych w graficznym interfejsie uzytkownika AVG.

Aby uruchomic skanowanie z poziomu wiersza polecen, nalezy uzyc nastepujacego polecenia w folderze, w którym zainstalowano system AVG:

- ***avgscanx*** - w przypadku 32-bitowych systemów operacyjnych
- ***avgscana*** - w przypadku 64-bitowych systemów operacyjnych

Skladnia polecenia

Skladnia polecenia jest nastepujaca:

- ***avgscanx /parametr*** ... np. ***avgscanx /comp*** w celu przeskanowania calego komputera
- ***avgscanx /parametr /parametr*** .. - jesli uzywanych jest wiele parametrów, nalezy wpisac je w jednym wierszu, rozdzielajac spacjami i ukosnikami
- jesli parametry wymagaja podania okreslonej wartosci, (np. parametr ***/scan*** wymaga informacji o wybranych do przeskanowania obszarach komputera - nalezy mu wskazac dokladna sciezke), wartosci nalezy rozdzielac przecinkami, na przyklad: ***avgscanx /scan=C:\,D:***

Parametry skanowania

Aby wyswietlic pelny przeglad dostepnych parametrów, nalezy wpisac odpowiednie polecenie oraz parametr /? lub /HELP (np. ***avgscanx /?***). Jedynym wymaganym parametrem jest /SCAN, który pozwala okreslic, jakie obszary komputera maja byc skanowane. Bardziej szczególowe informacje na temat opcji zawiera przeglad parametrów wiersza polecen.

Aby uruchomic skanowanie, nalezy nacisnac klawisz ***Enter***. Skanowanie mozna zatrzymac, naciskajac kombinacje klawiszy ***Ctrl+C*** lub ***Ctrl+Pause***.

Skanowanie z poziomu wiersza polecen uruchamiane za pomoca interfejsu graficznego

Gdy komputer dziala w trybie awaryjnym, skanowanie z poziomu wiersza polecen mozna równiez uruchomic za pomoca interfejsu graficznego uzytkownika. Skanowanie zostanie uruchomione z wiersza polecen, a okno dialogowe ***Kompozytor wiersza polecen*** umozliwi jedynie okreslenie wiekszosci parametrów skanowania w wygodnym interfejsie graficznym.

Poniewaz okno to jest dostepne tylko w trybie awaryjnym, jego szczególowy opis mozna znalezc w pliku pomocy dostepnym bezposrednio z tego okna.

11.4.1. Parametry skanowania z wiersza polecen

Ponizej przedstawiono liste wszystkich parametrów dostepnych dla skanowania z wiersza polecen:

- ***/SCAN*** Skanuj okreslone pliki lub foldery /SCAN=sciezka;sciezka (np. /SCAN=C:\;D:\)
- ***/COMP*** Skanuj caly komputer
- ***/HEUR*** Uzyj analizy heurystycznej***
- ***/EXCLUDE*** Wyklucz ze skanowania sciezke lub pliki
- ***/@*** Plik polecenia /nazwa pliku/
- ***/EXT*** Skanuj te rozszerzenia /na przyklad EXT=EXE,DLL/
- ***/NOEXT*** Nie skanuj tych rozszerzen /na przyklad NOEXT=JPG/
- ***/ARC*** Skanuj archiwa
- ***/CLEAN*** Lecz automatycznie
- ***/TRASH*** Przenies zainfekowane pliki do Przechowalni wirusów***
- ***/QT*** Szybki test
- ***/MACROW*** Raportuj pliki zawierajace makra
- ***/PWDW*** Raportuj pliki chronione haslem

- ***/IGNLOCKED*** Ignoruj pliki zablokowane
- ***/REPORT*** Raportuj do pliku /nazwa pliku/
- ***/REPAPPEND*** Dopisz do pliku raportu
- ***/REPOK*** Raportuj niezainfekowane pliki jako OK
- ***/NOBREAK*** Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- ***/BOOT*** Wlacz sprawdzanie MBR/sektora rozruchowego
- ***/PROC*** Skanuj aktywne procesy
- ***/PUP*** Raportuj potencjalnie niechciane programy
- ***/REG*** Skanuj rejestr
- ***/COO*** Skanuj pliki cookie
- ***/?*** Wyswietl pomoc na ten temat
- ***/HELP*** Wyswietl pomoc na ten temat
- ***/PRIORITY*** Ustaw priorytet skanowania /Niski, Automatyczny, Wysoki/ (zobacz Ustawienia zaawansowane/ Skany)
- ***/SHUTDOWN*** Zamknij komputer po ukonczeniu skanowania
- ***/FORCESHUTDOWN*** Wymus zamkniecie komputera po ukonczeniu skanowania
- ***/ADS*** Skanuj alternatywne strumienie danych (tylko NTFS)
- ***/ARCBOMBSW*** Raportuj wielokrotnie skompresowane archiwa

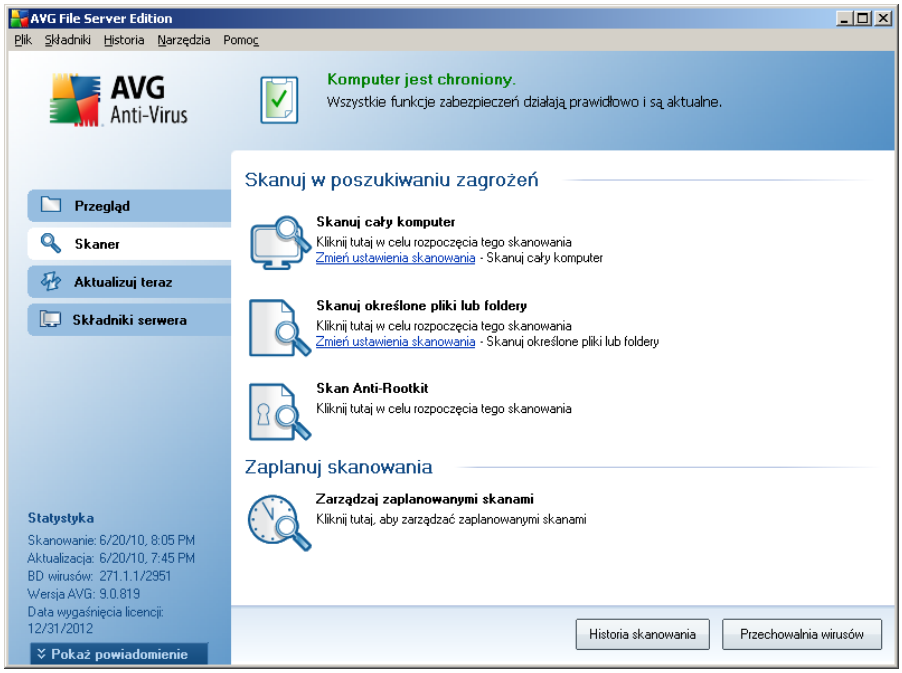
11.5. Planowanie skanowania

System **AVG 9.0 File Server** pozwala uruchamiac skanowanie na zadanie (na przyklad gdy podejrzewa sie infekcje komputera) lub zgodnie z zalozonym harmonogramem. Stanowczo zaleca sie korzystac z harmonogramu: ten sposób daje pewnosc, ze komputer jest chroniony przed infekcjami i zwalnia uzytkownika z obowiazku pamietania o regularnych testach.

Skan calego komputera nalezy uruchamiac regularnie co najmniej raz na tydzien. Jesli

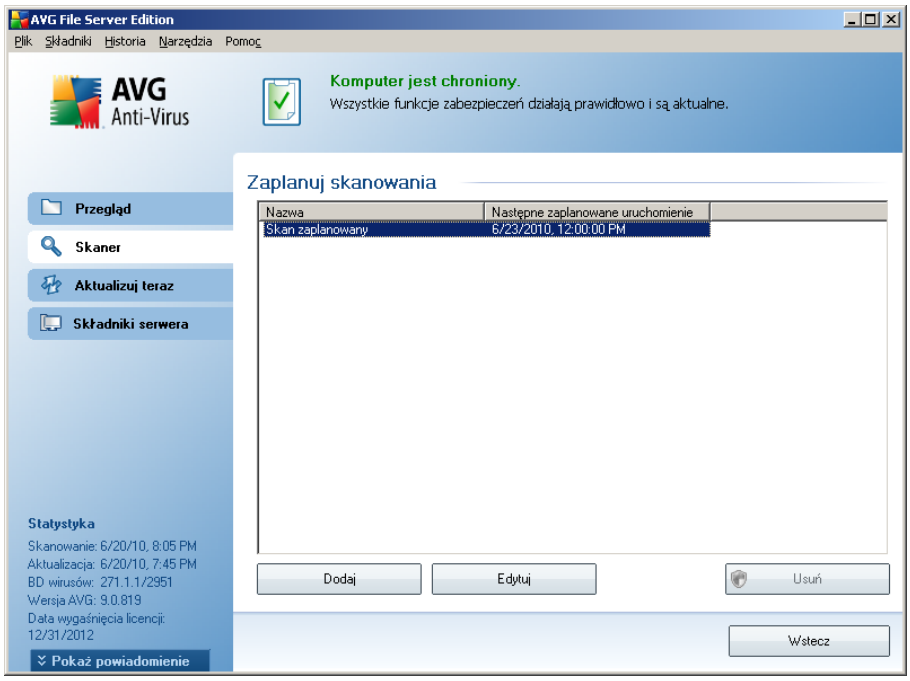
jest to mozliwe, nalezy skanowac komputer codziennie - zgodnie z domyslna konfiguracja harmonogramu skanowania. Jesli komputer dziala 24 godziny na dobe, mozna zaplanowac skanowanie poza czasem pracy. Jesli komputer jest czasami wylaczany, pominiete z tego powodu skany uruchamiane sa po ponownym wlaczeniu komputera.

Aby utworzyc nowe harmonogramy, skorzystaj z przycisku znajdujacego sie w dolnej czesci interfejsu skanera AVG, w sekcji ***Zaplanuj skanowania***:



Zaplanuj skanowania

Kliknij ikone w sekcji ***Planowanie skanowania***, aby otworzyc nowe okno dialogowe ***planowanie skanowania***, które zawiera liste wszystkich zaplanowanych testów:

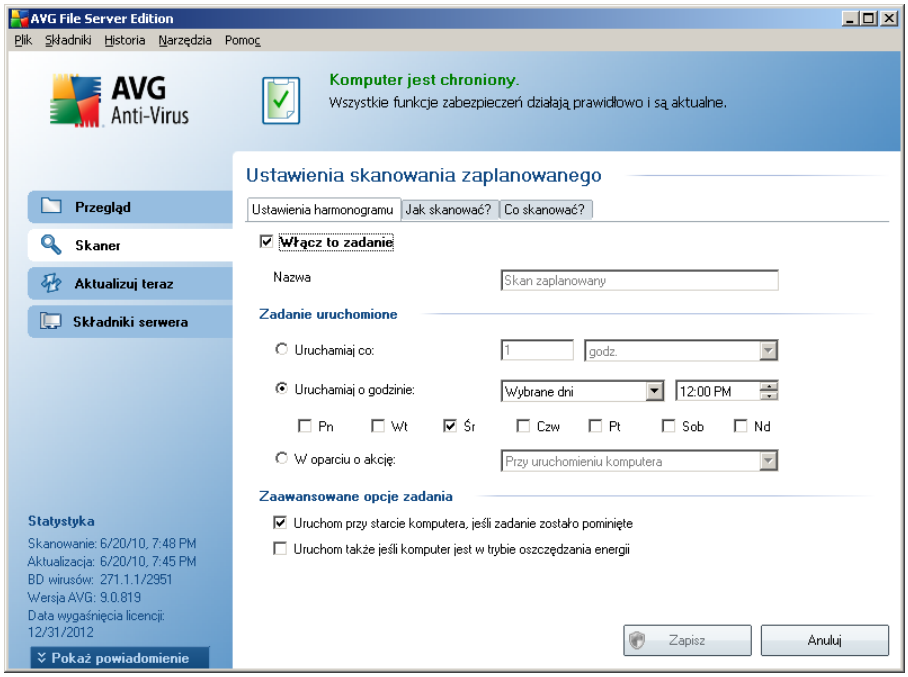


Zawartosc okna mozna edytowac, uzywajac nastepujacych przycisków:

- ***Dodaj*** - otwiera okno ***Ustawienia skanowania zaplanowanego***, a w nim karte ***Ustawienia harmonogramu***. W oknie tym mozna okreslic parametry definiowanego testu.
- ***Edytuj*** - jest aktywny tylko, jesli wybrano istniejacy test na liscie zaplanowanych testów. W takim przypadku klikniecie przycisku powoduje przejscie do okna dialogowego ***Ustawienia skanowania zaplanowanego***, na karte ***Ustawienia harmonogramu***. Parametry wybranego testu sa juz okreslone i mozna je edytowac.
- ***Usun*** - jest aktywny tylko, jesli wybrano istniejacy test na liscie zaplanowanych skanów. Klikniecie przycisku spowoduje usuniecie wybranej pozycji z listy. Usuwac mozna jedynie testy zdefiniowane przez uzytkownika; nie da sie usunac domyslnego ***Skanu zaplanowanego*** .
- ***Wstecz*** - pozwala wrócic do interfejsu skanera AVG

11.5.1. Ustawienia harmonogramu

Aby zaplanowac nowy test i uruchamiac go regularnie, nalezy przejsc do okna dialogowego ***Ustawienia zaplanowanego testu*** (*klikajac przycisk* ***Dodaj harmonogram skanowania*** *w oknie dialogowym* ***Planowanie skanowania***). Okno dialogowe jest podzielone na trzy karty: ***Ustawienia harmonogramu*** - *zobacz ilustracja ponizej (karta otwierana domyslnie),* ***Jak skanowac*** i ***Co skanowac***.



Na karcie ***Ustawienia harmonogramu*** mozna zaznaczyc/odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowany test lub wlaczyc go ponownie, gdy zajdzie taka potrzeba.

Nastepnie nalezy nazwac nowo tworzony skan. Nazwe mozna wpisac w polu tekstowym obok etykiety ***Nazwa.*** Nalezy uzywac krótkich, opisowych nazw, aby ulatwic rozpoznawanie ich przez innych uzytkowników w przyszlosci.

Przyklad: *Nazwy takie jak „Nowy skan" lub „Mój skan" nie sa odpowiednie, poniewaz nie informuja o tym, co jest przedmiotem skanowania. Przykladem dobrej, opisowej nazwy jest „Skan obszarów systemowych". Ponadto, nie ma potrzeby okreslac w nazwie skanowania, czy skanowany jest caly komputer, czy tylko jego wybrane obszary - wlasne testy uzytkownika sa zawsze specyficznym skanowaniem okreslonych plików lub folderów.*

W tym samym oknie mozna szczególowo okreslic nastepujace parametry skanowania:

- ***Zadanie uruchomione*** - nalezy okreslic interwal przeprowadzanych testów. Skanowanie moze byc powtarzane w okreslonych odstepach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia zdefiniowanego zdarzenia (***W oparciu o akcje, np. uruchomienie komputera***).

- ***Zaawansowane opcje zadania*** - ta sekcja umozliwia zdefiniowanie warunków skanowania w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

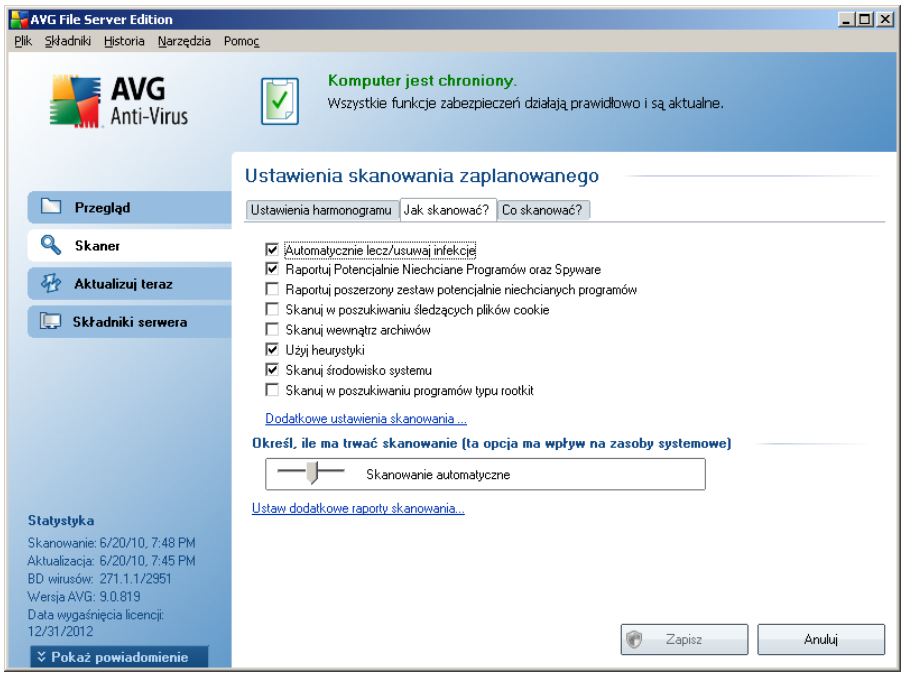
Przyciski kontrolne konfiguracji harmonogramu

Na wszystkich trzech kartach okna z ***konfiguracja skanu zaplanowanego*** (***Ustawienia harmonogramu***, ***Jak skanowac?*** i ***Co skanowac?***) dostepne sa dwa przyciski kontrolne. Ich dzialanie na kazdej karcie jest takie samo:

- ***Zapisz*** - powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyslnego okna Interfejsu uzytkownika AVG. Oznacza to, ze aby zapisac nowe parametry testów na wszystkich kartach, nalezy kliknac ten przycisk po zakonczeniu wprowadzania ustawien.

- ***Anuluj*** - powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do Interfejsu uzytkownika AVG.

11.5.2. Jak skanowac?



Karta ***Jak skanowac?*** zawiera liste parametrów testu, które mozna wlaczyc lub wylaczyc. Domyslnie wiekszosc funkcji jest wlaczona, a odpowiadajace im ustawienia sa stosowane podczas skanowania. Ustawienia te nalezy zmieniac tylko w uzasadnionych przypadkach, w pozostalych zachowujac wstepnie zdefiniowana konfiguracje:

- ***Automatycznie lecz/usuwaj infekcje*** - jezeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jesli zainfekowanego pliku nie mozna wyleczyc, lub jesli opcja ta zostanie wylaczona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcje. Zalecana czynnoscia jest przeniesienie zainfekowanego pliku do ***Przechowalni wirusów***.

- ***Raportuj potencjalnie niechciane programy i oprogramowanie szpiegujace*** - parametr ten kontroluje funkcje skladnika ***Anti-Virus***, które pozwalaja wykrywac potencjalnie niechciane programy (*pliki wykonywalne mogace dzialac jak oprogramowanie szpiegujace lub reklamowe*), a nastepnie blokowac je lub usuwac.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** - to pole nalezy zaznaczyc, aby mozliwe bylo wykrywanie wiekszej ilosci oprogramowania szpiegujacego, czyli programów, które sa zupelnie bezpieczne

w momencie nabywania ich od producenta, ale pózniej moga zostac wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze wiekszego bezpieczenstwa Twojego komputera. Funkcja ta moze jednak blokowac prawidlowo dzialajace programy, dlatego tez domyslnie jest wylaczona;

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** - ten parametr skladnika ***Anti-Spyware*** okresla, czy skanowanie ma wykrywac pliki cookie (*pliki cookie uzywane sa w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkownikach, np. ich preferencji dotyczacych wygladu witryny czy zawartosci koszyków w sklepach internetowych*);

- ***Skanuj wewnatrz archiwów*** - parametr ten okresla, czy skanowanie ma obejmowac pliki znajdujace sie wewnatrz niektórych typów archiwów, np. ZIP, RAR itd.

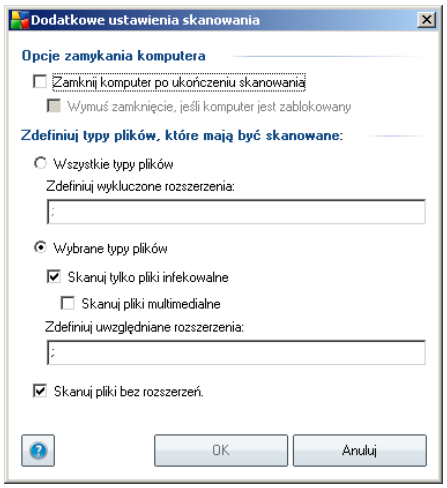
- ***Uzyj heurystyki*** - analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w srodowisku wirtualnej maszyny*) jest jedna z metod wykrywania wirusów w czasie rzeczywistym.

- ***Skanuj srodowisko systemu*** - skanowanie obejmie takze obszary systemowe komputera;

- ***Skanuj w poszukiwaniu programów typu rootkit*** - zaznaczenie tej pozycji pozwala dolaczyc wykrywanie programów typu rootkit do operacji skanowania calego komputera. Test Anti-Rootkit mozna takze uruchomic niezaleznie, dzieki interfejsowi skladnika ***Anti-Rootkit***

Nastepnie mozna zmienic konfiguracje skanowania zgodnie z ponizszym opisem:

- ***Dodatkowe ustawienia skanowania*** - link do okna dialogowo ***Dodatkowe ustawienia skanowania***, w którym mozna okreslic nastepujace parametry:



- ***Opcje wylaczania komputera*** - okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).

- ***Zdefiniuj typy plików do skanowania*** - nalezy zdecydowac, które z ponizszych elementów maja byc skanowane:

  - ***Wszystkie typy plików*** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;

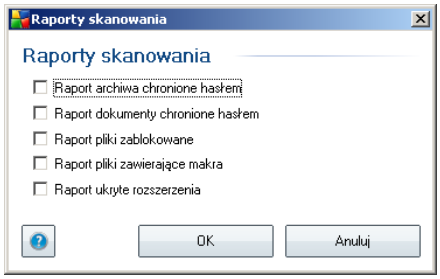
  - ***Wybrane typy plików*** - skanowane bede tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio - jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.

  - Opcjonalnie mozna zdecydowac o ***skanowaniu plików bez rozszerzenia*** - ta opcja jest domyslnie wlaczona i zaleca sie niezmienianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- ***Priorytet procesu skanowania*** - za pomoca suwaka mozna zmienic priorytet

procesu skanowania. Domyslnie ustawiony jest priorytet sredni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkosc skanowania, jak i wykorzystanie zasobów systemowych. Dostepne sa takze inne opcje: mozna wybrac skanowanie wolne, które minimalizuje obciazenie zasobów systemowych (*przydatne, gdy komputer jest uzywany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), badz skanowanie szybkie, które oznacza wyzsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo uzywany*).

- ***Ustaw dodatkowe raporty skanowania*** - link ten pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic elementy lub zdarzenia, które maja byc zglaszane:



Uwaga: *Domyslnie konfiguracja jest ustawiona pod katem optymalnej wydajnosci. Konfiguracje skanowania nalezy zmieniac tylko w uzasadnionych sytuacjach. Stanowczo zaleca sie stosowanie wstepnie zdefiniowanych ustawien. Wszelkie zmiany powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników. Wiecej opcji dostepne jest w oknie* ***Ustawienia zaawansowane****, (****Menu glówne/Plik/ Ustawienia zaawansowane****).*

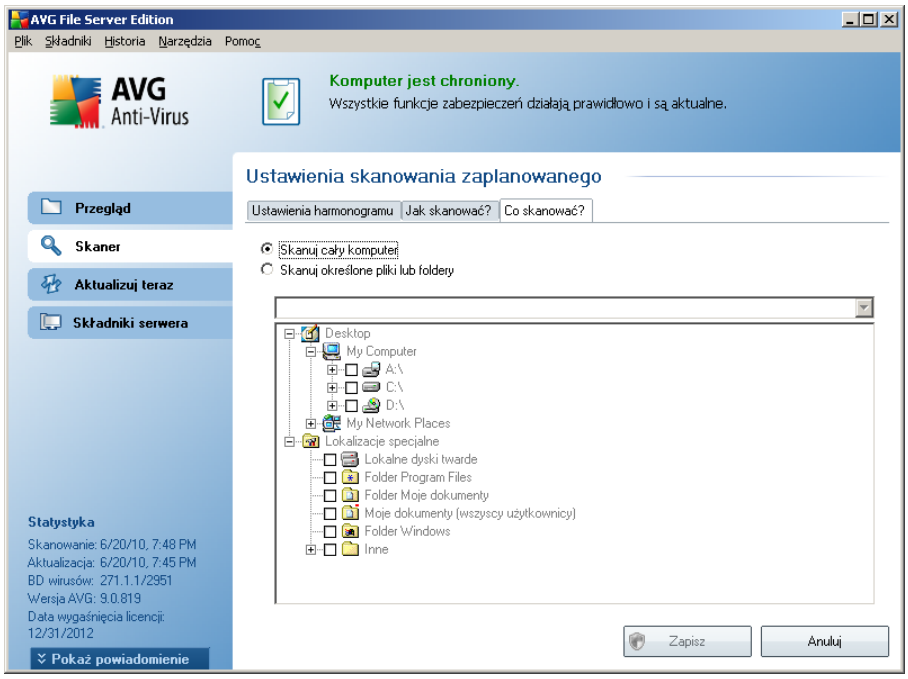
Przyciski kontrolne

Na wszystkich trzech kartach okna z ***konfiguracja skanu zaplanowanego*** (***Ustawienia harmonogramu***, ***Jak skanowac?*** i***Co skanowac?***) dostepne sa dwa przyciski kontrolne. Ich dzialanie na kazdej karcie jest takie samo:

- ***Zapisz*** - powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyslnego okna Interfejsu uzytkownika AVG. Oznacza to, ze aby zapisac nowe parametry testów na wszystkich kartach, nalezy kliknac ten przycisk po zakonczeniu wprowadzania ustawien.

- ***Anuluj*** - powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do Interfejsu uzytkownika AVG.

11.5.3. Co skanowac?



Na karcie ***Co skanowac?*** mozna okreslic, czy planowane jest skanowanie calego komputera, czy skanowanie okreslonych plików lub folderów. W przypadku skanowania okreslonych plików lub folderów, w dolnej czesci okna dialogowego aktywowane jest drzewo katalogów, w którym mozna wybrac obszar skanowania.

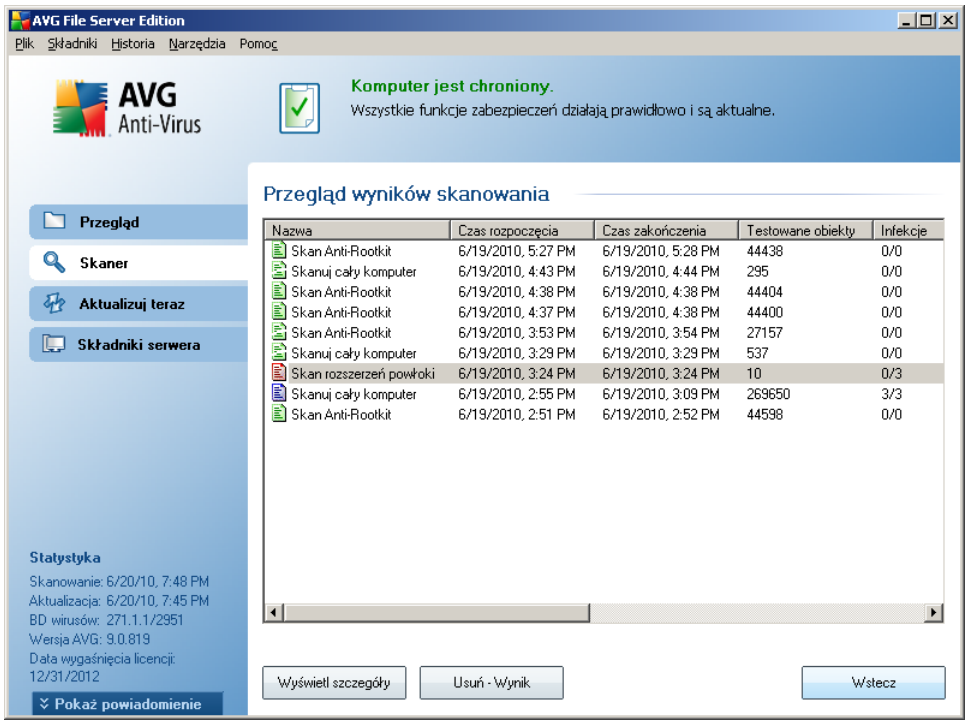
Przyciski kontrolne konfiguracji harmonogramu

Na wszystkich trzech kartach okna z ***konfiguracja skanu zaplanowanego*** (***Ustawienia harmonogramu***, ***Jak skanowac?*** i ***Co skanowac?***) dostepne sa dwa przyciski kontrolne. Ich dzialanie na kazdej karcie jest takie samo:

- ***Zapisz*** - powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do domyslnego okna Interfejsu uzytkownika AVG. Oznacza to, ze aby zapisac nowe parametry testów na wszystkich kartach, nalezy kliknac ten przycisk po zakonczeniu wprowadzania ustawien.

- ***Anuluj*** - powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do Interfejsu uzytkownika AVG.

11.6. Przeglad wyników skanowania



Dostep do okna ***Przeglad wyników skanowania*** mozliwy jest z poziomu Interfejsu skanera AVG, przez kliknięcie przycisku ***Historia skanowania***. Okno to zawiera liste wszystkich wczesniejszych testów oraz informacje o ich wynikach:

- ***Nazwa*** - oznaczenie skanowania; moze to byc nazwa jednego ze wstepnie zdefiniowanych skanów lub nazwa nadana przez uzytkownika jego skanowi zaplanowanemu. Kazdej nazwie towarzyszy ikona okreslajaca wynik skanowania:

  - zielona oznacza, ze nie wykryto zadnych infekcji;

  - niebieska ikona oznacza, ze wykryto infekcje, ale zainfekowany obiekt zostal automatycznie usuniety.

  - czerwona oznacza, ze wykryto infekcje i nie udalo sie jej usunac.

  Kazda z ikon moze byc widoczna w calosci lub „przerwana” - jesli ikona jest cala, skanowanie zostalo prawidlowo ukonczone; w przeciwnym razie skanowanie zostalo anulowane lub przerwane.

Uwaga: *Szczególowe informacje na temat kazdego testu zawiera okno* ***Wyniki skanowania*** *dostepne po klknieciu przycisku* ***Wyswietl szczegóły*** *(w dolnej czesci okna).*

- ***Czas rozpoczecia*** - data i godzina uruchomienia testu.
- ***Czas zakonczenia*** - data i godzina zakonczenia skanowania.
- ***Przetestowano obiektów*** - liczba obiektów sprawdzonych podczas skanowania.
- ***Infekcje*** - liczba infekcji wirusowych, które zostaly wykryte/usuniete.
- ***Oprogramowanie szpiegujace*** - liczba programów szpiegujacych, które zostaly wykryte/usuniete.
- ***Informacji w dzienniku skanowania*** - informacje dotyczace przebiegu i wyniku skanowania (zwykle o jego zakonczeniu lub przerwaniu).

Przyciski kontrolne

Przyciski kontrolne dostepne w oknie ***Przeglad wyników skanowania*** to:

- ***Wyswietl szczegóły*** - przycisk jest aktywny tylko, jesli w sekcji znajdujacej sie powyzej wybrano którys z testów; klikniecie go otwiera okno ***Wyniki skanowania***, w którym mozna przejrzec szczególowe informacje o wybranym skanowaniu.
- ***Usun wynik*** - przycisk jest aktywny tylko, jesli w sekcji znajdujacej sie powyzej wybrano którys z testów; klikniecie go powoduje usuniecie wybranej pozycji z przegladu wyników skanowania.
- ***Wstecz*** - otwiera ponownie domyslne okno Interfejsu skanera AVG.

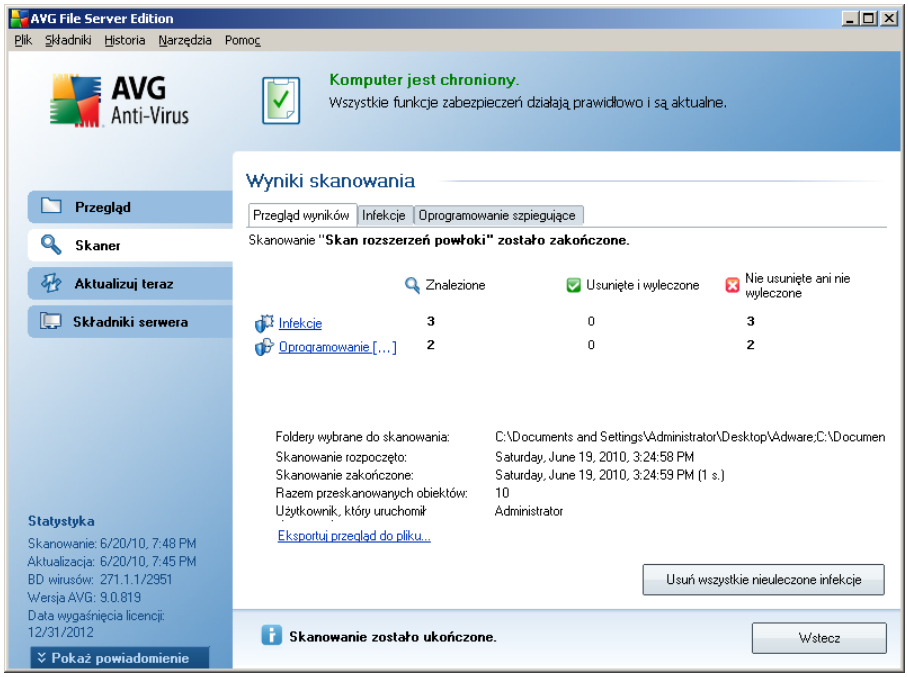
11.7. Szczegóły wyników skanowania

Po wybraniu w oknie ***Przeglad wyników skanowania*** któregos z testów, mozna kliknac przycisk ***Wyswietl szczegóły***, aby przejsc do okna ***Wyniki skanowania***, które zawiera dodatkowe informacje o jego przebiegu.

Okno to podzielone jest na kilka kart:

- ***Przeglad wyników*** - karta jest zawsze wyswietlana; zawiera statystyki dotyczace przebiegu skanowania.
- ***Infekcje*** - karta jest wyswietlana tylko, jesli w czasie skanowania wykryto co najmniej jedna infekcje wirusowa.
- ***Oprogramowanie szpiegujace*** - karta jest wyswietlana tylko, jesli w czasie skanowania wykryto oprogramowanie szpiegujace.
- ***Ostrzezenia*** - karta jest wyswietlana tylko, jesli w czasie skanowania wykryto obiekty, których nie mozna bylo przeskanowac.
- ***Programy typu rootkit*** - karta jest wyswietlana tylko, jesli w czasie skanowania wykryto programy typu rootkit.
- ***Informacje*** **-** karta jest wyswietlana tylko, jesli w czasie skanowania wykryto potencjalne zagrozenia, których nie mozna bylo zakwalifikowac do powyzszych kategorii; dla kazdego znalezionego obiektu wyswietlany jest komunikat ostrzegawczy

11.7.1. Karta Przeglad wyników



Na karcie ***Wyniki skanowania*** mozna znalezc szczególowe statystyki oraz informacje o:

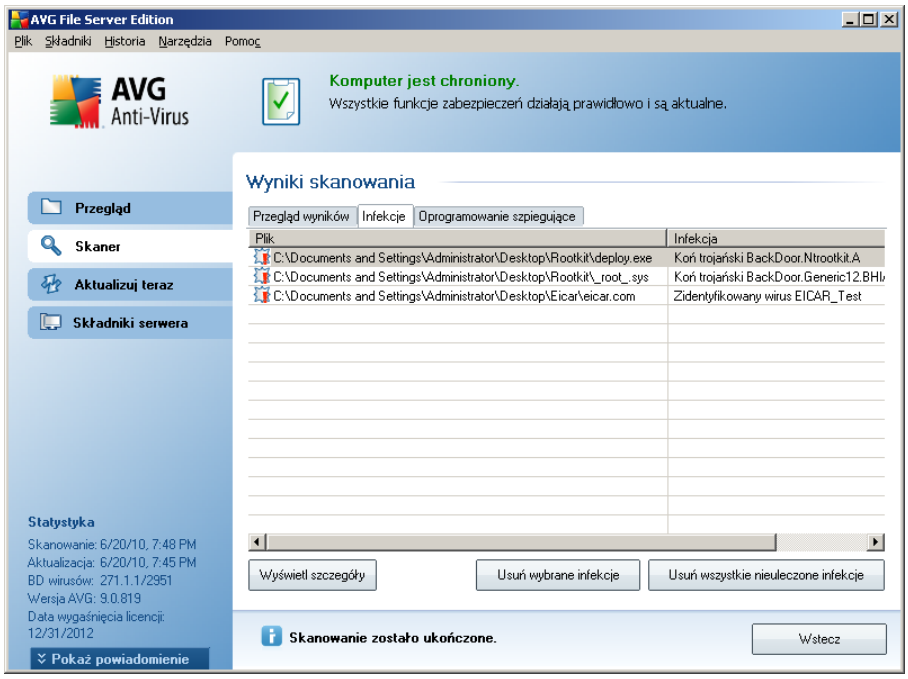
- wykrytych infekcjach wirusowych / programach szpiegujacych / ostrzezeniach / programach typu rootkit***
- usunietych infekcjach wirusowych / programach szpiegujacych / ostrzezeniach / programach typu rootkit
- liczbie infekcji wirusowych /programów szpiegujacych / ostrzezen / programów typu rootkit, których nie udalo sie usunac ani wyleczyc

Ponadto, znajduja sie tu informacje o dacie i godzinie uruchomienia skanowania, lacznej liczbie przeskanowanych obiektów, czasie trwania skanowania, liczbie napotkanych bledów, a nawet o uzytkowniku, który uruchomil skanowanie.

Przyciski kontrolne

W tym oknie dialogowym dostepne sa tylko dwa przyciski kontrolne. Kliknięcie przycisku ***Zamknij wyniki*** powoduje powrót do okna ***Przeglad wyników skanowania***. Przycisk ***Usun wszystkie niewyleczone pliki*** staje sie dostepny, gdy w procesie skanowania zostaly wykryte zagrozenia, których nie mozna bylo usunac automatycznie. Kliknięcie go powoduje przeniesienie takich zagrozen do ***Przechowalni wirusów***.

11.7.2. Karta Infekcje



Karta ***Infekcje*** jest wyswietlana w oknie dialogowym ***Wyniki skanowania*** tylko, jesli podczas skanowania wykryto wirusa. Karta jest podzielona na trzy obszary, które zawieraja nastepujace informacje:

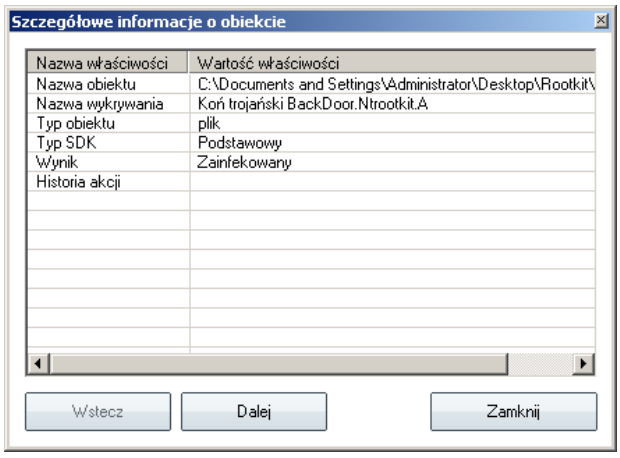
- ***Plik*** - pelna sciezka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** - nazwa wykrytego wirusa (*szczególowe informacje na temat wirusów zawiera Encyklopedia Wirusów dostepna online*).
- ***Wynik*** - okresla biezacy stan zainfekowanego obiektu, który wykryto podczas skanowania:
  - ***Zainfekowany*** - zainfekowany obiekt zostal wykryty i pozostawiony w oryginalnej lokalizacji (*np. jesli wylaczono opcje automatycznego leczenia w szczególowych ustawieniach skanowania).*
  - ***Wyleczony*** - zainfekowany obiekt zostal automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
  - ***Przeniesiony do Przechowalni*** - zainfekowany obiekt zostal przeniesiony do ***Przechowalni wirusów***.

- **Usuniety** - zainfekowany obiekt zostal usuniety.
- **Dodany do listy wyjatków PNP** - znaleziony obiekt zostal uznany za wyjatek i dodany do listy wyjatków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie* ***Wyjatki PNP***).
- **Plik zablokowany - nie testowany** - obiekt jest zablokowany i program AVG nie mógl go przeskanowac.
- **Obiekt potencjalnie niebezpieczny** - obiekt zostal uznany za potencjalnie niebezpieczny, ale nie zainfekowany (*moze na przyklad zawierac makra*); informacje te nalezy traktowac wylacznie jako ostrzezenie.
- **Wymagany restart systemu** - aby calkowicie usunac zainfekowany obiekt, nalezy ponownie uruchomic komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

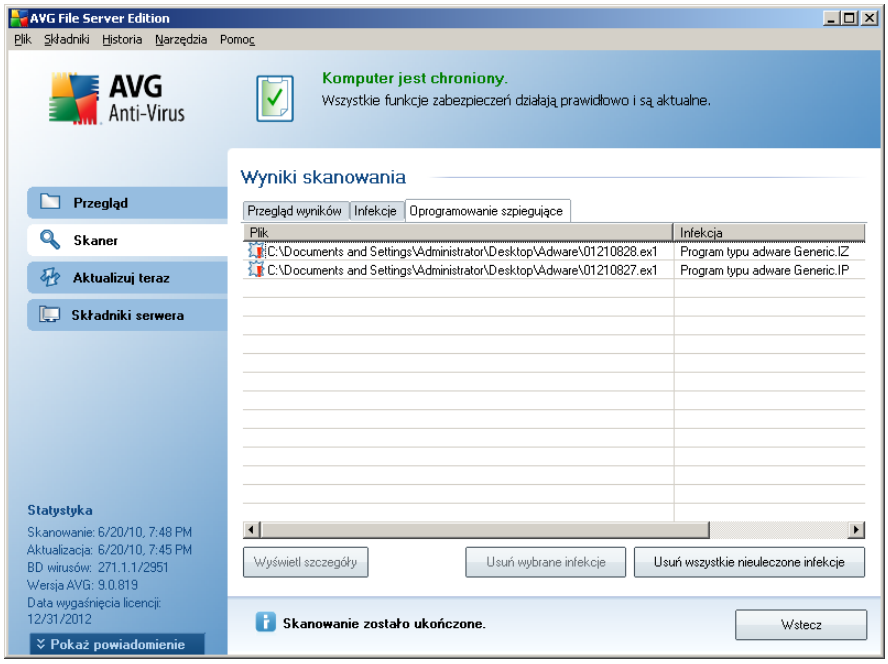
- ***Wyswietl szczegóły***- otwiera nowe okno dialogowe ze ***szczególowymi informacjami o obiekcie***:



Mozna w nim znalezc informacje o lokalizacji wykrytego pliku (***Nazwa wlasciwosci***). Za pomoca przycisków ***Wstecz*** / ***Dalej*** mozna wyswietlac informacje o wybranych znalezionych obiektach. Przycisk ***Zamknij*** zamyka okno.

- ***Usun wybrane infekcje*** - ten przycisk sluzy do leczenia wybranych zagrozen lub przenoszenia ich do ***Przechowalni wirusów*** (jesli nie mozna ich wyleczyc).
- ***Usun wszystkie niewyleczone pliki*** - ten przycisk pozwala wyleczyc wszystkie zagrozenia na liscie lub przeniesc je do ***Przechowalni wirusów*** (jesli nie mozna ich wyleczyc).
- ***Zamknij wyniki*** - powoduje zamkniecie szczegółowych wyników i powrót do okna ***Przeglad wyników skanowania***.

11.7.3. Karta Oprogramowanie szpiegujace



Karta ***Oprogramowanie szpiegujace*** jest wyswietlana w oknie dialogowym ***Wyniki skanowania*** tylko, jesli podczas skanowania wykryto oprogramowanie szpiegujace. Karta jest podzielona na trzy obszary, które zawieraja nastepujace informacje:

- ***Plik*** - pelna sciezka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** - nazwa wykrytego oprogramowania szpiegujacego (*szczególowe informacje na temat wirusów zawiera* ***Encyklopedia Wirusów*** *dostepna online*).
- ***Wynik*** - okresla biezacy stan obiektu, który wykryto podczas skanowania:

- ***Zainfekowany*** - zainfekowany obiekt zostal wykryty i pozostawiony w oryginalnej lokalizacji (np. jesli wylaczono opcje automatycznego leczenia w szczególowych ustawieniach skanowania).

- ***Wyleczony*** - zainfekowany obiekt zostal automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.

- ***Przeniesiony do Przechowalni*** - zainfekowany obiekt zostal przeniesiony do ***Przechowalni wirusów***.

- ***Usuniety*** - zainfekowany obiekt zostal usuniety.

- ***Dodany do listy wyjatków PNP*** - znaleziony obiekt zostal uznany za wyjatek i dodany do listy wyjatków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie **Wyjatki PNP***).

- ***Plik zablokowany - nie testowany*** - obiekt jest zablokowany i program AVG nie mógl go przeskanowac.

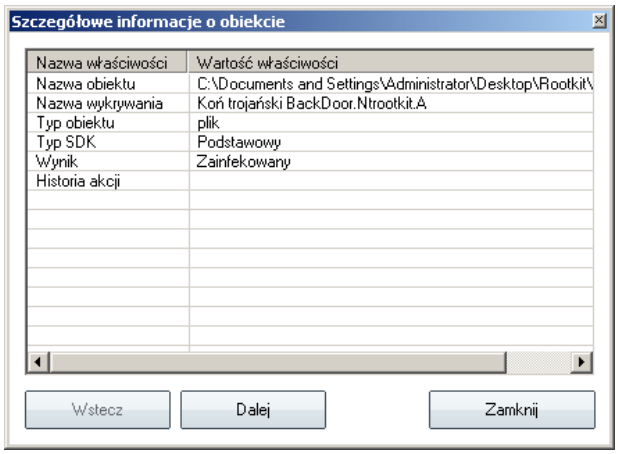
- ***Obiekt potencjalnie niebezpieczny*** - obiekt zostal uznany za potencjalnie niebezpieczny, ale nie zainfekowany (moze np. zawierac makra); informacja ta jest wylacznie ostrzezeniem.

- ***Wymagany restart systemu*** - aby calkowicie usunac zainfekowany obiekt, nalezy ponownie uruchomic komputer.

Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

- ***Wyswietl szczegóły*** - otwiera nowe okno ze ***szczególowymi informacjami o wyniku testu***:



Mozna w nim znalezc informacje o lokalizacji wykrytego pliku (***Nazwa wlasciwosci***). Za pomoca przycisków ***Wstecz*** / ***Dalej*** mozna wyswietlac informacje o wybranych znalezionych obiektach. Przycisk ***Zamknij*** zamyka okno.

- ***Usun wybrane infekcje*** - ten przycisk sluzy do leczenia wybranych zagrozen lub przenoszenia ich do ***Przechowalni wirusów*** (jesli nie mozna ich wyleczyc).
- ***Usun wszystkie niewyleczone pliki*** - ten przycisk pozwala wyleczyc wszystkie zagrozenia na liscie lub przeniesc je do ***Przechowalni wirusów*** (jesli nie mozna ich wyleczyc).
- ***Zamknij wyniki*** - powoduje zamkniecie szczególowych wyników i powrót do okna ***Przeglad wyników skanowania***.

11.7.4. Karta Ostrzezenia

Karta ***Ostrzezenia*** zawiera informacje o „podejrzanych" obiektach (*zwykle plikach*) wykrytych podczas skanowania. Gdy ***Ochrona Rezydentna*** wykryje takie pliki, zazwyczaj blokuje do nich dostep. Typowe przyklady obiektów tego typu to: ukryte pliki, cookies, podejrzane klucze rejestru, zabezpieczone haslem archiwa i dokumenty itp.Pliki te nie stanowia zadnego bezposredniego zagrozenia dla bezpieczenstwa komputera i uzytkownika. Informacje o nich przydatne sa jednak w wypadku wykrycia na komputerze oprogramowania reklamowego lub szpiegujacego. Jesli podczas testu AVG pojawily sie tylko ostrzezenia, nie jest konieczne podejmowanie jakichkolwiek dzialan.

Oto krótki opis najbardziej popularnych obiektów tego typu:

- ***Pliki ukryte*** Pliki ukryte sa domyslnie niewidoczne dla uzytkownika w systemie

Windows. Niektóre wirusy moga próbowac uniknac wykrycia przez wykorzystanie tej wlasciwosci. Jesli system AVG zglasza obecnosc ukrytego pliku, który moze byc szkodliwy, mozna przeniesc go do ***Przechowalni wirusów AVG***.

- ***Pliki cookie*** Pliki cookie to pliki tekstowe wykorzystywane przez strony internetowe do przechowywania informacji wlasciwych dla danego uzytkownika. Sa one pózniej uzywane do ladowania witryn internetowych dostosowanych do wymagan uzytkownika, itp.

- ***Podejrzane klucze rejestru*** Niektóre szkodliwe oprogramowanie przechowuje informacje w rejestrze systemu Windows, aby uruchamiac sie podczas ladowania systemu lub rozszerzyc zakres swojego dzialania.

11.7.5. Karta Rootkity

Karta ***Programy typu rootkit*** zawiera informacje o programach typu rootkit wykrytych podczas skanowania (jesli zostal uruchomiony ***skan Anti-Rootkit***).

Program typu rootkit to wirus zaprojektowany w celu przejecia calkowitej kontroli nad systemem komputerowym bez zgody jego wlascicieli czy upowaznionych administratorów. Bezposredni dostep do sprzetu jest rzadko wymagany, poniewaz programy typu rootkit w pelni zdalnie kontroluja system operacyjny komputera. Zwykle ukrywaja one swoja obecnosc mylac lub unikajac standardowych mechanizmów bezpieczenstwa systemu operacyjnego. Wiele z nich jest jednoczesnie konmi trojanskimi, które dodatkowo staraja sie przekonac uzytkowników, ze ich systemy sa bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorujacymi) oraz plików lub danych przed samym systemem operacyjnym.

Struktura tej karty jest w zasadzie taka sama jak kart ***Infekcje*** i ***Oprogramowanie szpiegujace***.

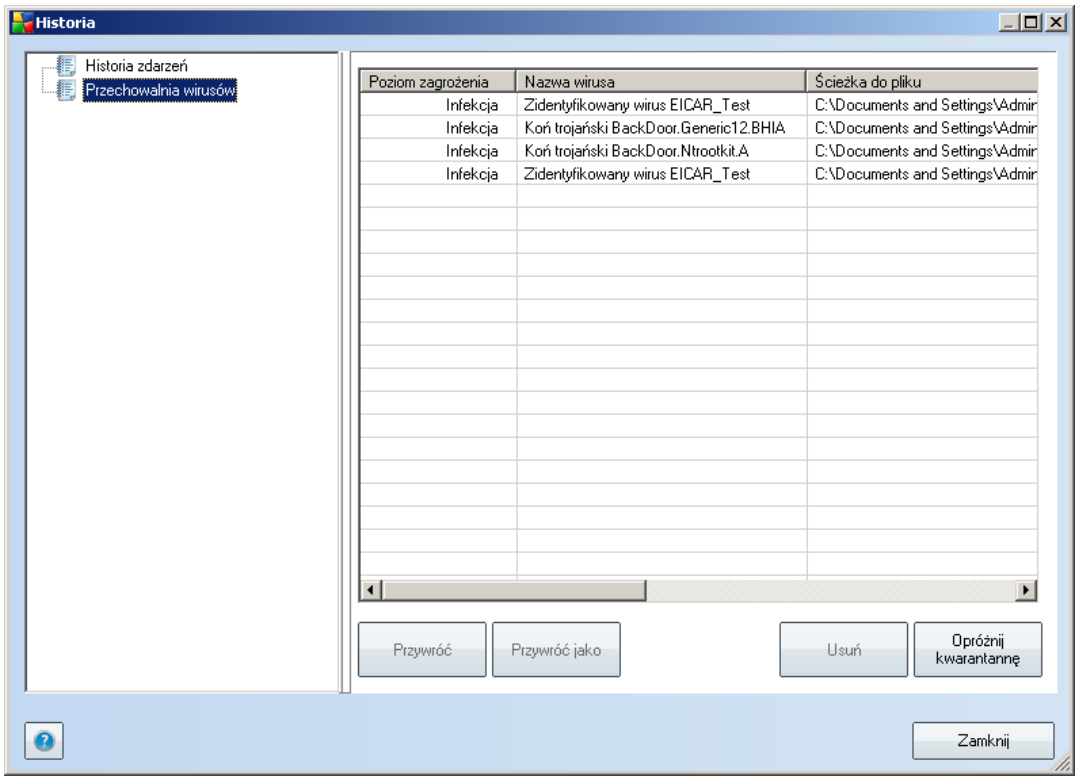
11.7.6. Karta Informacje

Karta ***Informacje*** zawiera dane dotyczace znalezionych obiektów, których nie mozna zakwalifikowac jako infekcje, oprogramowanie szpiegujace itp. Obiektów tych nie mozna w stu procentach uznac za niebezpieczne, ale czesto wymagaja one uwagi uzytkownika. Skaner AVG jest w stanie wykryc pliki, które moga nie byc zainfekowane, ale sa podejrzane. Zglaszane beda one jako ***lub*** Informacja.

Informacje o zagrozeniu moga byc zglaszane z jednego z nastepujacych powodów:

- ***Plik kompresowany w czasie rzeczywistym*** - Plik zostal skompresowany przy uzyciu jednego z mniej popularnych programów kompresujacych w czasie wykonania, co moze wskazywac na próbe uniemozliwienia skanowania takiego pliku. Nie kazde zgloszenie takiego pliku oznacza obecnosc wirusa.
- ***Plik rekurencyjnie kompresowany w czasie rzeczywistym*** - Podobny do powyzszego, ale rzadziej spotykany wsród zwyklego oprogramowania. Takie pliki sa podejrzane i nalezy rozwazyc ich usuniecie lub przeslanie do analizy.
- ***Archiwum lub dokument chroniony haslem*** - Pliki chronione haslem nie moga byc skanowane przez program AVG (*ani generalnie przez zaden inny program chroniacy przed szkodliwym oprogramowaniem*).
- ***Dokument zawierajacy makra*** - zgloszone dokumenty zawieraja makra, które moga byc szkodliwe.
- ***Ukryte rozszerzenie*** - pliki z ukrytymi rozszerzeniami moga udawac np. obrazy, podczas gdy w rzeczywistosci sa plikami wykonywalnymi (*np. "obrazek. jpg.exe"*). Drugie rozszerzenie jest w systemie Windows domyslnie niewidoczne. Program AVG zglasza takie pliki, aby zapobiec ich przypadkowemu uruchomieniu.
- ***Niewlasciwa sciezka do pliku*** - jezeli jakis wazny plik systemowy jest uruchamiany z innej sciezki niz domyslna (*np. plik "winlogon.exe" jest uruchamiany z folderu innego niz Windows*), system AVG zglasza te niezgodnosc. W niektórych przypadkach wirusy uzywaja nazw standardowych procesów systemowych, aby ich obecnosc w systemie byla trudniejsza do wychwycenia przez uzytkownika.
- ***Plik zablokowany*** - raportowany plik jest zablokowany, dlatego nie moze zostac przeskanowany przez system AVG. Oznacza to zazwyczaj, ze dany plik jest stale uzywany przez system (*np. plik wymiany*).

11.8. Przechowalnia wirusów



Przechowalnia wirusów to bezpieczne srodowisko przeznaczone do zarzadzania podejrzanymi/zainfekowanymi obiektami, które zostaly wykryte podczas testów przeprowadzonych przez AVG. Po wykryciu zainfekowanego obiektu podczas skanowania (w przypadku, gdy AVG nie jest w stanie automatycznie go wyleczyc), uzytkownik zostanie poproszony o dokonanie wyboru reakcji na to zagrozenie. Zalecanym rozwiazaniem jest przeniesienie obiektu do ***Przechowalni wirusów***, skad mozna bedzie podjac dalsze dzialanie zwiazane z analiza, wyleczeniem lub usunieciem pliku.

Interfejs ***Przechowalni wirusów*** jest otwierany w nowym oknie i zawiera przeglad informacji o izolowanych, zainfekowanych obiektach:

- ***Poziom zagrozenia*** - wyswietla identyfikacje poziomu i typu zagrozenia odpowiedniej pozycji
- ***Typ infekcji*** - klasyfikuje obiekty wedlug typu infekcji (*wszystkie obiekty na liscie sa prawdopodobnie lub na pewno zainfekowane*).

- ***Nazwa wirusa*** - nazwa wykrytej infekcji pochodzaca z Encyklopedii wirusów (online).
- ***Sciezka do pliku*** - pelna sciezka do oryginalnej lokalizacji zainfekowanego pliku.
- ***Pierwotna nazwa obiektu*** - wszystkie wykryte obiekty na liscie zostaly oznaczone standardowymi nazwami okreslanymi przez AVG w trakcie skanowania. W przypadku gdy obiekt mial okreslona nazwe, która jest znana (*np. nazwa zalacznika wiadomosci e-mail, która nie odpowiada faktycznej zawartosci zalacznika*), jest ona podawana w tej kolumnie.
- ***Data zachowania*** - data i godzina wykrycia podejrzanego pliku i przeniesienia go do ***Przechowalni.***

Przyciski kontrolne

Interfejs ***Przechowalni wirusów*** zawiera nastepujace przyciski kontrolne:

- ***Przywróc*** - przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- ***Przywróc jako*** - jesli zainfekowany obiekt ma zostac przeniesiony poza ***Przechowalnie***, do okreslonego folderu, ten przycisk pozwala zapisac obiekt z nazwa inna niz pierwotna. Jesli nazwa pierwotna nie jest znana, uzyta zostanie nazwa standardowa.
- ***Usun*** - usuwa bezpowrotnie zainfekowany plik z ***Przechowalni wirusów***.
- ***Opróznij kwarantanne*** - usuwa bezpowrotnie cala zawartosc ***Przechowalni***

12. Aktualizacje AVG

Zapewnienie aktualnosci programu AVG jest niezbedne, poniewaz tylko w ten sposób wszystkie nowo pojawiajace sie wirusy beda wykrywane we wlasciwym czasie. Aktualizacje programu AVG nie sa publikowane zgodnie z jakimkolwiek harmonogramem - powstaja jako reakcja na pojawiajace sie zagrozenia. Dlatego tez zalecamy sprawdzanie dostepnosci aktualizacji przynajmniej raz dziennie. Sprawdzanie co 4 godziny gwarantuje, ze baza danych wirusów bedzie aktualna takze w ciagu dnia.

12.1. Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

- ***Aktualizacja definicji*** zawiera aktualizacje niezbedne do zapewnienia niezawodnej ochrony antywirusowej. Na ogól nie zawiera modyfikacji programu i aktualizuje tylko baze definicji. Ta aktualizacja powinna zostac zastosowana, gdy tylko bedzie dostepna.

- ***Aktualizacja programu*** zawiera rózne zmiany w programie glównym, oraz poprawki i udoskonalenia.

Podczas planowania aktualizacji mozna wybrac poziom priorytetu aktualizacji, które maja zostac pobrane i zastosowane.

12.2. Typy aktualizacji

Mozna wyróznic dwa typy aktualizacji:

- ***Aktualizacja na zadanie*** - natychmiastowa aktualizacja oprogramowania AVG, której mozna dokonac w dowolnym momencie, w razie wystapienia takiej koniecznosci.

- ***Aktualizacja zaplanowana*** - system AVG umozliwia przygotowanie harmonogramu aktualizacji. Aktualizacja zaplanowana jest wykonywana regularnie, zgodnie z ustawiona konfiguracja. Gdy dostepne sa nowe pliki aktualizacyjne, AVG pobiera je bezposrednio z internetu lub katalogu sieciowego. W przypadku braku nowych aktualizacji proces ten konczy sie, nie dokonujac zadnych zmian.

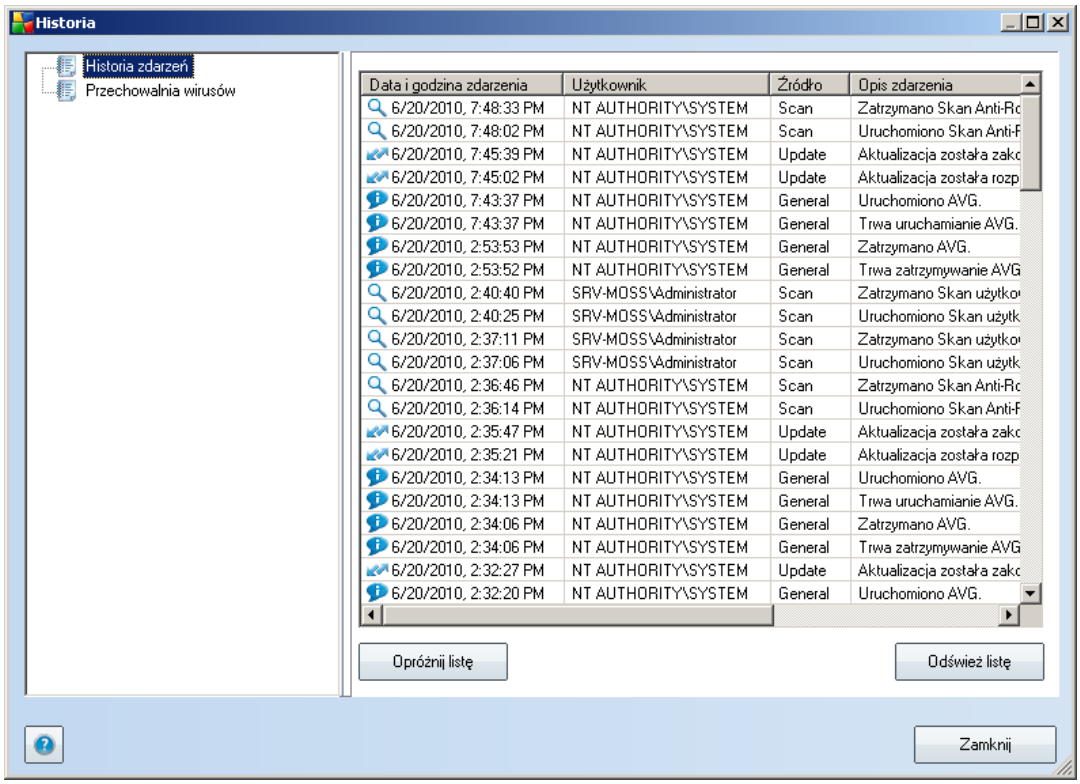
12.3. Proces aktualizacji

Proces aktualizacji mozna uruchomic natychmiast, gdy jest ona potrzebna, klikajac szybki link ***Aktualizuj teraz***. Link ten jest zawsze dostepny w glównym oknie interfejsu uzytkownika AVG. Mimo to, zaleca sie regularne aktualizowanie systemu, zgodnie z harmonogramem, który mozna edytowac za pomoca Menedzera aktualizacji.

Po uruchomieniu tego procesu program AVG sprawdza, czy dostepne sa nowe pliki aktualizacyjne. Jesli tak, system pobiera je i uruchamia wlasciwy proces aktualizacji. W tym czasie otwierany jest interfejs ***Aktualizacja***, w którym mozna sledzic przedstawiony graficznie postep aktualizacji oraz przegladac szereg parametrów (*rozmiar pliku aktualizacji, ilosc odebranych danych, szybkosc pobierania, czas pobierania itd., ...*).

Uwaga*: Przed zaktualizowaniem programu AVG tworzony jest punkt odtwarzania systemu. Przy jego uzyciu mozliwe bedzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Funkcja ta jest dostepna po kolejnym wybraniu opcji: Start / Wszystkie programy / Akcesoria / Narzedzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoswiadczonym uzytkownikom!*

13. Historia zdarzen



Do interfejsu ***Historii zdarzen*** mozna dostac sie poprzez menu główne ***Historia/ Dziennik historii zdarzen***. Okno to zawiera podsumowanie najwazniejszych wydarzen, które wystapily w czasie pracy systemu **AVG 9.0 File Server**. ***Dziennik historii zdarzen*** zawiera rekordy odpowiadajace nastepujacym typom zdarzen:

- Informacje o aktualizacjach oprogramowania AVG;
- Uruchomienie, zakonczenie lub wstrzymanie testu (lacznie z testami wykonywanymi automatycznie);
- Zdarzenia powiazane z wykryciem wirusa (przez Ochrone Rezydentna lub podczas zwyklego skanowania), wraz ze wskazaniem lokalizacji zainfekowanego pliku;
- Inne wazne zdarzenia.

Przyciski kontrolne

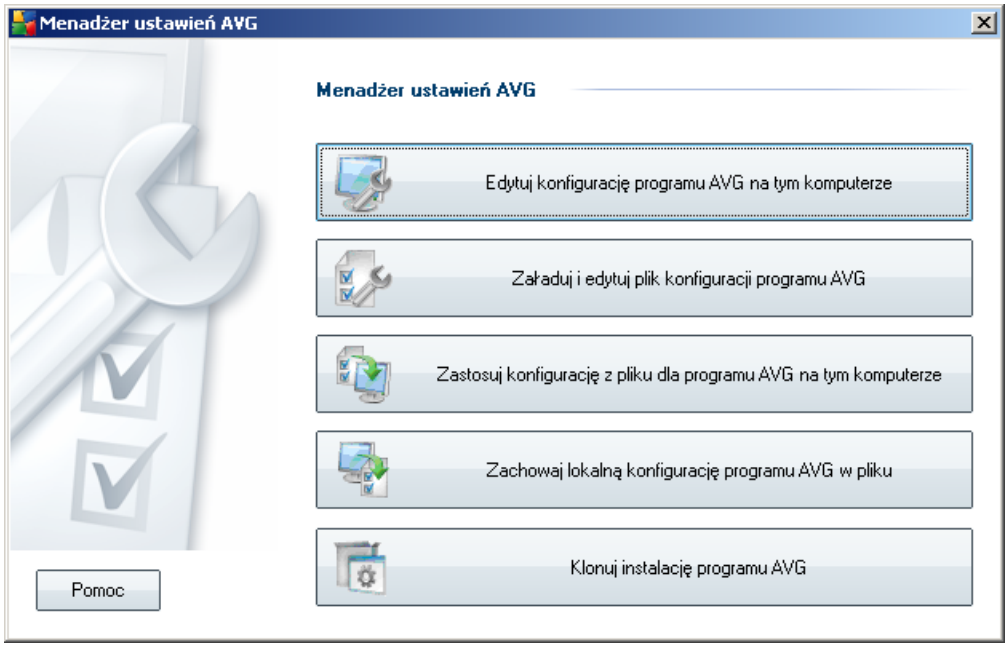
- ***Opróznij liste*** - powoduje usuniecie wszystkich wpisów z listy zdarzen.
- ***Odswiez liste*** - powoduje odswiezenie zawartosci listy zdarzen.

14. Menedzer ustawien AVG

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

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

Wszystkie programy/AVG 9.0/Menedzer ustawien systemu AVG



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

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

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

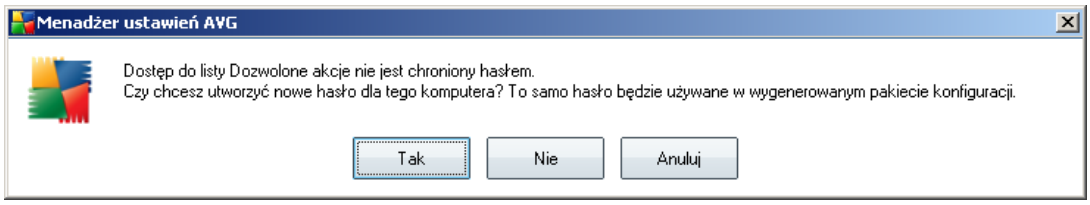
  Jesli plik konfiguracyjny AVG (.pck) juz istnieje, mozna go otworzyc do edycji za pomoca tego przycisku. Po zatwierdzeniu zmian przyciskiem ***OK*** lub ***Zastosuj*** plik zostanie zastapiony nowymi ustawieniami!

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

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

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

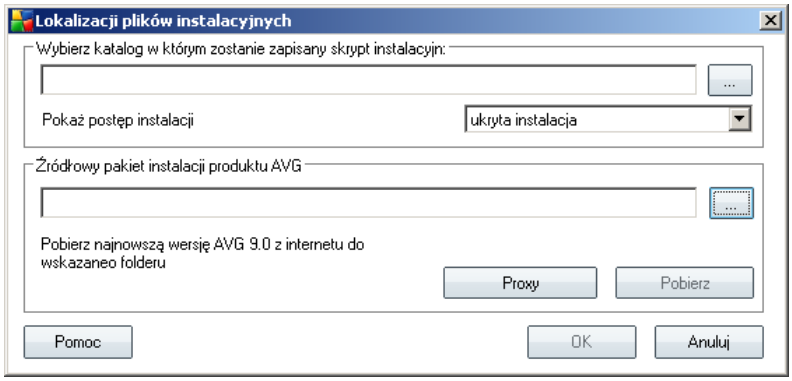
  Ten przycisk pozwala zapisac plik konfiguracyjny (.pck) lokalnej instalacji systemu AVG. Jesli dla dozwolonych akcji nie zostalo ustawione haslo, moze zostac wyswietlone nastepujace okno dialogowe:



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

- ***Klonuj instalacje systemu AVG***

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



  Nastepnie z menu rozwijanego nalezy wybrac jedna z nastepujacych opcji:

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

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

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

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

15. FAQ i pomoc techniczna

W przypadku jakichkolwiek problemów z oprogramowaniem AVG (w kwestiach handlowych lub technicznych) nalezy skorzystac z sekcji ***FAQ*** witryny systemu AVG (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***.