AVG 8.5 Anti-Virus plus Firewall Edition

Podrecznik uzytkownika

Wersja dokumentu 85.1 (26.1.2009)

Spis tresci

1. Wprowadzenie

Ten podrecznik uzytkownika zawiera dokumentacje systemu **AVG 8.5 Anti-Virus plus Firewall**.

Gratulujemy zakupu produktu AVG 8.5 Anti-Virus plus Firewall!

AVG 8.5 Anti-Virus plus Firewall nalezy do linii uznanych i nagradzanych produktów AVG, które zapewniaja uzytkownikom spokój ducha, a ich komputerom — pelne bezpieczenstwo. Podobnie jak pozostale produkty AVG, **AVG 8.5 Anti-Virus plus Firewall** zaprojektowano od podstaw pod katem zapewnienia slynnego juz poziomu ochrony, w nowy, bardziej przyjazny dla uzytkownika sposób.

Najnowszy produkt **AVG 8.5 Anti-Virus plus Firewall** zyskal poprawiony interfejs oraz bardziej agresywny i szybszy silnik skanujacy. 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 AVG

2.1. Obslugiwane systemy operacyjne

AVG 8.5 Anti-Virus plus Firewall jest przeznaczony do ochrony stacji roboczych z nastepujacymi systemami operacyjnymi:

- Windows 2000 Professional z dodatkiem SP4 + pakiet zbiorczy aktualizacji 1
- Windows XP Home Edition z dodatkiem SP2
- Windows XP Professional z dodatkiem SP2
- Windows XP Professional x64 Edition z dodatkiem SP1
- Windows Vista (x86 i x64, wszystkie edycje)

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

2.2. Minimalne wymagania sprzetowe

Minimalne wymagania sprzetowe dla systemu **AVG 8.5 Anti-Virus plus Firewall** sa nastepujace:

- Procesor Intel Pentium 1,2 GHz
- 70 MB wolnego miejsca na dysku twardym (dla instalacji),
- 256 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 firmy AVG (www.avg.com).

Przed rozpoczeciem instalacji systemu AVG zalecamy odwiedzenie naszej witryny w celu sprawdzenia, czy jest dostepny nowy plik instalacyjny. W ten sposób zyskasz pewnosc, ze zostanie zainstalowana najnowsza wersja systemu AVG 8.5 Anti-Virus plus Firewall.

Zalecamy takze wypróbowanie nowego narzedzia — AVG Download Manager pomoze Ci wybrac odpowiedni plik instalacyjny!

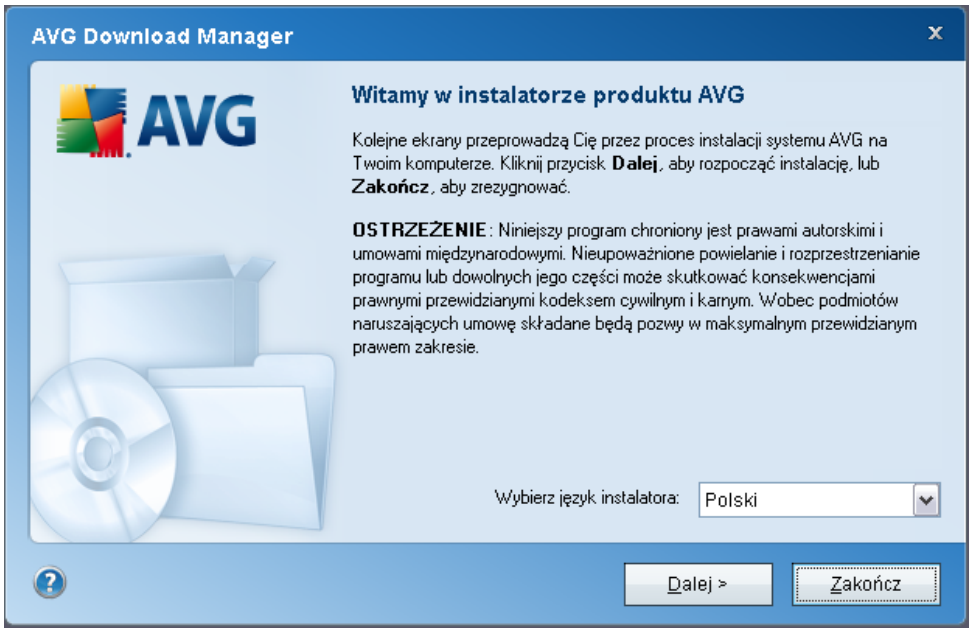
Podczas samego procesu konieczne bedzie podanie numeru licencji/sprzedazy. Nalezy wiec przygotowac go przed rozpoczeciem instalacji. Numer sprzedazy znajduje sie na opakowaniu dysku CD. W przypadku zakupienia pakietu AVG przez internet, numer licencji dostarczany jest poprzez e-mail.

4. AVG Download Manager

AVG Download Manager to proste narzedzie pomagajace wybrac odpowiedni plik instalacyjny dla danego produktu AVG. Na podstawie wprowadzonych przez uzytkownika informacji, menedzer wybierze odpowiedni produkt, typ licencji, zestaw skladników i jezyk. Na koniec **AVG Download Manager** pobierze odpowiednie pliki i rozpocznie proces instalacji.

Ponizej znajduje sie krótki opis wszystkich kroków, przez które przeprowadzi Cie **AVG Download Manager**:

4.1. Wybór jezyka

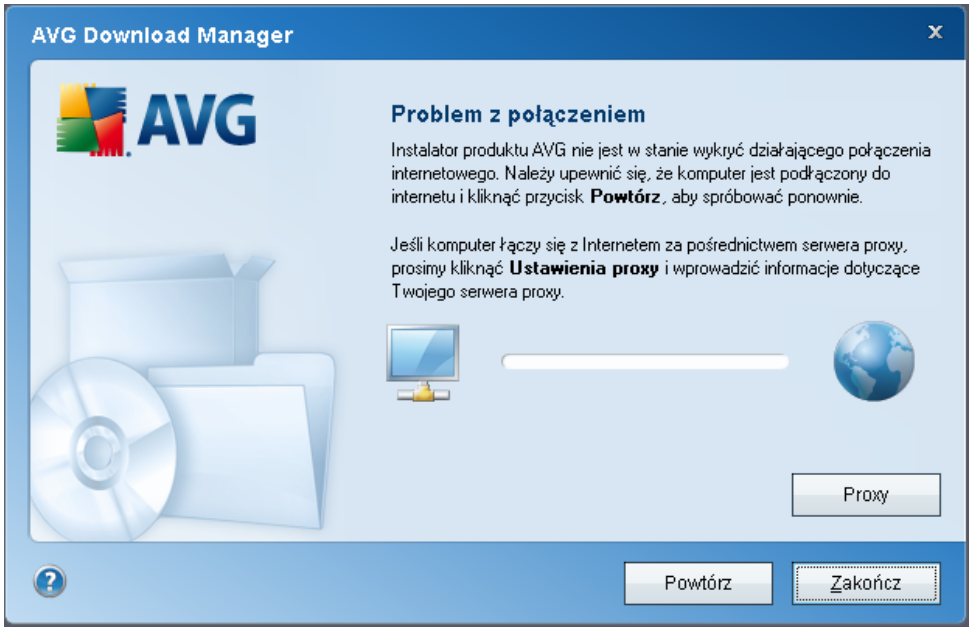


AVG Download Manager pozwoli w pierwszym kroku wybrac jezyk instalacji. Nalezy pamietac, ze wybór ten dotyczy tylko procesu instalacji; po jej zakonczeniu jezyk programu bedzie mozna zmienic bezposrednio w jego ustawieniach. Aby kontynuowac, kliknij przycisk ***Dalej***.

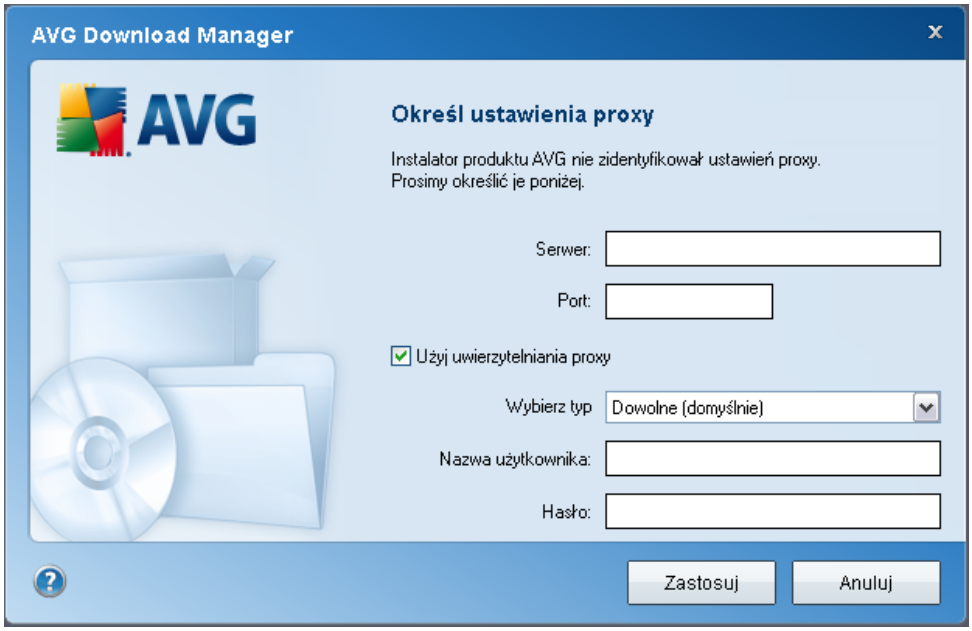
4.2. Test polaczenia

W nastepnym kroku **AVG Download Manager** próbuje nawiazac lacznosc z serwerem aktualizacyjnym. Przejscie dalej nie bedzie mozliwe, dopóki **AVG Download Manager** nie zakonczy testu polaczenia.

- Jesli test wykaze brak lacznosci, nalezy upewnic sie, ze komputer jest faktycznie polaczony z internetem. Aby ponowic próbe, kliknij przycisk ***Powtórz***

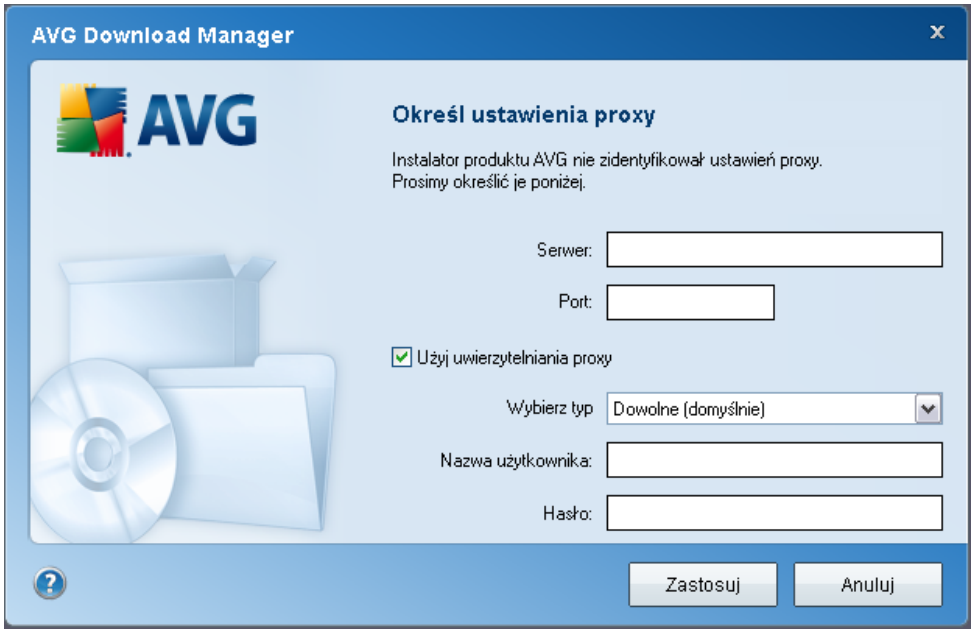


- Jesli uzywasz serwera proxy, kliknij przycisk ***Ustawienia proxy*** i podaj wymagane szczegóły:



- Jesli test wypadl pomyslnie, kliknij przycisk ***Dalej***, aby kontynuowac.

4.3. Ustawienia proxy



Jesli **AVG Download Manager** nie moze zidentyfikowac ustawien proxy, trzeba okreslic je recznie. Podaj nastepujace informacje:

- ***Serwer*** — prawidlowa nazwa lub adres IP serwera proxy.
- ***Port*** — odpowiedni numer portu.
- ***Uzyj uwierzytelniania proxy*** — zaznacz to pole, jesli Twój serwer proxy wymaga uwierzytelniania.
- ***Wybierz typ uwierzytelniania*** — wybierz z listy rozwijanej typ uwierzytelniania. Stanowczo zalecamy, aby zachowac wartosc domyslna (*serwer sam poda swoje wymagania*). Doswiadczeni uzytkownicy moga jednak wybrac opcje "Podstawowe" (*wymagane przez niektóre serwery*) lub "NTLM" (*wymagane przez wszystkie serwery ISA*). Nastepnie podaj prawidlowa ***Nazwe uzytkownika*** i ***Haslo*** (opcjonalnie).

Po potwierdzeniu ustawien (za pomoca przycisku ***Zastosuj***), **AVG Download Manager** automatycznie przejdzie do nastepnego kroku.

4.4. Wybór typu licencji

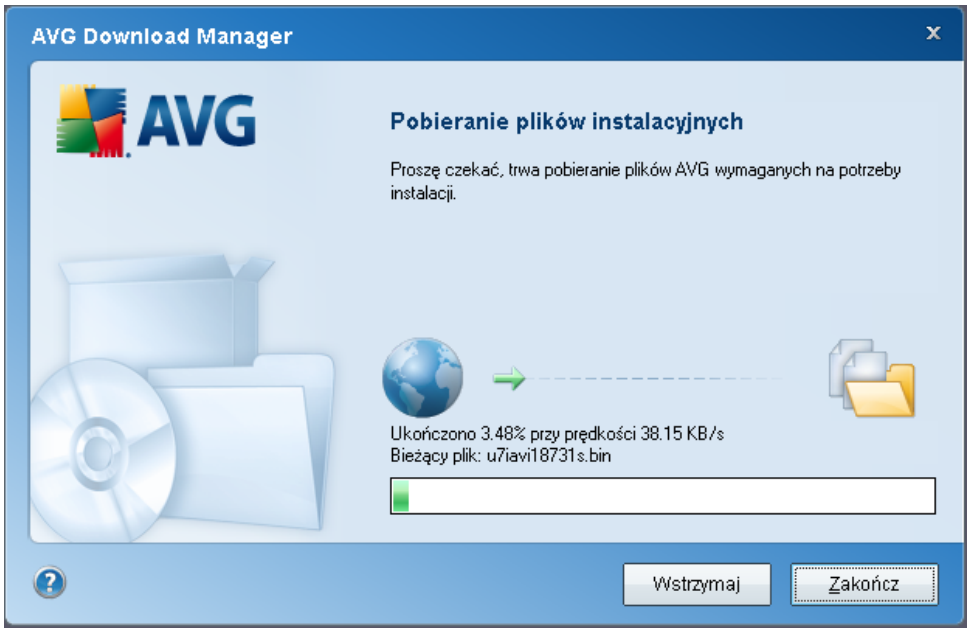
W tym kroku nalezy wybrac typ licencji produktu, który ma zostac pobrany. Dostepne typy to:

- ***Wersja pelna*** — tj. ***AVG Anti-Virus***, ***AVG Anti-Virus plus Firewall*** lub ***AVG Internet Security.***

- ***Wersja próbna*** — daje mozliwosc wypróbowania wszystkich funkcji wersji pelnej przez okres 30 dni.

- ***Wersja bezplatna*** — oferuje bezplatna ochrone uzytkownikom prywatnym. Posiada jednak pewne ograniczenia. Wersja bezplatna zapewnia tylko niektóre funkcje oferowane przez wersje komercyjna.

4.5. Pobieranie plików instalacyjnych



Wszystkie informacje, których **AVG Download Manager** potrzebuje do pobrania pakietów instalacyjnych i uruchomienia instalacji, zostaly juz podane. Mozna rozpoczac instalacje systemu AVG.

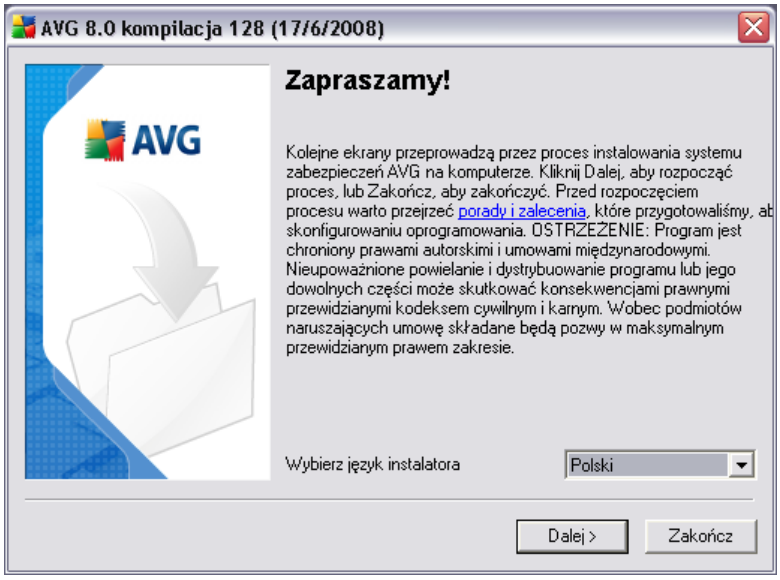
5. Proces instalacji systemu AVG

Aby zainstalowac na komputerze system AVG, nalezy najpierw zdobyc najnowszy instalator programu. 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 (pod adresem www.avg.com) w sekcji ***Pobierz.*** Mozna równiez uzyc nowego narzedzia — **AVG Download Manager** pomaga wybrac odpowiedni pakiet i automatycznie uruchamia proces instalacji.

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

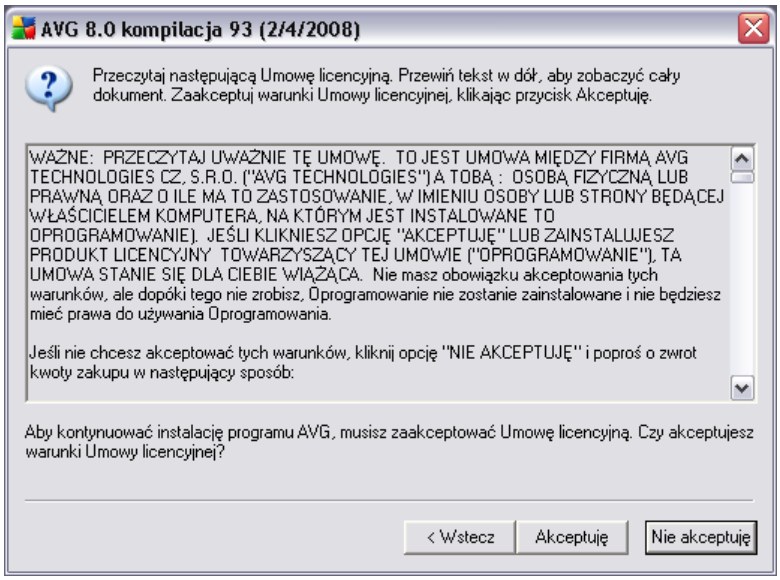
5.1. Uruchamianie instalacji



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.

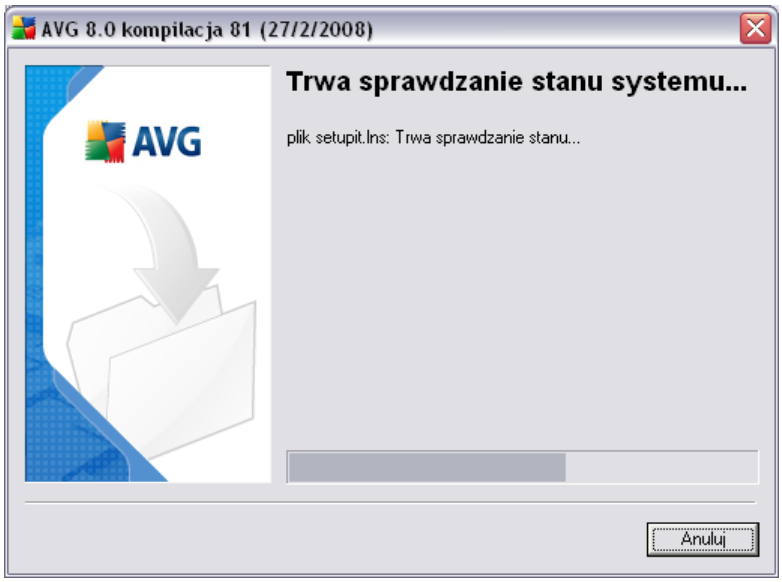
Uwaga: *W tym miejscu wybierany jest tylko jezyk instalatora. Nie jest to jezyk samego systemu AVG — ten zostanie wybrany na dalszym etapie instalacji.*

5.2. Umowa licencyjna



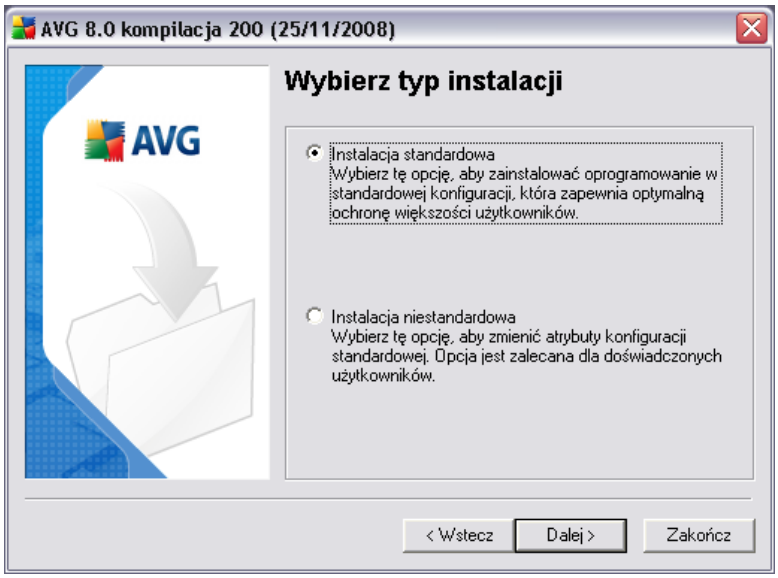
Okno dialogowe ***Umowa licencyjna*** zawiera pelna tresc umowy licencyjnej AVG. Nalezy uwaznie ja przeczytac, a nastepnie kliknac przycisk ***Akceptuje***, aby potwierdzic, ze zostala ona przeczytana, zrozumiana i zaakceptowana. Jesli nie zgadzasz sie na postanowienia umowy, kliknij przycisk ***Nie akceptuje***; instalacja zostanie natychmiast przerwana.

5.3. 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.

5.4. 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 programu AVG z domyslnymi ustawieniami, np. na komputerach o specyficznej konfiguracji sprzetowej.

5.5. Uaktywnienie licencji AVG

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

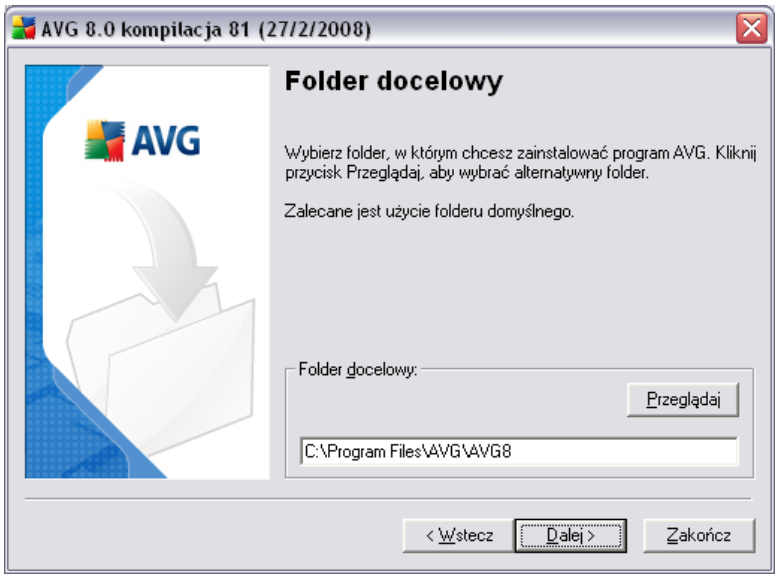
Nastepnie wprowadz numer licencji (lub numer sprzedazy) w polu tekstowym ***Numer licencji/sprzedazy***. Numer sprzedazy znajduje sie na opakowaniu dysku CD z oprogramowaniem AVG. Numer licencji jest wysylany poprzez e-mail po zakupieniu

oprogramowania AVG 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***.

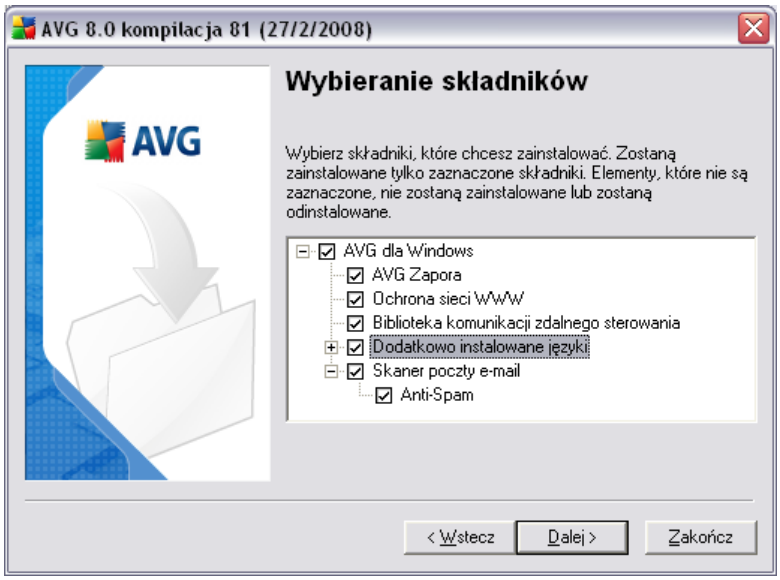
Jesli w poprzednim kroku zostala wybrana instalacja standardowa, nastapi przekierowanie bezposrednio do okna ***Podsumowanie instalacji*** . Jesli zostala wybrana instalacja niestandardowa, zostanie wyswietlone okno ***Folder docelowy***.

5.6. Instalacja niestandardowa — Folder docelowy



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

5.7. Instalacja niestandardowa — Wybór skladników



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

Wybierac mozna jednak tylko skladniki nalezace do zakupionej edycji systemu AVG. Tylko one beda widoczne w niniejszym oknie dialogowym!

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.

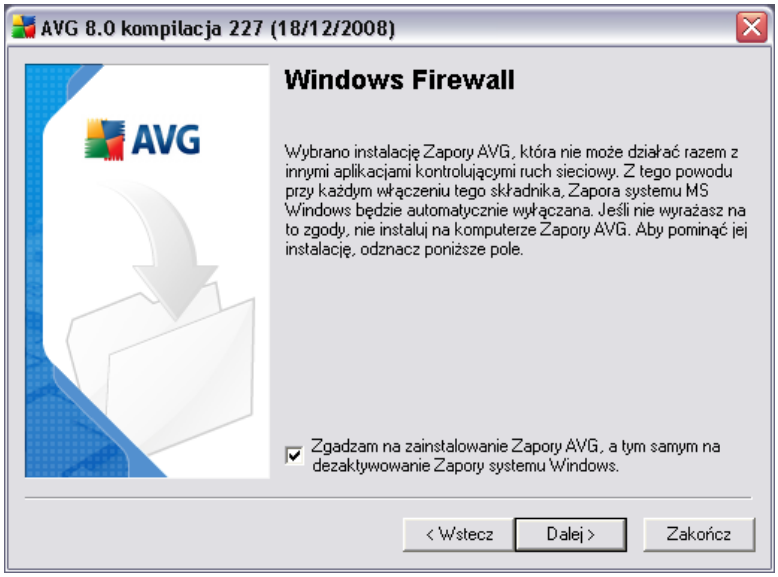
Wybranie pozycji ***Skaner poczty e-mail*** pozwala wskazac pluginy, które maja zostac zainstalowane w celu zapewnienia ochrony wiadomosci. Domyslnie instalowany jest ***Dodatek dla programu Microsoft Outlook***. Inna opcja jest ***Dodatek dla programu The Bat!*** W przypadku korzystania z innego klienta poczty e-mail (*MS Exchange, Qualcomm Eudora, ...*) nalezy wybrac ***Uniwersalny skaner poczty e-mail*** , który chroni wiadomosci e-mail niezaleznie od uzywanego programu pocztowego.

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

5.8. Pasek narzedzi AVG Security Toolbar

W oknie dialogowym ***AVG Security Toolbar*** nalezy okreslic, czy ma zostac zainstalowany ***Pasek narzedzi AVG Security Toolbar*** — jesli pozostawisz ustawienia domyslne, skladnik ten bedzie automatycznie zainstalowany w przegladarce internetowej. Zapewnia on wszechstronna ochrone w sieci WWW dzieki technologii AVG 8.0 i AVG XPL.

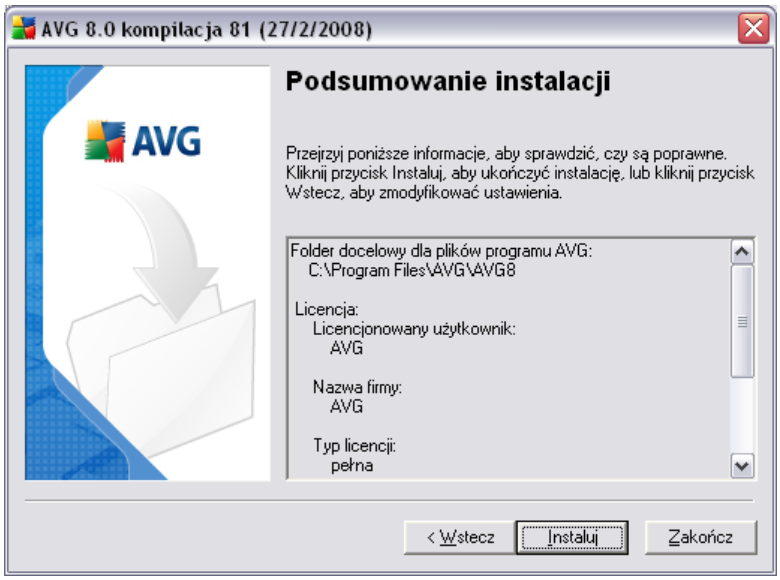
5.9. Zapora systemu Windows



Podany w jednym z wczesniejszych kroków numer licencji odpowiada wersji pakietu **AVG 8.5 Anti-Virus plus Firewall** zawierajacej ***Zapore***. ***Zapora AVG*** nie moze współpracowac z zadna inna zapora internetowa. W tym oknie dialogowym nalezy potwierdzic, ze chcesz zainstalowac ***Zapore AVG*** i jednoczesnie wylaczyc Zapore systemu Windows.

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

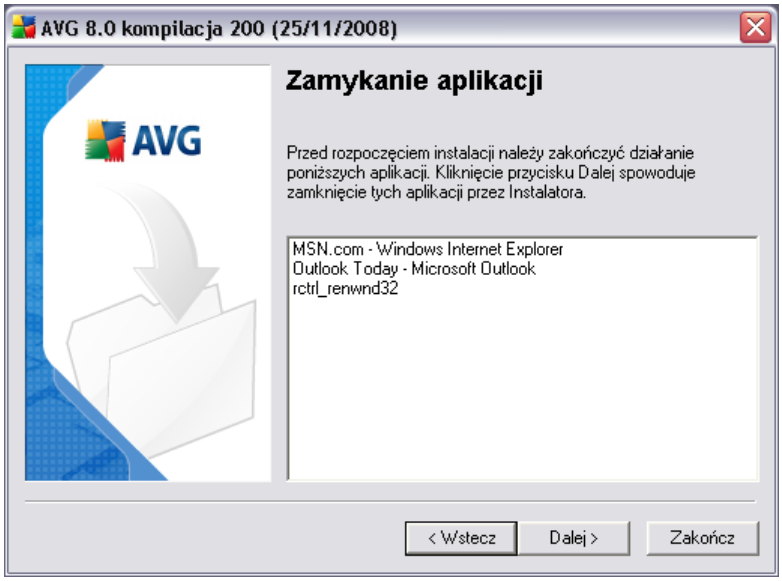
5.10.Podsumowanie instalacji



Okno ***Podsumowanie instalacji*** zawiera przeglad wszystkich jej parametrów. Prosimy upewnic sie, ze podane informacje sa poprawne. Jesli tak, kliknij przycisk ***Zakoncz***, aby kontynuowac. W przeciwnym razie kliknij przycisk ***Wstecz***, aby powrócic do poprzednich kroków i skorygowac ustawienia.

5.11.Zakonczenie programu

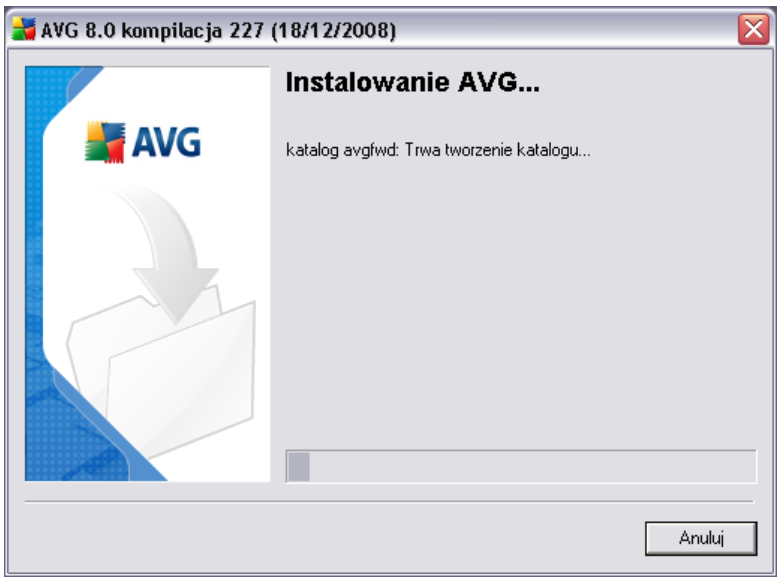
Przed rozpoczeciem instalacji moze pojawic sie monit proszacy o zamkniecie okreslonych programów, które moga zaklócic proces instalacji systemu AVG. W takim przypadku wyswietlane jest nastepujace okno (***Zamykanie aplikacji***). Okno ma charakter wylacznie informacyjny i nie wymaga dzialania ze strony uzytkownika — jesli wymienione programy moga zostac automatycznie zamkniete, wystarczy wybrac przycisk ***Dalej***, aby kontynuowac:



Uwaga: *Przed potwierdzeniem zamkniecia dzialajacych programów nalezy zapisac wszystkie uzywane przez nie pliki.*

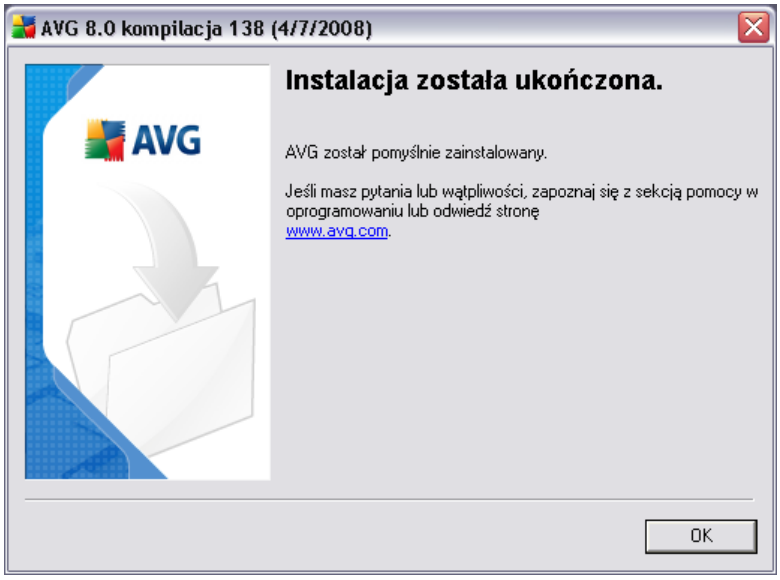
5.12.Instalowanie

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



Nalezy poczekac na ukonczenie instalacji, po której nastapi przekierowanie do okna ***Instalacja zakonczona***.

5.13.Instalacja zakonczona



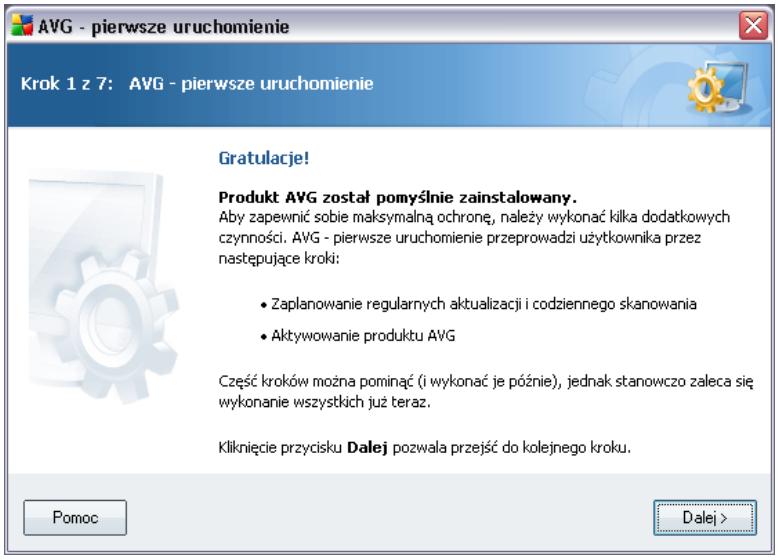
Okno ***Instalacja zostala ukonczona!*** to ostatni krok procesu instalacji systemu AVG. Program AVG jest zainstalowany na komputerze i w pelni funkcjonalny. System ten dziala w tle, calkowicie automatycznie.

Po zakonczeniu instalacji automatycznie uruchomiony zostanie ***Kreator Konfiguracji Podstawowej AVG***, który w kilku krokach pomoze Ci **AVG 8.5 Anti-Virus plus Firewall** w uzyskaniu optymalnej konfiguracji. Konfiguracje programu AVG bedzie mozna edytowac w dowolnym momencie. Zalecamy jednak zdefiniowanie podstawowych ustawien za pomoca kreatora.

6. Kreator pierwszego uruchomienia AVG

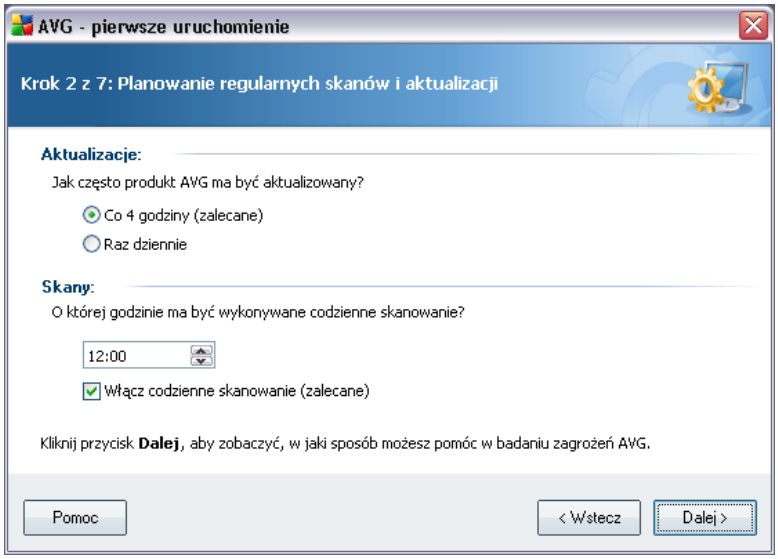
Po pierwszym zainstalowaniu programu AVG, wyswietlone zostanie okno ***Kreatora konfiguracji podstawowej AVG***, umozliwiajacego wprowadzenie poczatkowych ustawien programu**AVG 8.5 Anti-Virus plus Firewall**. Pomimo tego, ze wszystkie wymagane parametry mozna ustawic później, zaleca sie skorzystanie z kreatora, aby w prosty i szybki sposób zabezpieczyc komputer. Postepuj zgodnie z krokami opisanymi w poszczególnych oknach kreatora :

6.1. Wprowadzenie do Kreatora pierwszego uruchomienia AVG



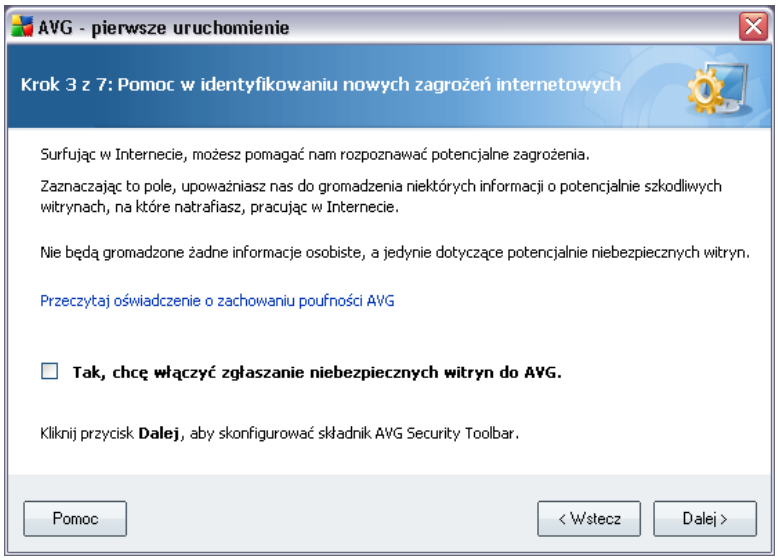
Okno ***Witamy w Kreatorze pierwszego uruchomienia AVG*** zawiera krótkie podsumowanie stanu programu AVG na komputerze oraz sugestie, jakie czynnosci nalezy wykonac, aby zapewnic calkowita ochrone. Kliknij przycisk ***Dalej***, aby kontynuowac instalacje.

6.2. Zaplanowanie regularnych skanów i aktualizacji



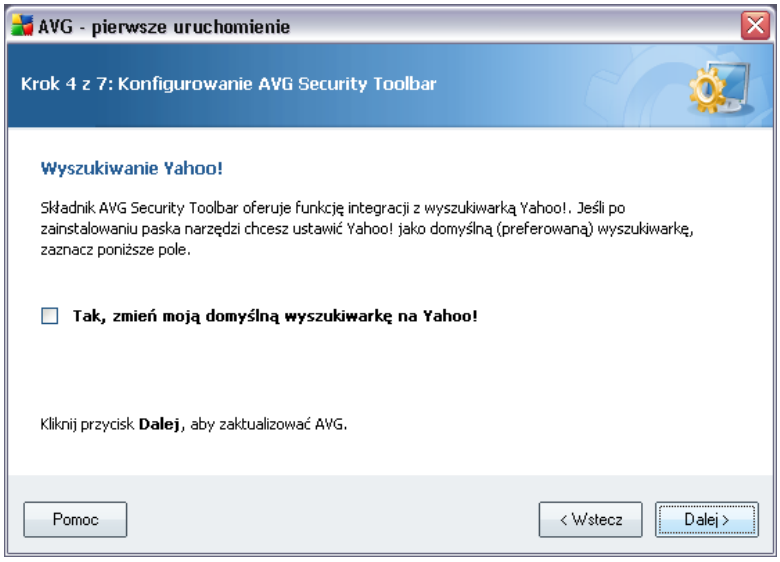
W oknie dialogowym ***Planowanie cyklicznych skanów i aktualizacji*** okresla sie czestotliwosc sprawdzania dostepnosci nowych plików aktualizacji i zdefiniowanie czasu, w którym nalezy uruchomic skan zaplanowany. Zaleca sie zachowanie wartosci domyslnych. Aby kontynuowac, kliknij przycisk ***Dalej***.

6.3. Pomoc w identyfikacji nowych zagrozen internetowych



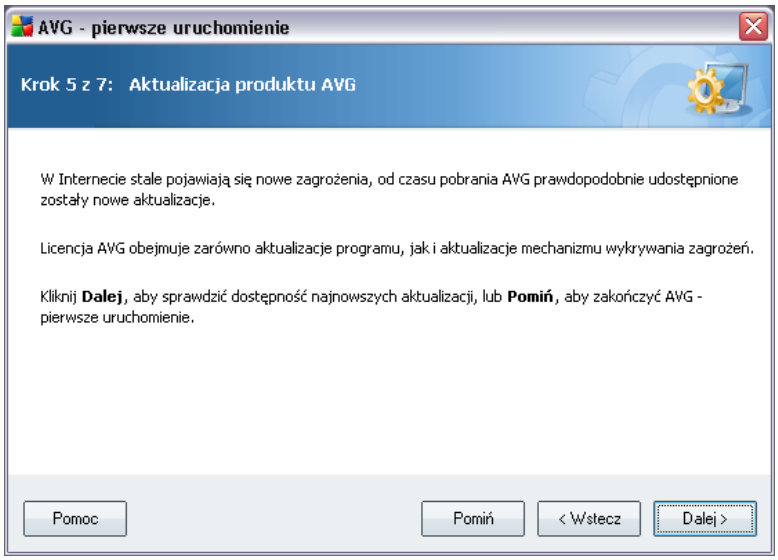
W oknie o nazwie ***Pomóz nam identyfikowac nowe zagrozenia*** nalezy okreslic, czy ma zostac wlaczona opcja zglaszania niebezpiecznych i szkodliwych witryn znalezionych przy uzyciu funkcji ***AVG Surf-Shield / AVG Search-Shield*** , co pomoze uzupelnic baze danych AVG. Zaleca sie zachowanie ustawien domyslnych i korzystanie z funkcji raportowania. Aby kontynuowac, kliknij przycisk ***Dalej***.

6.4. Konfiguracja paska narzedzi AVG Security Toolbar



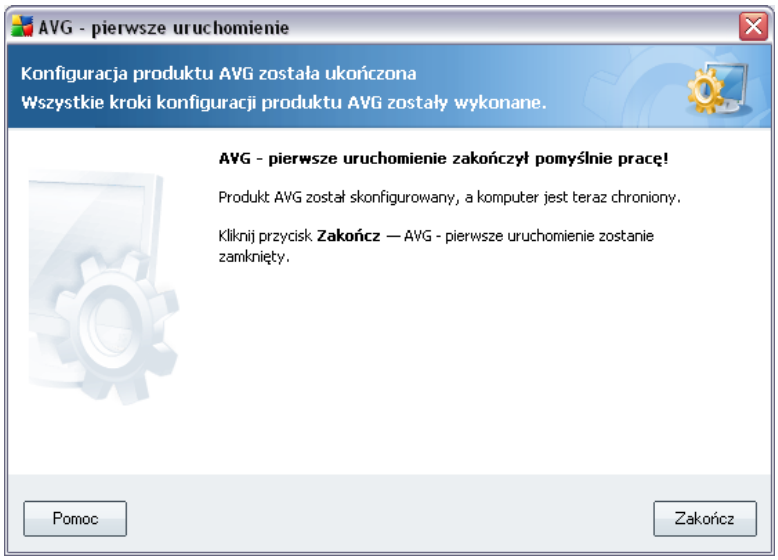
W oknie dialogowym ***Skonfiguruj pasek narzedzi zabezpieczen systemu AVG*** mozna zaznaczyc pole wyboru w celu okreslenia, ze serwis Yahoo! ma byc domyslna wyszukiwarka.

6.5. Aktualizacja ochrony AVG



Korzystajac z okna ***Aktualizacja ochrony AVG***, mozna automatycznie sprawdzic i pobrac najnowsze aktualizacje programu AVG. Nalezy kliknac przycisk ***Dalej***, aby pobrac najnowsze pliki aktualizacji i wykonac aktualizacje.

6.6. Konfiguracja programu AVG zostala ukonczona



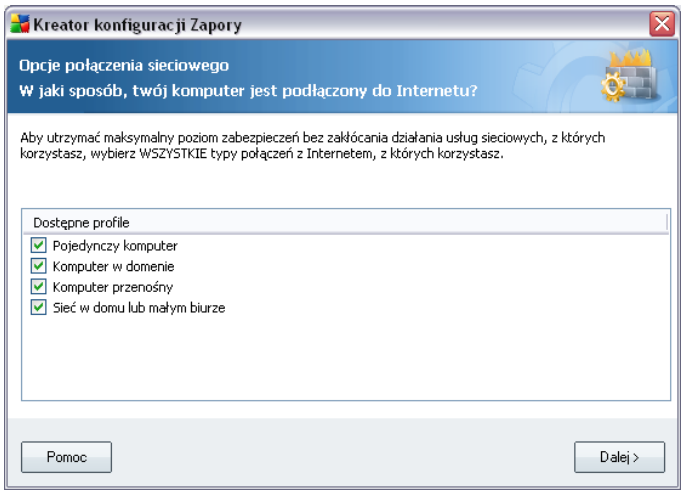
Program **AVG 8.5 Anti-Virus plus Firewall** zostal skonfigurowany. Kliknij przycisk ***Zakoncz***, aby rozpoczac korzystanie z AVG.

7. Kreator konfiguracji Zapory

Kreator konfiguracji Zapory jest uruchamiany automatycznie po instalacji **AVG 8.5 Anti-Virus plus Firewall**. Mimo, ze mozliwe jest skonfigurowanie parametrów programu w pózniejszym czasie, zaleca sie skorzystanie z kreatora , aby juz od poczatku zapewnic prawidlowe dzialanie ***Zapory***.

Kreator konfiguracji Zapory moze byc takze wywolany bezposrednio z interfejsu skladnika Zapora, poprzez kliknieciе przycisku ***Kreator konfiguracji***.

7.1. Opcje polaczen sieciowych



W tym oknie, ***Kreator konfiguracji Zapory*** wyswietla pytanie o sposób podlaczenia komputera do internetu. Na przyklad: notebook laczacy sie z internetem z wielu róznych lokalizacji (*lotniska, pokoje hotelowe itp.*) wymaga bardziej rygorystycznych regul zabezpieczen niz komputer pracujacy w domenie (*siec firmowa itp.*). Domyslne reguly ***Zapory*** zostana dopasowane do poziomu zabezpieczen zapewnianych przez wybrany rodzaj polaczenia.

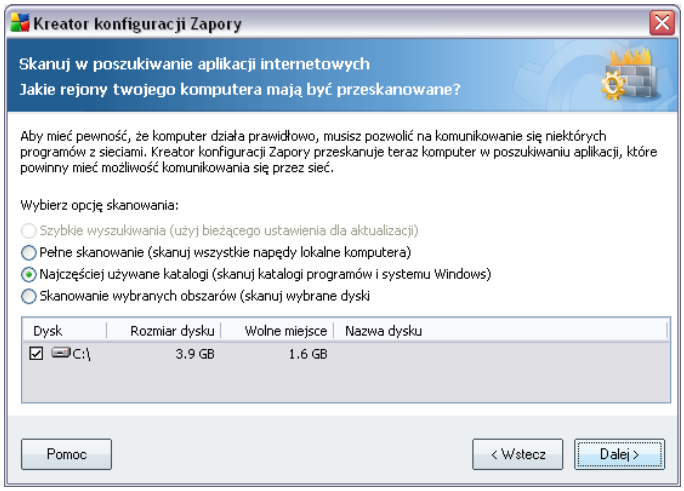
Dostepne sa trzy opcje:

- ***Pojedynczy komputer***
- ***Komputer w domenie*** (siec firmowa).
- ***Komputer przenosny (***zazwyczaj notebook).

- ***Siec w domu lub malym biurze***

Zaznacz typ polaczenia, które odpowiada najczestszemu sposobowi uzywania komputera. Mozna zaznaczyc wiecej niz jedna opcje, jesli komputer jest uzywany na kilka sposobów. Wybór nalezy potwierdzic kliknieciem przycisku ***Dalej***, co spowoduje przejscie do nastepnego okna dialogowego.

7.2. Skanowanie w poszukiwaniu aplikacji internetowych



Do utworzenia poczatkowej konfiguracji ***Zapory*** konieczne jest przeskanowanie komputera i okreslenie wszystkich aplikacji i uslug systemowych, które musza komunikowac sie poprzez siec. Dla wszystkich takich aplikacji i uslug nalezy utworzyc poczatkowe reguly ***Zapory***.

Uwaga: *Kreator wykrywa wiekszosc ogólnie znanych aplikacji komunikujacych sie poprzez siec i definiuje dla nich wlasne reguly. Moze sie jednak zdarzyc, ze nie wszystkie aplikacje zostana wykryte.*

W oknie dialogowym ***Skanuj w poszukiwaniu aplikacji internetowych*** nalezy okreslic, czy ma byc przeprowadzone:

- ***Szybkie wyszukiwanie*** — ta opcja jest aktywna tylko, jesli skladnik ***Firewall*** zostal wczesniej odpowiednio skonfigurowany; wyszukiwane beda tylko aplikacje obecnie zapisane w istniejacej konfiguracji skladnika ***Firewall***. Zostanie dla nich zastosowana nowa domyslna konfiguracja (tj. zalecana przez producenta). Nalezy zwrócic uwage na fakt, ze nie zostana wykryte zadne nowe aplikacje! Ta opcja jest zalecana, jesli uzytkownik okreslil juz reguly skladnika***Firewall*** i chce uniknac powtórnego procesu skanowania.

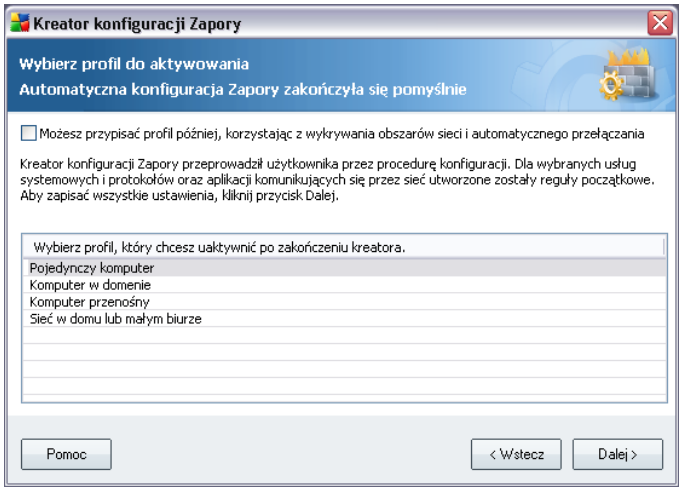
- ***Pelne skanowanie*** — skanowanie wszystkich napedów lokalnych komputera;
- ***Najczesciej uzywane katalogi*** — (*domyslnie*) skanowanie tylko katalogów programów i systemu Windows (czas skanowania jest znacznie krótszy);
- ***Skanowanie wybranych obszarów*** — nalezy okreslic dyski twarde, które maja zostac przeskanowane.

7.3. Wybór profilu do aktywowania

Okno ***Wybierz profil, który chcesz aktywowac*** zawiera informacje o konfiguracji ***Zapory*** utworzonej we wczesniejszych krokach.

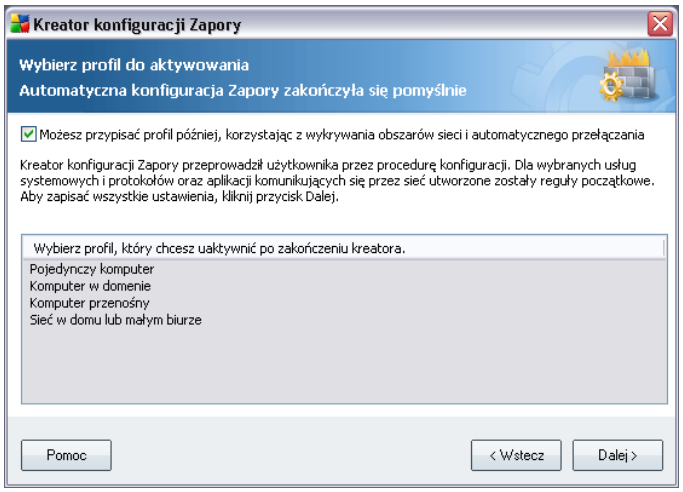
Przed zamknieciem ***Kreatora konfiguracji Zapory*** nalezy wybrac profil, który bedzie aktualnie uzywany. Dostepne beda maksymalnie trzy opcje (pojedynczy komputer, komputer w domenie i komputer przenosny), zgodnie z parametrami polaczenia wybranymi w pierwszym oknie Kreatora (***Opcje polaczen sieciowych***). W pózniejszym czasie mozna przelaczac wstepnie zdefiniowane profile ***Zapory***, zgodnie z biezacym stanem komputera.

W tym momencie wystarczy wybrac zadany profil z listy i aktywowac go, wybierajac przycisk ***Dalej***:



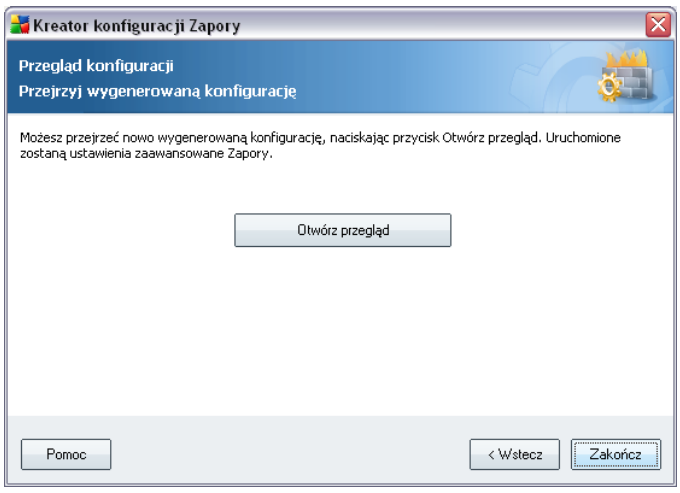
Jesli nie chcesz recznie definiowac profili, mozesz uzyc funkcji automatycznego wykrywania. W takim wypadku ***Zapora AVG*** bedzie automatycznie wybierala profil najodpowiedniejszy dla biezacej lokalizacji i aktywnych polaczen sieciowych. Automatyczne wykrywanie profili zapewnia maksymalna ochrone komputera. Aby uzyc tej opcji, zaznacz pole ***Przypisz profil pózniej, korzystajac z wykrywania***

obszarów i automatycznego przelaczania profili w górnej czesci okna dialogowego:



Spowoduje to dezaktywacje listy profili; wystarczy kliknac wówczas przycisk ***Dalej*** i przejsc do kolejnego okna dialogowego.

7.4. Przeglad konfiguracji



Okno ***Przeglad konfiguracji*** konczy dzialanie ***Kreatora konfiguracji Zapory***. Kliknij przycisk ***Zakoncz***, aby zapisac wstepne ustawienia skladnika ***Zapora***. Jesli chcesz wyswietlic zastosowane parametry lub kontynuowac szczególowa konfiguracje skladnika ***Zapora***, kliknij przycisk ***Otwórz przeglad***, aby przelaczyc sie do interfejsu

ustawien Zapory.

8. Po instalacji

8.1. Rejestracja produktu

Po ukonczeniu instalacji systemu **AVG 8.5 Anti-Virus plus Firewall**, nalezy zarejestrowac produkt online na stronie internetowej AVG, w dziale ***Rejestracja*** (*postepujac zgodnie z wyswietlanymi tam instrukcjami*). Rejestracja daje pelny dostep do konta uzytkownika AVG, biuletynu aktualizacji AVG i innych uslug oferowanych wylacznie zarejestrowanym klientom.

8.2. 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/Wszystkie programy/AVG 8.0/Interfejs uzytkownika AVG.***

8.3. Skanowanie calego komputera

Istnieje ryzyko, ze Twój komputer zostal zainfekowany jeszcze przed zainstalowaniem systemu **AVG 8.5 Anti-Virus plus Firewall**. 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***.

8.4. Test Eicar

W celu potwierdzenia poprawnosci instalacji systemu **AVG 8.5 Anti-Virus plus Firewall**, mozna wykonac 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 rozpoczeciu pobierania pliku, skladnik ***Ochrona sieci WWW*** zareaguje wyswietleniem ostrzezenia. Pojawienie sie komunikatu ***Ochrony sieci WWW*** potwierdza, ze oprogramowanie AVG jest prawidlowo zainstalowane na komputerze.

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

8.5. Konfiguracja domyslna AVG

Konfiguracja domyslna (*ustawienia stosowane zaraz po zainstalowaniu*) pakietu **AVG 8.5 Anti-Virus plus Firewall** , wstepnie zdefiniowana przez dostawce oprogramowania, ma na celu zapewnienie optymalnej wydajnosci wszystkich skladników i 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 polecenie menu systemowego ***Narzedzia/Ustawienia zaawansowane*** i edytujac opcje w otwartym oknie dialogowym ***Zaawansowane ustawienia AVG***.

9. Interfejs uzytkownika AVG

AVG 8.5 Anti-Virus plus Firewall otwórz w głównym oknie

Główne okno Interfejsu Uzytkownika AVG jest podzielone na kilka sekcji:

- ***Menu główne*** *(górny wiersz okna)* to standardowe narzedzie nawigacyjne umozliwiajac 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 >>
- ***Linki*** *(lewa kolumna)* umozliwia uzyskanie szybkiego dostepu najwazniejszych i najczesciej uzywanych funkcji programu AVG — szczegóły >>
- ***Przeglad skladników*** *(centralna czesc okna)* zawiera przeglad zainstalowanych komponentów 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 >>

9.1. Menu systemowe

Menu systemowe to standardowa metoda nawigacji we wszystkich aplikacjach w systemie Windows. Znajduje sie ono na samej górze interfejsu uzytkownika **AVG 8.5 Anti-Virus plus Firewall**. Menu systemowe zapewnia dostep do poszczególnych skladników AVG, funkcji i uslug.

Menu systemowe jest podzielone na piec sekcji:

9.1.1. Plik

- ***Zakoncz*** — powoduje zamkniecie interfejsu uzytkownika **AVG 8.5 Anti-Virus plus Firewall** . System AVG dziala jednak w tle, a komputer jest nadal chroniony!

9.1.2. Skladniki

Pozycja ***Skladniki*** w menu glównym zawiera linki do wszystkich zainstalowanych skladników AVG; kliknięcie 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.

- ***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***.

- ***Zapora*** — otwiera domyslne okno interfejsu skladnika ***Zapora***.

-

-

- ***Skaner poczty e-mail*** — otwiera domyslne okno interfejsu skladnika ***Skaner***

poczty e-mail.

- ***Licencja*** — otwiera domyslne okno interfejsu skladnika ***Licencja***.
- ***Skaner laczy*** — otwiera domyslne okno dialogowe skladnika ***Skaner laczy***.
- ***Ochrona sieci WWW*** — otwiera domyslne okno interfejsu skladnika ***Ochrona sieci WWW***.
- ***Ochrona rezydentna*** — otwiera domyslne okno interfejsu skladnika ***Ochrona rezydentna***.
- ***Menedzer aktualizacji*** — otwiera domyslne okno interfejsu skladnika ***Menedzer aktualizacji***.

9.1.3. Historia

- ***Wyniki skanowania*** — powoduje przelaczenie do interfejsu skanera AVG, konkretnie do okna dialogowego ***Przeglad wyników skanowania***.
- ***Zagrozenia wykryte przez Ochrone Rezydentna*** — powoduje otwarcie okna dialogowego zawierajacego przeglad zagrozen wykrytych przez ***Ochrone Rezydentna.***
- ***Zagrozenie wykryte przez Skaner poczty e-mail*** — powoduje otwarcie okna zawierajacego przeglad zalaczników e-mail uznanych za niebezpieczne przez ***Skaner poczty e-mail***.
- ***Zagrozenia wykryte przez Ochrone sieci WWW*** — powoduje otwarcie okna dialogowego zawierajacego przeglad zagrozen wykrytych przez ***Ochrone sieci WWW.***
- ***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 8.5 Anti-Virus plus Firewall** .
- ***Zapora*** — powoduje otwarcie karty ***Dzienniki*** (dostepnej równiez w Konfiguracji Zapory), która zawiera szczegółowy przeglad wszystkich dzialan tego skladnika

9.1.4. Narzedzia

- ***Skanuj komputer*** — przelacza do Interfejsu skanera AVG i uruchamia skanowanie calego komputera.

- ***Skanuj wybrany folder*** — przelacza do Interfejsu skanera AVG i umozliwia zdefiniowanie (w ramach struktury katalogów i dysków) plików oraz folderów, które maja byc przeskanowane.

- ***Skanuj plik*** — umozliwia uruchomienie na zadanie testu pojedynczego, wskazanego pliku.

- ***Aktualizuj*** — automatycznie uruchamia proces aktualizacji. **AVG 8.5 Anti-Virus plus Firewall**

- ***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 **AVG 8.5 Anti-Virus plus Firewall** . Na ogól zaleca sie zachowanie domyslnych ustawien zdefiniowanych przez producenta oprogramowania AVG.

- ***Ustawienia Zapory*** — otwiera okno zaawansowanej konfiguracji skladnika ***Zapora AVG***.

9.1.5. Pomoc

- ***Spis tresci*** — powoduje otwarcie plików Pomocy systemu AVG.

- ***Uzyskaj pomoc online*** — otwiera witryne firmy AVG na stronie Centrum Pomocy Technicznej dla klientów.

- ***AVG - Twoje WWW*** — powoduje otwarcie strony glównej programu AVG (www.avg.com).

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

- ***Aktywuj ponownie*** — otwiera okno ***Aktywacja programu AVG*** zawierajace dane wprowadzone na etapie ***personalizacja 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*).

- ***Zarejestruj*** — powoduje polaczenie z witryna rejestracyjna www.avg.com. Nalezy tam podac swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysluguje bezplatna pomoc techniczna.

- ***AVG — informacje*** — powoduje otwarcie okna ***Informacje*** zawierajacego piec kart, z których mozna odczytac nazwe programu, wersje silnika antywirusowego i jego bazy danych, informacje o systemie, umowe licencyjna oraz informacje kontaktowe dotyczace firmy ***AVG Technologies CZ***.

9.2. Status bezpieczenstwa

Sekcja ***Status Bezpieczenstwa*** znajduje sie w górnej czesci Interfejsu uzytkownika AVG. Znajdziesz tam informacje o biezacym stanie bezpieczenstwa systemu **AVG 8.5 Anti-Virus plus Firewall**. W obszarze 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 równiez jest wyswietlana w sekcji ***Status Bezpieczenstwa*** .

Ikona jest takze wyswietlana, gdy z jakiegos powodu stan bledu skladnika ma byc ignorowany (opcja ***Ignoruj stan skladnika*** jest dostepna po kliknieciu prawym przyciskiem ikony odpowiedniego skladnika w sekcji przegladu skladników okna glównego AVG). Uzycie tej opcji moze byc wskazane a okreslonych sytuacjach, ale stanowczo zaleca sie jak najszybsze ponowne wylaczenie opcji ***Ignoruj stan skladnika***.

 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 równiez ikona na pasku zadan.*

9.3. Linki

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

- ***Przeglad*** — pozwala przelaczac miedzy biezacym interfejsem AVG i 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 ***Testy AVG >>***
- ***Aktualizuj teraz*** — otwiera interfejs aktualizacji i uruchamia proces aktualizacji systemu AVG (zobacz rozdzial ***Aktualizacje AVG >>***

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. Ponadto, dzialajacy proces jest dodatkowo

przedstawiony w formie graficznej — *zobacz obrazek nr 2*.

9.4. 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 stanie komponentów)
- Opis wybranego skladnika.

W systemie **AVG 8.5 Anti-Virus plus Firewall** sekcja ***Przeglad skladników*** zawiera informacje o nastepujacych skladnikach:

- ***Anti-Virus*** — zapewnia ochrone przed wirusami, które moga zainfekowac komputer — szczegóły >>

- ***Anti-Spyware*** — skanuje uruchamiane aplikacje w tle — szczegóły >>
- ***Anti-Rootkit*** — wykrywa programy i technologie próbujace ukryc w systemie szkodliwe oprogramowanie — szczegóły >>
- ***Zapora*** — kontroluje wymiane danych z innymi komputerami w sieci internet lub w sieci lokalnej — szczegóły >>
- ***Skaner poczty e-mail*** — sprawdza wszystkie przychodzace i wychodzace wiadomosci e-mail w poszukiwaniu wirusów — szczegóły >>
- ***Licencja*** — zawiera pelna tresc umowy licencyjnej AVG — szczegóły >>
- ***Skaner laczy sprawdza wyniki wyszukiwania wyswietlane przez przegladarke internetowa —*** szczegóły >>
- ***Ochrona sieci WWW*** — skanuje wszystkie dane pobierane przez przegladarke WWW — 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 interfejs skladnika, ale takze wybrac opcje ***ignorowania stanu skladnika***. Opcje te nalezy wybrac, jesli stan bledu skladnika jest znany, ale z dowolnego powodu system AVG ma byc nadal uzywany, a ikona na pasku zadan nie ma byc wyszarzona jako ostrzezenie.

9.5. 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 ostatniej aktualizacji.

- ***BD wirusów*** — aktualnie uzywana wersja bazy wirusów.
- ***Wersja AVG*** — zainstalowana wersja systemu AVG *(numer w formacie 8.0. xx, gdzie 8.0 to wersja linii produktów, a xx — numer kompilacji).*
- ***Data wygasniecia licencji*** — data wygasniecia licencji systemu AVG.

9.6. Ikona na pasku zadan

Ikona AVG na pasku zadan (*systemu Windows*) informuje o biezacym stanie programu **AVG 8.5 Anti-Virus plus Firewall**. Ikona ta jest zawsze widoczna, niezaleznie od tego, czy Interfejs uzytkownika AVG jest otwarty, czy tez nie.

Jesli ***ikona na pasku zadan*** jest kolorowa, oznacza to, ze 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 szara ze znakiem wykrzyknika oznacza problem (nieaktywny skladnik, stan bledu itd.). 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, przelaczenia profilu Zapory, zmiany stanu skladników, bledu itp.*) w wyskakujacym okienku:

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

- ***Otwórz Interfejs uzytkownika AVG*** — otwiera Interfejs uzytkownika.
- ***Aktualizuj*** — uruchamia natychmiastowa aktualizacje
- ***Zakoncz*** — zamyka system AVG *(zamykany jest tylko Interfejs uzytkownika, system AVG nadal dziala w tle i calkowicie chroni Twój komputer!)*

10. Skladniki AVG

10.1.Anti-Virus

10.1.1.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.

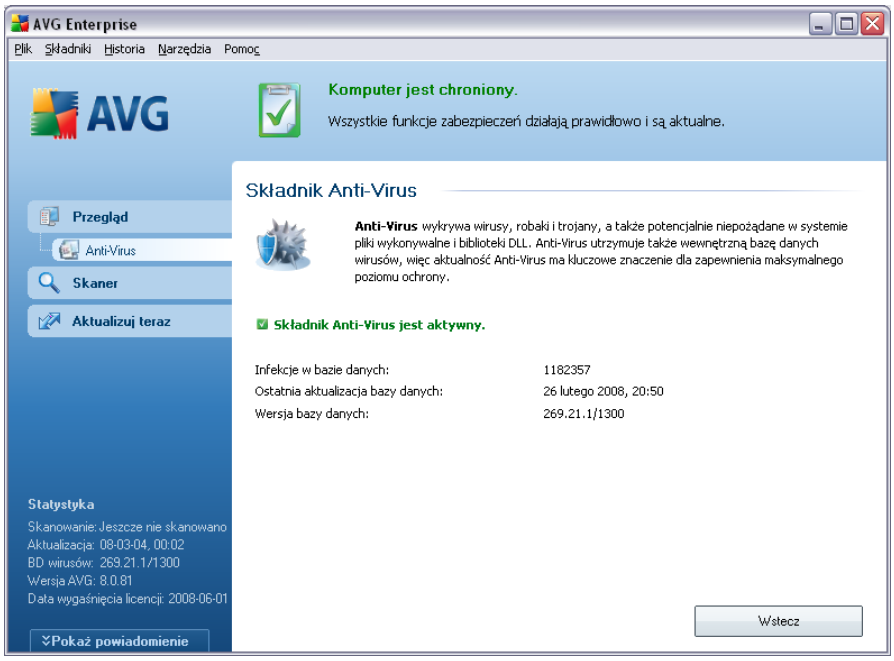
Wazna zaleta ochrony antywirusowej jest fakt, ze nie pozwala ona na uruchomienie zadnych znanych wirusów na komputerze!

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.

10.1.2.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; zwiekszany jest przy kazdej jej aktualizacji.

Interfejs tego skladnika zawiera tylko jeden przycisk (***Wstecz***) — kliknięcie go powoduje powrót do domyslnego Interfejsu uzytkownika 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 Zaawansowane ustawienia AVG.*

10.2.Anti-Spyware

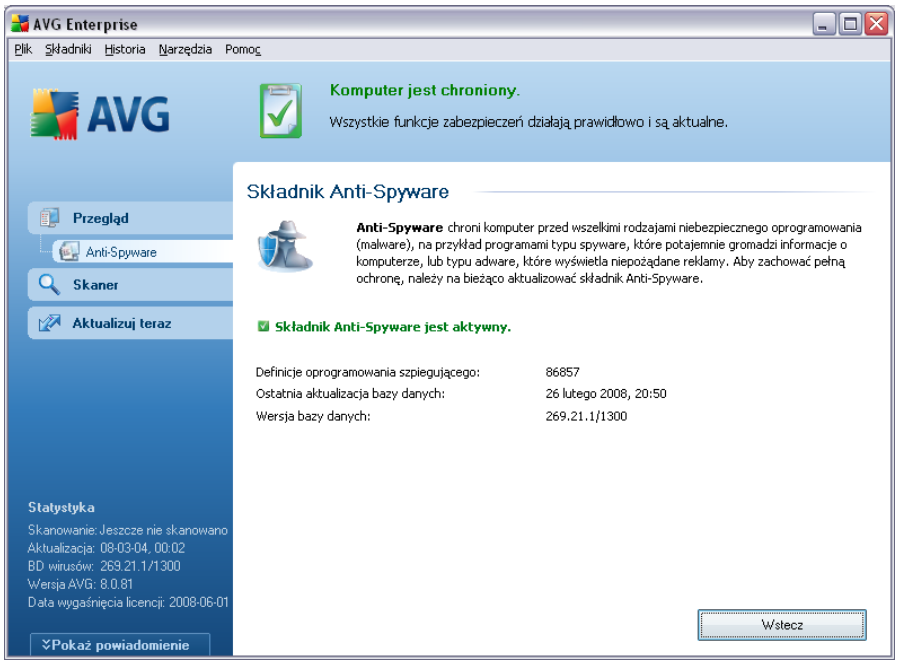
10.2.1.Zasady dzialania skladnika Anti-Spyware

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 pakietu **AVG 8.5 Anti-Virus plus Firewall**, 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.

10.2.2.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; zwiekszany jest on przy kazdej aktualizacji.

Interfejs tego skladnika zawiera tylko jeden przycisk (***Wstecz***) — klikniecie go powoduje powrót do domyslnego Interfejsu uzytkownika 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 Zaawansowane ustawienia AVG.*

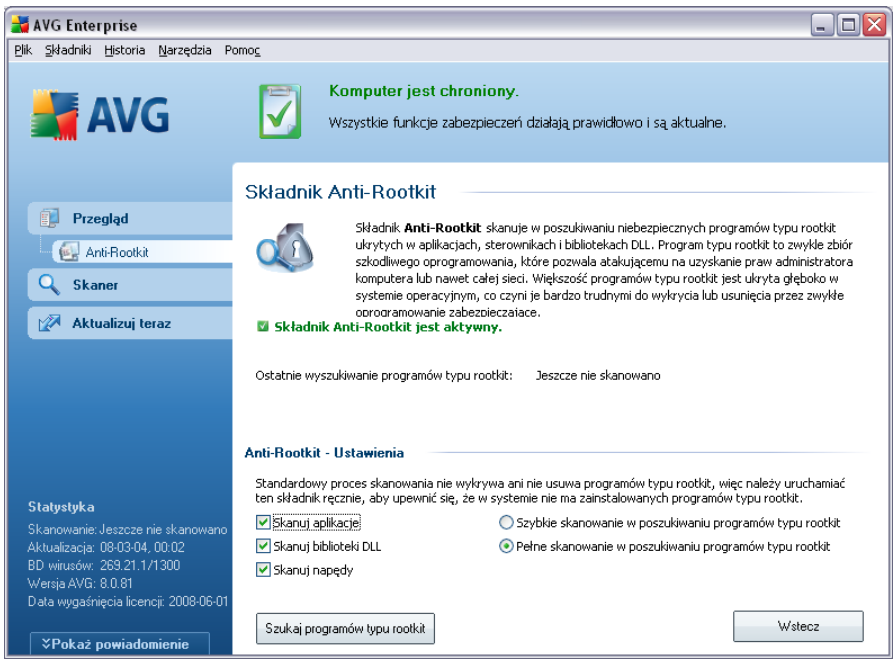
10.3.Anti-Rootkit

10.3.1.Zasady dzialania skladnika Anti-Rootkit

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.

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.

10.3.2.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 napedy***

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 przyciski sterujace to:

- ***Szukaj programów typu rootkit*** — poniewaz to skanowanie 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.

10.4.Zapora

10.4.1.Zasady dzialania Zapory

Zapora internetowa to system, który wymusza stosowanie zasad kontroli dostepu miedzy dwoma lub wieksza liczba sieci, blokujac lub umozliwiajac przeplyw danych. Zapora sklada sie z zestawu regul, które steruja komunikacja na kazdym indywidualnym porcie sieciowym, chroniac w ten sposób siec lokalna przed atakami,

których zródlo znajduje sie na zewnatrz (zazwyczaj w internecie). Komunikacja jest oceniana (w oparciu o zdefiniowane reguly), a nastepnie akceptowana lub blokowana. Jesli zapora wykryje próbe ataku, blokuje ja i nie pozwala intruzowi przejac kontroli nad komputerem.

Konfiguracja Zapory pozwala blokowac lub dopuszczac komunikacje wewnetrzna lub zewnetrzna (zarówno wychodzaca, jak i przychodzaca) na konkretnych portach i dla zdefiniowanych programów. Zapora moze np. akceptowac tylko ruch WWW, z którego korzysta program Microsoft Internet Explorer. Próba transmisji danych WWW przez jakakolwiek inna przegladarke bedzie w takim przypadku blokowana.

Zapora chroni równiez Twoje dane osobowe - nikt nie uzyska ich z Twojego komputera bez wyraznej zgody. Decyduje tez o tym, jak wymieniane sa dane z innymi komputerami w sieci lokalnej lub internecie. Zapora w srodowisku komercyjnym chroni równiez pojedyncze komputery przed atakami przeprowadzanymi z wnetrza tej samej sieci.

Uwaga: *Zapora AVG nie jest przeznaczona do współpracy z serwerami!*

Jak dziala Zapora AVG

W systemie AVG ***Zapora*** kontroluje caly ruch na kazdym porcie sieciowym komputera. Na podstawie zdefiniowanych regul ***Zapora*** ocenia uruchomione aplikacje (chcace nawiazac polaczenie z siecia lokalna lub internetem) oraz programy usilujace z zewnatrz polaczyc sie z Twoim komputerem. ***Zapora*** dopuszcza lub blokuje komunikacje tych aplikacji na okreslonych portach sieciowych. Domyslnie, jesli aplikacja jest nieznana (tj. nie posiada zdefiniowanych regul ***Zapory***), wyswietlone bedzie pytanie, czy jej komunikacja ma zostac zaakceptowana.

Zapora potrafi:

- Automatycznie zablokowac lub zezwolic na komunikacje znanych aplikacji, albo poprosic uzytkownika o potwierdzenie
- Korzystac z kompletnych profili zawierajacych wstepnie zdefiniowane reguly (zgodnie z Twoimi potrzebami)
- Prowadzic archiwum wszystkich zdefiniowanych profili i ustawien
- Automatycznie przelaczac profile przy laczeniu sie z róznymi sieciami lub przy uzywaniu róznych kart sieciowych

10.4.2.Profile Zapory

Skladnik ***Zapora*** umozliwia definiowanie okreslonych regul bezpieczenstwa w oparciu o srodowisko i tryb pracy komputera. Kazda z opcji wymaga innego poziomu zabezpieczen, a dostosowywanie ich odbywa sie za pomoca odpowiednich profili. Krótko mówiac, ***profil Zapory*** to okreslona konfiguracja tego skladnika. Dostepna jest pewna liczba wstepnie zdefiniowanych profili.

Dostepne profile

- ***Odblokuj wszystko*** to systemowy profil Zapora, wstepnie skonfigurowany przez producenta; jest zawsze dostepny. Gdy profil ten jest aktywny, cala komunikacja sieciowa jest akceptowana, bez stosowania jakichkolwiek regul zabezpieczen - tak, jakby skladnik ***Zapora*** byl wylaczony *(tj. wszystkie programy moga wymieniac dane, ale pakiety wciaz obslugiwane sa przez sterownik filtra AVG - aby tego uniknac, calkowicie wylacz Zapore)*. Tego profilu systemowego nie mozna powielic ani usunac, a jego ustawien nie da sie modyfikowac.

- ***Blokuj wszystko*** to systemowy profil ***Zapory*** wstepnie skonfigurowany przez producenta; jest zawsze dostepny. Gdy zostanie on aktywowany, wszystkie próby komunikacji z siecia beda blokowane. Komputer nie bedzie ani dostepny z sieci zewnetrznej, ani nie bedzie mógl sie z nia polaczyc. Tego profilu systemowego nie mozna powielic ani usunac, a jego ustawien nie da sie modyfikowac.

- ***Wlasne profile*** - utworzone przy pomocy ***Kreatora konfiguracji Zapory***. Za pomoca kreatora mozna wygenerowac maksymalnie trzy wlasne profile:

    - *Pojedynczy komputer* — odpowiedni dla zwyklych komputerów domowych podlaczonych bezposrednio do Internetu.

    - *Komputer w domenie* — odpowiedni dla komputerów pracujacych w sieci lokalnej, np. w szkolach lub sieci firmowej. Zaklada sie, ze wspomniana siec chroniona jest przy uzyciu pewnych dodatkowych srodków, wiec poziom bezpieczenstwa moze byc nizszy niz dla pojedynczego komputera.

    - *Siec w domu lub malym biurze* — odpowiedni dla komputerów w mniejszej sieci, np. w domu lub w malej firmie (zazwyczaj tylko kilka komputerów polaczonych ze soba, bez „centralnego” administratora).

    - *Komputer przenosny* — odpowiedni dla notebooków. Zaklada sie, ze

komputer uzywany w podróży laczy sie z internetem przy wykorzystaniu róznych nieznanych zródel, a wiec takze w miejscach niezabezpieczonych (kawiarnia internetowa, pokój hotelowy itp.),. Profil ten zapewnia najwyzszy poziom bezpieczenstwa.

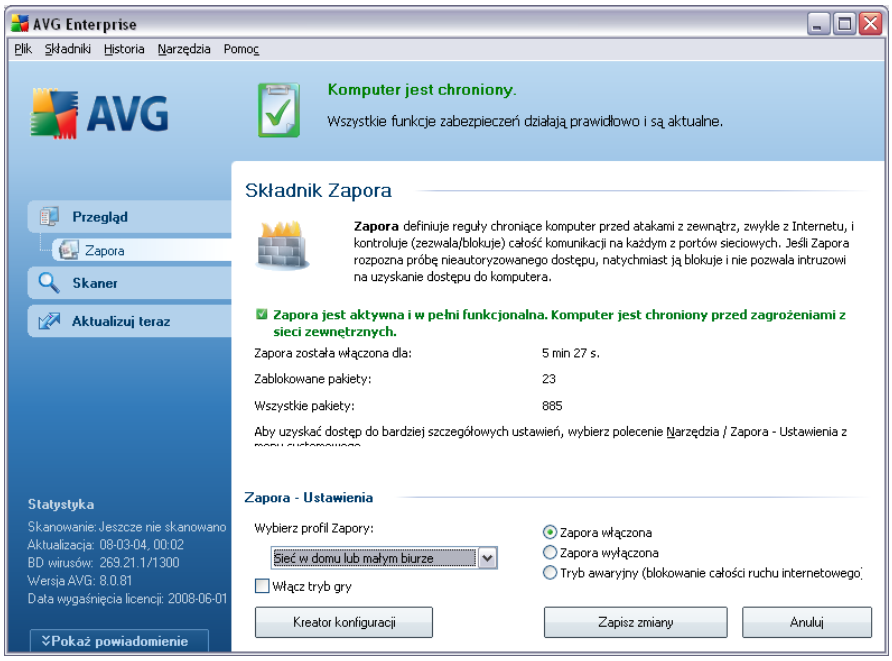
Przelaczanie profili

Funkcja przelaczania profili umozliwia skladnikowi ***Zapora*** automatyczne przelaczenie sie na zdefiniowany wczesniej profil w przypadku uzycia okreslonej karty sieciowej lub polaczenia z okreslonym typem sieci. Jesli do obszaru sieciowego nie zostal jeszcze przypisany zaden profil, przy najblizszym polaczeniu z tym obszarem ***Zapora*** wyswietli okno dialogowe z prosba o przypisanie profilu.

Profile mozna tworzyc dla dowolnych interfejsów sieciowych lub obszarów. Ich dalsze ustawienia dostepne sa w oknie ***Profile kart sieciowych i obszarów***, w którym mozna równiez w razie potrzeby wylaczyc te funkcje (*w takim przypadku dla kazdego rodzaju polaczenia bedzie uzywany profil domyslny*).

Zazwyczaj funkcja ta bedzie przydatna dla uzytkowników korzystajacych z notebooka i róznych typów polaczen. W przypadku komputera stacjonarnego korzystajacego tylko z jednego typu polaczenia (*tj. kablowego polaczenia z internetem*) funkcja przelaczania profili prawdopodobnie nigdy nie bedzie uzywana.

10.4.3.Interfejs Zapory



Interfejs skladnika ***Zapora*** udostepnia niektóre podstawowe informacje na temat funkcji oraz krótkie omówienie statystyk ***Zapory***:

- ***Zapora jest aktywna od*** — czas, jaki uplynal od jej ostatniego uruchomienia.
- ***Zablokowane pakiety*** — liczba zablokowanych pakietów (ze wszystkich sprawdzonych).
- ***Wszystkie pakiety*** — liczba wszystkich pakietów sprawdzonych przez Zapore.

Ustawienia ZaporySekcja

- ***Wybierz profil Zapory*** — z menu rozwijanego wybierz jeden ze zdefiniowanych profili — dwa profile sa dostepne przez caly czas (*domyslny profil o nazwie* ***Odblokuj wszystko*** *oraz* ***Blokuj wszystko***). Inne profile byly dodane podczas dzialania ***Kreatora konfiguracji Zapory*** lub w wyniku edycji profili w oknie ***Profile*** (w ***ustawieniach Zapory***.
- Stan Zapory:

- ***Zapora wlaczona*** — nalezy zaznaczyc te opcje, aby zezwalac na komunikacje wszystkim aplikacjom, którym w zbiorze regul zdefiniowanych dla wybranego profilu ***Zapory*** przypisano akcje „pozwól”.

- ***Zapora wylaczona*** — ta opcja calkowicie wylacza ***Zapore***. Ruch sieciowy nie bedzie blokowany ani monitorowany!

- ***Tryb awaryjny (blokowanie calosci ruchu internetowego)*** — nalezy zaznaczyc te opcje, aby blokowac caly ruch na wszystkich portach. ***Zapora*** wciaz dziala, lecz komunikacja z siecia jest zablokowana.

- ***Wlacz tryb gry*** — Zaznaczenie tego pola daje pewnosc, ze podczas dzialania aplikacji pelnoekranowych (gier, prezentacji programu PowerPoint itp.), ***Zapora AVG*** nie bedzie wyswietlala okien dialogowych z pytaniami, czy komunikacja dla nieznanej aplikacji ma zostac odblokowana. Jesli w tym czasie nowa aplikacja spróbuje polaczyc sie z siecia, ***Zapora*** automatycznie odblokuje lub zablokuje te próbe (zgodnie z ustawieniami biezacego profilu).

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 Zapory AVG, nalezy wybrac z menu glównego* ***Plik / Ustawienia Zapory*** *i skorzystac z interfejsu* ***Ustawienia Zapory****.*

Dostepne przyciski sterujace to:

- ***Kreator konfiguracji*** — kliknij ten przycisk, jezeli chcesz uruchomic ***Kreator konfiguracji Zapory, który przeprowadzi Cie przez proces automatycznej konfiguracji Zapory***.

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.

- ***Anuluj*** — kliknięcie tego przycisku powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (*przegladu skladników*).

10.5.Skaner poczty e-mail

10.5.1.Zasady dzialania Skanera poczty e-mail

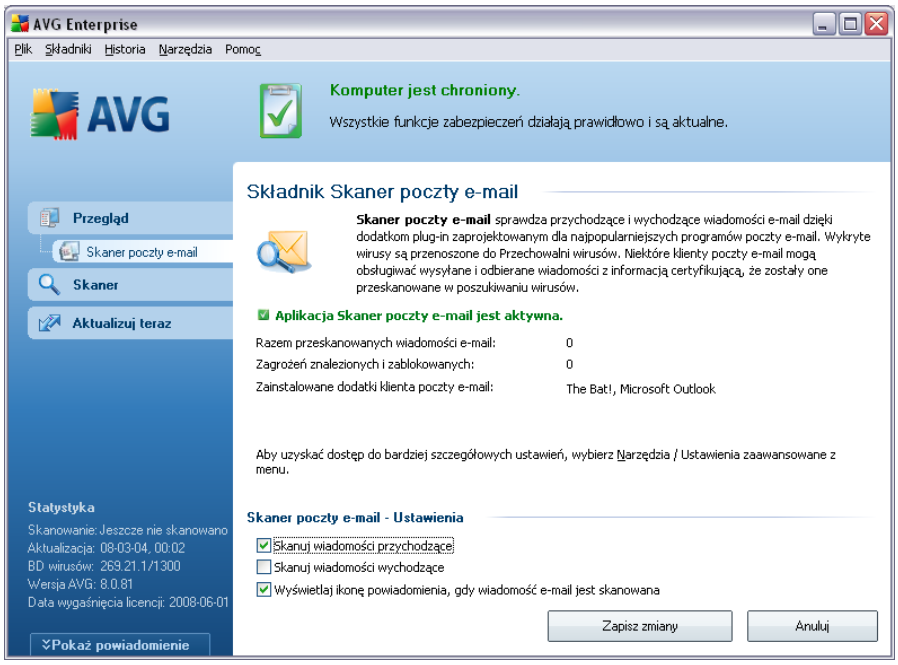
Poczta e-mail to od dawna czeste zródlo wirusów i koni trojanskich. Wyludzenia danych i spam powoduja, ze stala sie ona jeszcze wiekszym zagrozeniem. Darmowe konta pocztowe sa szczególnie narazone na otrzymywanie niepozadanych wiadomosci, gdyz ich operatorzy rzadko korzystaja z technologii antyspamowych. Niestety, uzytkownicy domowi najczesciej uzywaja takich wlasnie kont. Dodatkowo odwiedzaja oni nieznane witryny i wpisuja w formularzach dane osobowe (takie jak adres e-mail), co powoduje, ze w jeszcze wiekszym stopniu narazaja sie na ataki za posrednictwem poczty e-mail. Firmy uzywaja na ogól komercyjnych kont pocztowych, które w celu ograniczenia ryzyka korzystaja z filtrów antyspamowych i innych srodków bezpieczenstwa.

Skaner poczty e-mail obecny w pakiecie AVG sprawdza wszystkie wysylane i odbierane wiadomosci, zapewniajac ochrone przed zagrozeniami rozprzestrzenianymi ta metoda. Program AVG obsluguje wszystkie najpopularniejsze programy pocztowe, w tym: MS Outlook, The bat! i Eudora, a takze wszystkie inne aplikacje korzystajace z protokolu SMTP/POP3, takie jak Outlook Express. Obslugiwane sa takze polaczenia szyfrowane za pomoca protokolu SSL.

Uwaga: *Skaner poczty e-mail nie jest przeznaczony do współpracy z serwerami!*

Wykryte wirusy sa natychmiast poddawane kwarantannie w ***Przechowalni wirusów***. Niektóre programy zarzadzajace poczta e-mail moga obslugiwac certyfikacje wiadomosci (zalaczanie informacji, ze dany e-mail zostal wraz z zalacznikami sprawdzony pod katem obecnosci wirusów).

10.5.2.Interfejs Skanera poczty e-mail



Interfejs skladnika ***Skaner poczty e-mail*** zawiera krótki opis jego funkcji, informacje o stanie (Skladnik *Skaner poczty e-mail jest aktywny.*) oraz nastepujace statystyki:

- ***Razem przeskanowanych wiadomosci e-mail*** — liczba wiadomosci przeskanowanych od czasu ostatniego uruchomienia ***Skanera poczty e-mail*** (*w razie potrzeby, np. dla celów statystycznych, wartosc te mozna wyzerowac*)
- ***Zagrozen znalezionych i zablokowanych*** — liczba zainfekowanych wiadomosci wykrytych od czasu ostatniego uruchomienia ***Skanera poczty e-mail***.
- ***Zainstalowany plugin poczty e-mail*** — informacje o pluginie odpowiednim dla Twojego domyslnego klienta poczty

Podstawowa konfiguracja skladnika

W dolnej czesci okna znajduje sie sekcja ***Skaner poczty e-mail - Ustawienia*** , w której mozna skonfigurowac podstawowe funkcje skladnika:

- ***Skanuj wiadomosci przychodzace*** — zaznaczenie tej opcji pozwala

okreslic, czy powinny byc skanowane wszystkie wiadomosci e-mail dostarczane na konto pocztowe (*opcja ta jest domyslnie wlaczona, nie zaleca sie jej wylaczania!*).

- ***Skanuj wiadomosci wychodzace*** — zaznaczenie tej opcji pozwala okreslic, czy powinny byc skanowane wszystkie wiadomosci e-mail wysylane z konta pocztowego (*opcja ta jest domyslnie wylaczona*)

- ***Wyswietlaj powiadomienie podczas skanowania wiadomosci*** — pozwala okreslic, czy ***Skaner poczty e-mail*** ma podczas swojej pracy wyswietlac powiadomienie o aktualnie wykonywanym zadaniu (*laczenie z serwerem, pobieranie wiadomosci, skanowanie wiadomosci itd., ...*)

Dostep do zaawansowanej konfiguracji skladnika ***Skaner poczty e-mail*** mozna uzyskac z poziomu menu ***Narzedzia / Ustawienia zaawansowane***. Wszelkie zmiany w konfiguracji powinny byc wprowadzane wylacznie przez doswiadczonych uzytkowników.

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 Zaawansowane ustawienia AVG.*

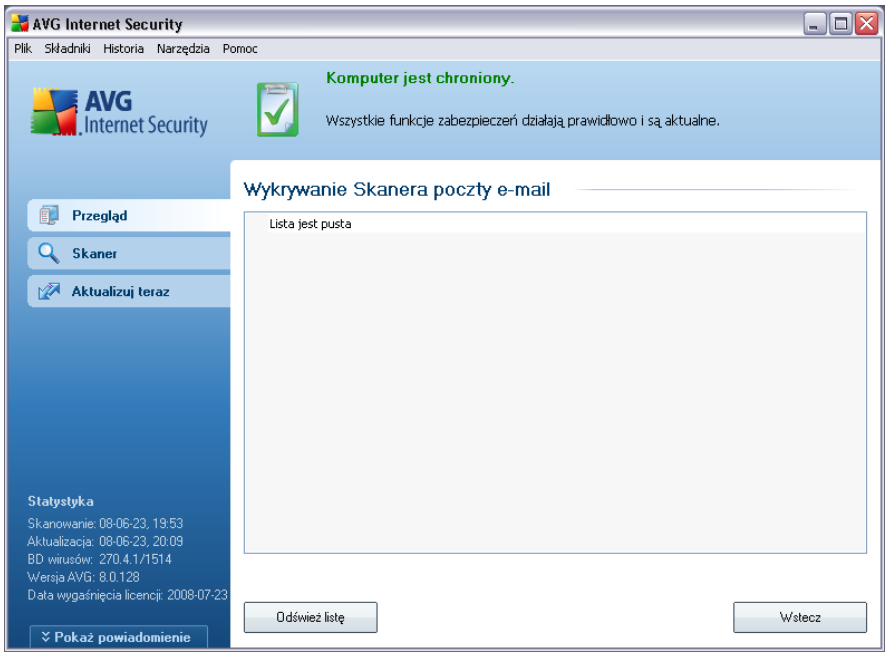
Przyciski kontrolne

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

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.

- ***Anuluj*** — kliknięcie tego przycisku powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (przegladu skladników).

10.5.3.Zagrozenia wykryte przez Skaner poczty e-mail

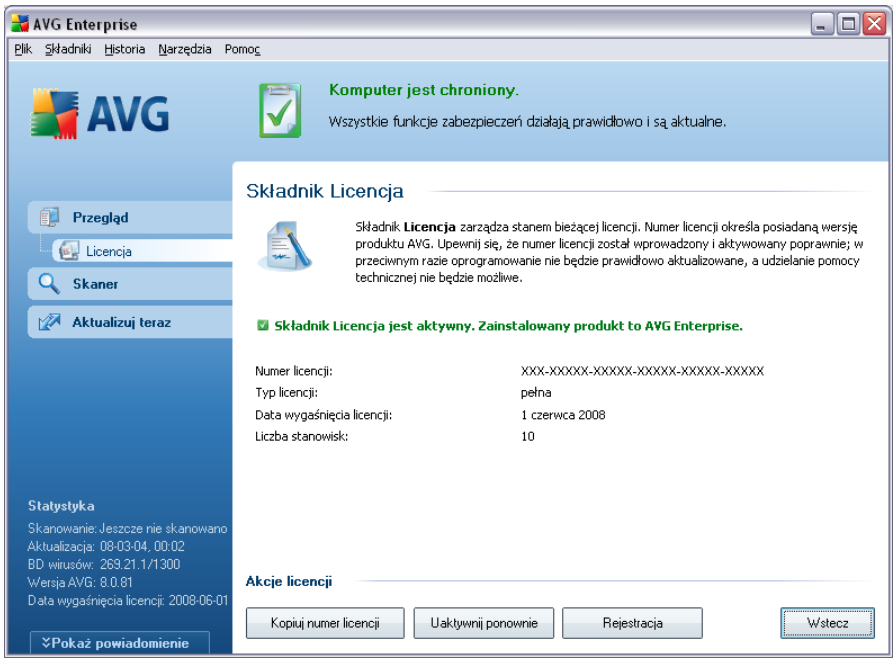


W oknie ***Zagrozenia wykryte przez Skaner poczty e-mail*** (*dostepnym poprzez menu Historia*) wyswietlana jest lista wszystkich obiektów znalezionych przez skladnik ***Skaner poczty e-mail*** . Podawane sa tam nastepujace informacje:

- ***Infekcja***— opis (ewentualnie nazwa) wykrytego zagrozenia.
- ***Obiekt*** — lokalizacja obiektu.
- ***Wynik*** — dzialanie podjete w zwiazku z wykryciem.
- ***Typ obiektu*** — typ wykrytego obiektu.

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***).

10.6.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. Dla wygody uzytkownika u dolu okna ***Licencja*** znajduje sie przycisk ***Kopiuj numer licencji***; kliknięcie go pozwala skopiowac numer licencji do schowka, aby nastepnie wkleic go w zadanym miejscu (***CTRL+V***).
- ***Typ licencji*** — edycja produktu zdefiniowana przez numer licencji.
- ***Data wygasniecia licencji*** — data okreslajace okres waznosci licencji. Aby korzystac z systemu AVG po tej dacie, nalezy odnowic licencje. Licencje mozna odnowic online, za posrednictwem witryny firmy AVG.
- ***Liczba stanowisk*** — liczba stacji roboczych, na których mozna zainstalowac system AVG.

Przyciski kontrolne

- ***Kopiuj numer licencji*** — kliknij ten przycisk, aby skopiowac numer aktualnie uzywanej licencji do Schowka (*tak jak w wypadku uzycia klawiszy CTRL+C*), skad wkleisz go do dowolnego pola tekstowego.

- ***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*).

- ***Zarejestruj*** — powoduje polaczenie z witryna rejestracyjna www.avg.com. Nalezy tam podac swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysluguje bezplatna pomoc techniczna.

- ***Wstecz*** — kliknięcie tego przycisku powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (przegladu skladników).

10.7.LinkScanner

10.7.1.Zasady dzialania technologii LinkScanner

LinkScanner współpracuje z programami Internet Explorer i Firefox (*wersja 1.5 oraz nowsze*), oferujac dwie funkcje: ***AVG Active Surf-Shield*** i ***AVG Search Shield***.

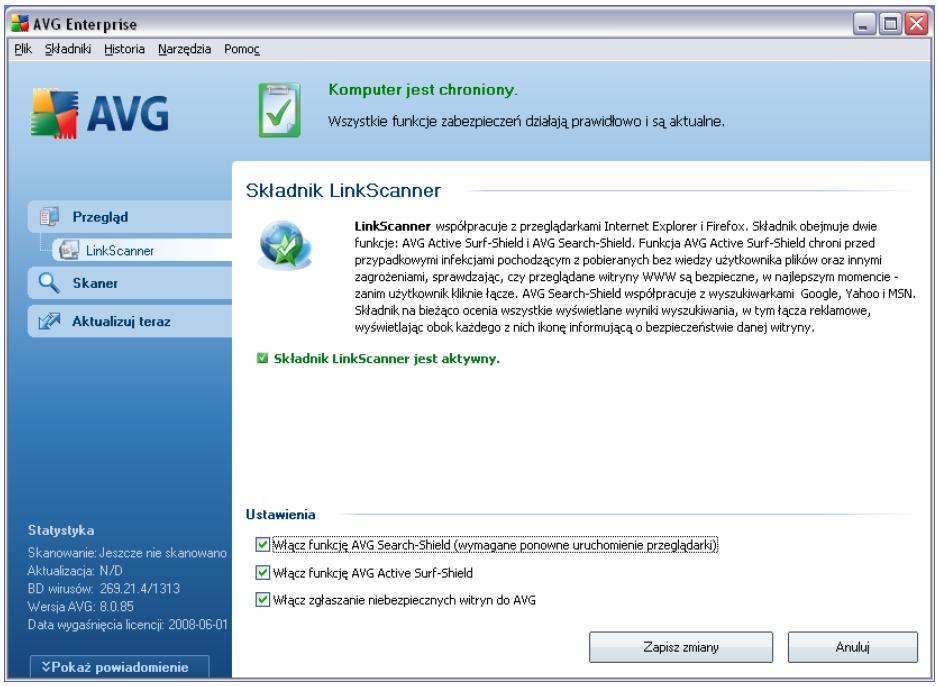
Funkcja AVG Active Surf-Shield chroni przed przypadkowymi infekcjami pochodzacym z pobieranych bez wiedzy uzytkownika plików, oraz innymi zagrozeniami. Sprawdza takze, czy przegladane witryny WWW sa bezpieczne, skanujac je w najodpowiedniejszym momencie - zanim uzytkownik kliknie link.

AVG Search Shield współpracuje z wyszukiwarkami Google, Yahoo! i MSN. Na biezaco ocenia wszystkie wyniki wyszukiwania (w tym linki sponsorowane), wyswietlajac obok kazdego z nich ikone informujaca o bezpieczenstwie danej witryny.

Uwaga: *Technologia AVG LinkScanner nie jest przeznaczona dla platform serwerowych!*

10.7.2.Interfejs LinkScanner

Skladnik ***LinkScanner*** sklada sie z dwóch funkcji, które mozna wlaczyc lub wylaczyc w jego interfejsie :



- ***Wlacz funkcje AVG Search-Shield*** — (*domyslnie wlaczona*): Skanuje wszystkie linki pojawiajace sie w wynikach wyszukiwania serwisów Google, Yahoo! oraz MSN, a nastepnie obok kazdego z nich wyswietla klasyfikacje bezpieczenstwa. Obslugiwane przegladarki to Internet Explorer i Mozilla Firefox.

- ***Wlacz funkcje AVG Active Surf-Shield*** — (*domyslnie wlaczona*): aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (*w czasie rzeczywistym*). Znane zlosliwe witryny i ich niebezpieczna zawartosc blokowane sa juz w momencie otwarcia ich przez uzytkownika za pomoca przegladarki (*lub jakiejkolwiek innej aplikacji korzystajacej z protokolu HTTP*).

- ***Wlacz zglaszanie niebezpiecznych witryn do AVG*** — Zaznacz to pole, aby wlaczyc raportowanie niebezpiecznych witryn znalezionych przy uzyciu funkcji ***Active Surf-Shield*** lub ***Search-Shield*** w celu przekazania ich do bazy danych pomagajacej chronic uzytkowników AVG.

10.7.3.AVG Search-Shield

Podczas wyszukiwania w Internecie funkcja z wlaczona funkcja ***Ochrona wyszukiwania systemu AVG*** wszystkie wyniki najbardziej popularnych wyszukiwarek internetowych, np. Yahoo!, Google, MSN itd., sa oceniane pod katem obecnosci niebezpiecznej lub podejrzanej zawartosci. Sprawdzajac te lacza i oznaczajac niebezpieczne, ***pasek narzedzi zabezpieczen systemu AVG*** ostrzega przed przejsciem na niebezpieczna lub podejrzana strone. W ten sposób mozna poruszac sie tylko po bezpiecznych witrynach WWW.

Obok ocenianego aktualnie wyniku wyszukiwania wyswietlany jest symbol informujacy o trwajacym sprawdzaniu lacza. Po zakonczeniu sprawdzania wyswietlana jest ikona informujaca o jego wynikach:

 Strona, do której prowadzi lacze, jest bezpieczna (*w wyszukiwarce Yahoo! ta ikona nie jest wyswietlana na pasku narzedzi zabezpieczen systemu AVG!*).

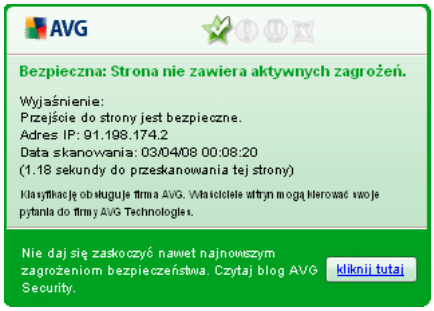
 Strona, do której prowadzi lacze, nie zawiera zagrozen, ale jest podejrzana (*watpliwosci budzi jej pochodzenie lub przeznaczenie, wiec nie zaleca sie dokonywania na niej zakupów itp.*).

 Strona, do której prowadzi lacze, jest bezpieczna, ale zawiera lacza do potencjalnie niebezpiecznych stron lub podejrzany kod (który jednak nie stanowi bezposredniego zagrozenia).

 Strona, do której prowadzi link, zawiera aktywne zagrozenia! Dla bezpieczenstwa uzytkownika dostep do tej strony zostanie zablokowany.

 Strona, do której prowadzi lacze, nie jest dostepna i nie udalo sie jej przeskanowac.

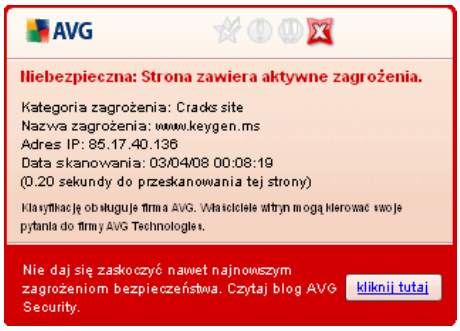
Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyswietlenie szczegółowych informacji o danym laczu. Informacje te obejmuja dodatkowe szczegóły dotyczace zagrozenia (jesli sa dostepne), adres IP lacza oraz czas przeskanowania strony przez AVG:



10.7.4.AVG Active Surf-Shield

Ta zaawansowana funkcja ochrony blokuje szkodliwa zawartosc dowolnej otwieranej witryny internetowej, zapobiegajac pobraniu jej na komputer. Gdy funkcja jest wlaczona, klikniecie lacza lub wpisanie adresu URL prowadzacego do niebezpiecznej witryny powoduje automatycznie zablokowanie otwarcia tej witryny, dzieki czemu komputer nie zostanie nieswiadomie zainfekowany. Nalezy pamietac, ze juz wyswietlenie niebezpiecznej witryny internetowej moze zainfekowac komputer. Dlatego gdy strona zostanie zawierajaca kod wykorzystujacy luki zabezpieczen lub inne powazne zagrozenia zostanie wywolana, ***pasek narzedzi zabezpieczen systemu AVG*** nie pozwoli na jej wyswietlenia w przegladarce.

Jesli uzytkownik trafi na szkodliwa strone internetowa, ***pasek narzedzi zabezpieczen systemu AVG*** wyswietli w przegladarce ostrzezenie podobne do tego:



Aby mimo wszystko przejsc do zainfekowanej strony, mozna kliknac lacze wyswietlane na ekranie, ***ale nie jest to zalecane!***

10.8.Ochrona sieci WWW

10.8.1.Zasady dzialania skladnika Ochrona sieci WWW

Ochrona sieci WWW to rodzaj programu rezydentnego, zapewniajacego ochrone w czasie rzeczywistym. Skanuje on zawartosc odwiedzanych stron internetowych (oraz znajdujacych sie na nich plików) jeszcze zanim zostana wyswietlone w przegladarce lub pobrane na dysk twardy.

Ochrona sieci WWW wykrywa strony zawierajace niebezpieczny kod javascript i blokuje ich ladowanie. Ponadto, identyfikuje szkodliwe oprogramowanie zawarte na stronach WWW i w razie podejrzen zatrzymuje pobieranie, aby nie dopuscic do infekcji komputera.

Uwaga: *Ochrona sieci WWW nie jest przeznaczona dla platform serwerowych!*

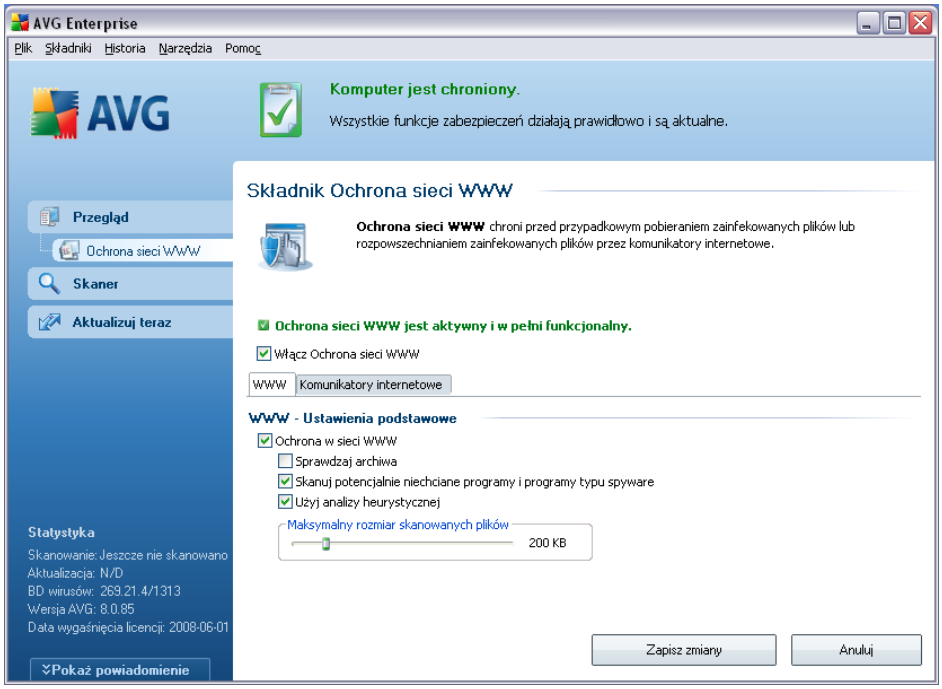
10.8.2.Interfejs skladnika Ochrona sieci WWW

Interfejs skladnika ***Ochrona sieci WWW*** opisuje dzialanie tego rodzaju ochrony. Znajduja sie tam informacje na temat biezacego stanu (*Skladnik Ochrona sieci WWW jest aktywny i w pelni funkcjonalny.*). W dolnej czesci okna widoczne sa podstawowe opcje Ochrony sieci WWW.

Podstawowa konfiguracja skladnika

Najistotniejsza opcja umozliwia natychmiastowe wlaczenie lub wylaczenie skladnika ***Ochrona sieci WWW*** (pole ***Wlacz Ochrone sieci WWW***). Pole to jest domyslnie zaznaczone, a skladnik ***Ochrona sieci WWW*** aktywny. Jednak jesli nie istnieja wazne powody do zmiany tego ustawienia, zaleca sie pozostawienie skladnika aktywnego. Jesli to pole jest zaznaczone (skladnik ***Ochrona sieci WWW*** dziala), na dwóch kolejnych kartach znajduja sie dalsze opcje konfiguracji.

- ***WWW*** — karta odpowiadajaca za skanowanie zawartosci witryny internetowych. Interfejs pozwala modyfikowac nastepujace ustawienia:

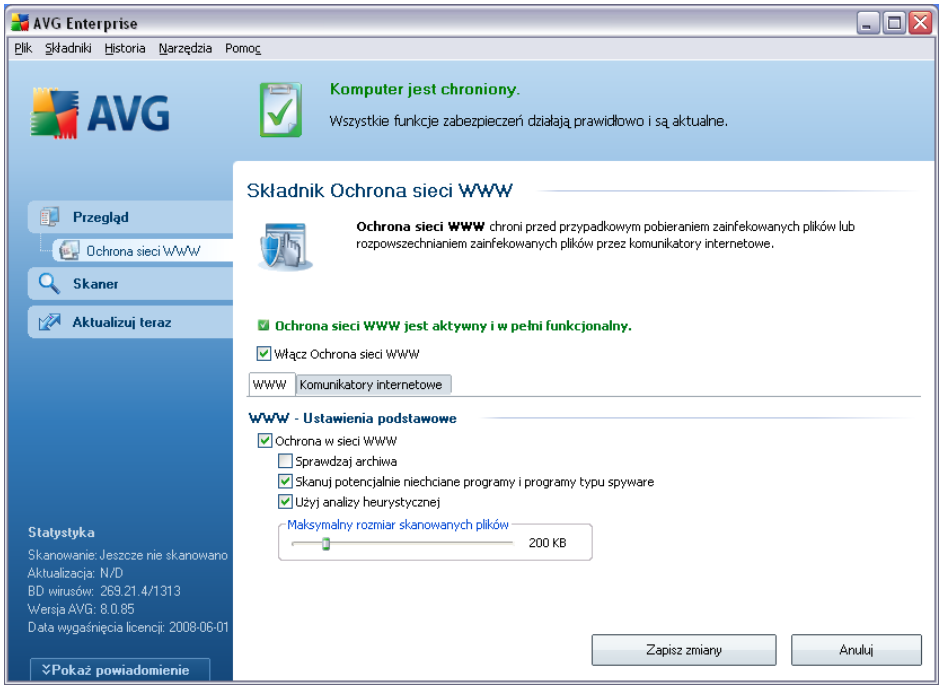


o ***Ochrona w sieci WWW*** — potwierdza, ze skladnik ***Ochrona sieci WWW*** ma skanowac zawartosc stron internetowych. Jesli ta opcja jest aktywna (*domyslnie*), mozna wlaczyc lub wylaczyc nastepujace funkcje:

- ***Skanuj wewnatrz archiwów*** — skanowanie ma obejmowac takze archiwa dostepne na odwiedzanych stronach WWW.
- ***Skanuj potencjalnie niechciane programy*** — skanowanie ma obejmowac potencjalnie niechciane programy (*pliki wykonywalne, które moga byc programami szpiegujacymi lub reklamowymi*) obecne na wyswietlanych stronach WWW.
- ***Uzyj analizy heurystycznej*** — skanowanie zawartosci wyswietlanych stron ma wykorzystywac metody analizy heurystycznej *(dynamiczna emulacje kodu skanowanego obiektu w srodowisku maszyny wirtualnej) — zobacz rozdzial Zasady dzialania skladnika Anti-Virus*).
- ***Maksymalny rozmiar skanowanych plików*** — jesli wyswietlana strona zawiera pliki, mozna skanowac ich zawartosc jeszcze przed pobraniem na twardy dysk. Poniewaz jednak skanowanie obszernych plików zajmuje dluzszy czas, otwieranie stron WWW moze zostac

znacznie spowolnione. Za pomoca tego suwaka mozna okreslic maksymalny rozmiar plików, które maja byc skanowane przez skladnik ***Ochrona sieci WWW***. Nawet jesli pobierany plik jest wiekszy od wybranego limitu i nie zostanie przeskanowany przez ***Ochrone sieci WWW***, nie zmniejsza to Twojego bezpieczenstwa: jesli plik jest zainfekowany, skladnik ***Ochrona rezydentna*** natychmiast to wykryje.

- ***Komunikatory internetowe*** — karta umozliwiajaca edycje ustawien monitorowania komunikatorów internetowych (*np. ICQ, MSN Messenger, Yahoo itp.*).



-

o Ochrona komunikatorów internetowych — zaznacz to pole, jesli chcesz, aby Ochrona sieci WWW zapewniala bezpieczenstwo komunikacji online. O ile opcja ta jest zaznaczona, mozna dodatkowo okreslic, które komunikatory internetowe maja byc kontrolowane — aktualnie program AVG**AVG 8.5 Anti-Virus plus Firewall** obsluguje aplikacje ICQ, MSN oraz Yahoo.

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.*

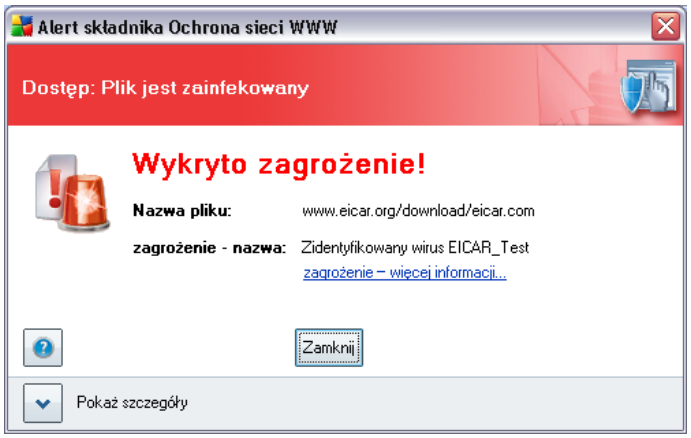
Dostepne przyciski

W interfejsie skladnika ***Ochrona sieci WWW*** dostepne sa nastepujace przyciski kontrolne:

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** — powoduje powrót do domyslnego okna Interfejsu uzytkownika AVG (*przegladu skladników*).

10.8.3.Zagrozenia wykryte przez Ochrone sieci WWW

Ochrona sieci WWW skanuje zawartosc odwiedzanych stron internetowych (oraz znajdujacych sie na nich plików) jeszcze zanim zostana wyswietlone w przegladarce lub pobrane na dysk twardy. Wykrycie jakiegokolwiek zagrozenia powoduje natychmiastowe wyswietlenie nastepujacego okna:



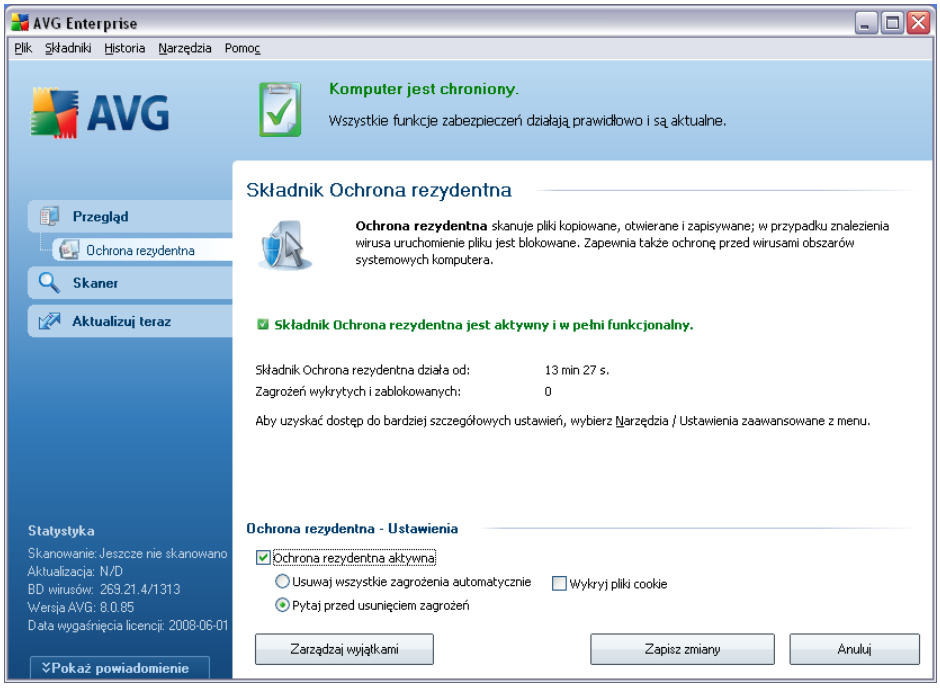
Podejrzana strona nie zostanie otwarta, a wykryty obiekt zostanie zapisany na liscie ***zagrozen wykrytych przez Ochrone sieci WWW*** (*dostepnej z menu Historia*).

10.9.Ochrona rezydentna

10.9.1.Zasady dzialania Ochrony rezydentnej

Skladnik ***Ochrona rezydentna*** sluzy do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Po wykryciu infekcji w pliku, do którego próbowano uzyskac dostep, ***Ochrona Rezydentna*** zatrzymuje wykonywana operacje i uniemozliwia uaktywnienie wirusa. Skladnik ***Ochrona Rezydentna***, ladowany do pamieci komputera podczas uruchamiania systemu, zapewnia podstawowa ochrone jego obszarów systemowych.

10.9.2.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 dziala od*** — okresla czas, jaki uplynal od ostatniego uruchomienia skladnika.

- ***Zagrozen wykrytych i zablokowanych*** — liczba wykrytych infekcji, do których uruchomienia nie dopuszczono (*w razie potrzeby, np. dla celów statystycznych, wartosc te mozna wyzerowac*)

Podstawowa konfiguracja skladnika

W dolnej czesci okna dialogowego znajduje sie sekcja o nazwie ***Ochrona rezydentna - Ustawienia*** , w której mozna edytowac niektóre podstawowe funkcje (*szczególowa 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. W protokole HTTP uzywane sa 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 glównego* ***Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

Dostepne przyciski

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

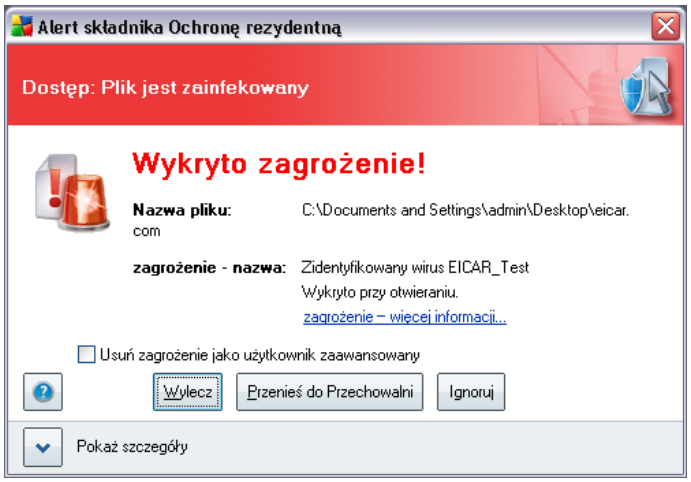
- ***Zarzadzaj wyjatkami*** - otwiera okno dialogowe ***Ochrona rezydentna — Wykluczone katalogi***, w którym mozna zdefiniowac foldery ignorowane przez skladnik ***Ochrona rezydentna***.

- ***Zapisz zmiany*** — kliknięcie tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.

- ***Anuluj*** — kliknięcie tego przycisku powoduje powrót do domyslnego okna ***Interfejsu uzytkownika AVG*** (przegladu skladników).

10.9.3.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:

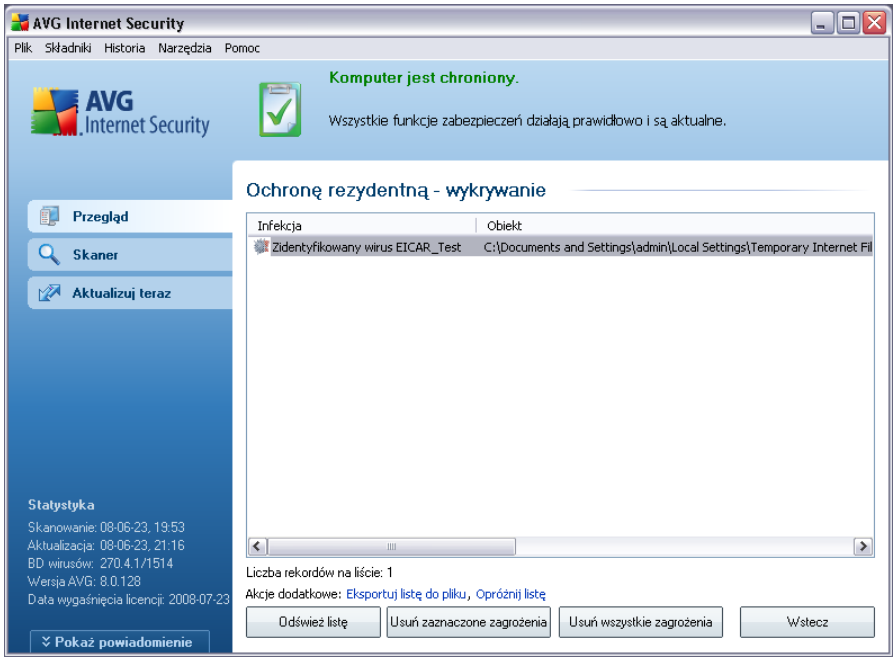


Okno to zawiera informacje dotyczace wykrytej infekcji i pozwala wybrac czynnosc, która ma zostac wykonana:

- ***Wylecz*** — jesli mozliwe jest wyleczenie pliku, system AVG zrobi to automatycznie (opcja zalecana).

- ***Przenies do Przechowalni*** — wirus zostanie przeniesiony do ***Przechowalni wirusów AVG***

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



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***). Dla kazdego wykrytego obiektu podawane sa nastepujace informacje:

- ***Infekcja***— opis (ewentualnie nazwa) wykrytego obiektu.
- ***Obiekt*** — lokalizacja obiektu.
- ***Wynik*** — dzialanie podjete w zwiazku z wykryciem.
- ***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***. Przycisk ***Wstecz*** przelacza z powrotem do domyslnego ***Interfejsu uzytkownika AVG*** (przegladu skladników).

10.1 Menedzer aktualizacji

10.10. Zasady dzialania Menedzera aktualizacji

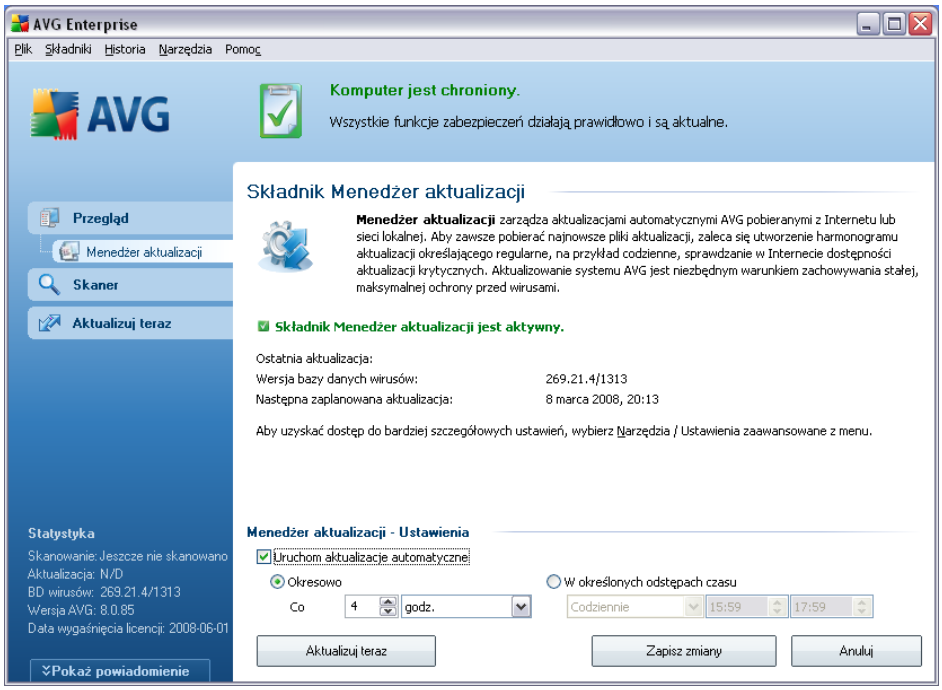
Zadne oprogramowanie zabezpieczajace nie moze zapewnic realnej ochrony przed róznymi typami zagrozen bez regularnych aktualizacji! Twórcy wirusów nieustannie szukaja nowych luk w programach i systemach operacyjnych, które mogliby wykorzystac. Nowe wirusy, szkodliwe oprogramowanie i metody ataków pojawiaja 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.*

10.10. 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.

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:

- o ***Okresowo*** — nalezy zdefiniowac interwal aktualizacji.
- o ***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 glównego* ***Narzedzia / Ustawienia zaawansowane*** *i skorzystac z interfejsu Zaawansowane ustawienia AVG.*

Przyciski kontrolne

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

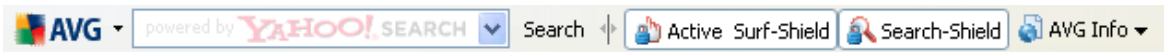
- ***Aktualizuj teraz*** — kliknieciе przycisku uruchamia natychmiastowa aktualizacje na zadanie.
- ***Zapisz zmiany*** — kliknieciе tego przycisku pozwala zapisac i zastosowac zmiany wprowadzone w biezacym oknie.
- ***Anuluj*** — kliknieciе tego przycisku powoduje powrót do domyslnego okna ***Interfejsu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

10.11. Pasek narzedzi AVG Security Toolbar

Pasek narzedzi AVG Security Toolbar jest zgodny z przegladarkami ***MS Internet Explorer*** (*wersja 6.0 lub nowsza*) i ***Mozilla Firefox*** (*wersja 1.5 lub nowsza*).

Uwaga: *AVG Security Toolbar nie jest przeznaczony dla platform serwerowych!*

Po zainstalowaniu ***pasek narzedzi AVG*** jest domyslnie wyswietlany pod paskiem adresu w oknie przegladarki:

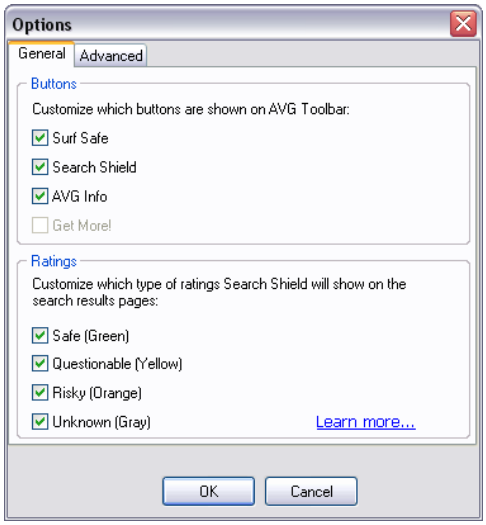


AVG Security Toolbar sklada sie z nastepujacych elementów:

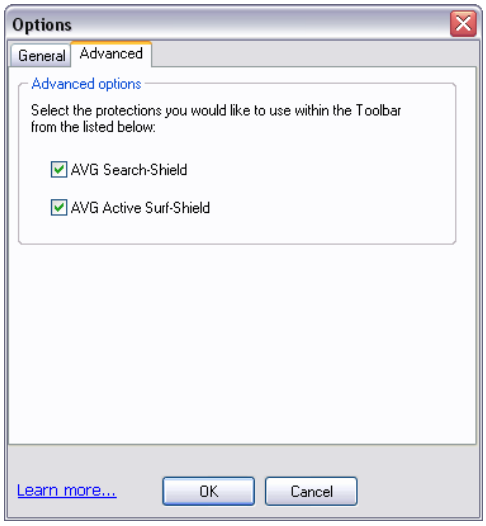
- ***Przycisk logo AVG*** — pozwala uzyskac dostep do glównych elementów paska narzedzi. Klikniecie go powoduje przejscie do witryny firmy AVG (www.avg.com). Kliknięcie strzalki obok ikony AVG powoduje otwarcie menu z nastepujacymi pozycjami:
  - ***Informacje o pasku narzedzi*** — lacze do strony glównej ***AVG Security Toolbar***, zawierajacej szczególowe informacje o dzialaniu paska.
  - ***Uruchom AVG 8.0*** — powoduje otwarcie Interfejsu uzytkownika systemu AVG 8.
  - ***Opcje*** — otwiera okno, w którym mozna dostosowac ustawienia ***Paska narzedzi AVG*** do swoich potrzeb. Okno to podzielone jest na dwie karty:
    - ***Ogólne*** — znajduja sie tu dwie sekcje: ***Przyciski*** i ***Klasyfikacja***.

      W sekcji ***Przyciski*** mozna okreslic, które przyciski maja byc widoczne (lub ukryte) na ***Pasku narzedzi AVG Security Toolbar***. Domyslnie wszystkie przyciski sa widoczne.

      W sekcji ***Klasyfikacja*** mozna zdefiniowac typy klasyfikacji dla wyników wyszukiwania. Domyslnie wyswietlane sa wszystkie klasyfikacje, ale mozna ukryc niektóre z nich (*w przypadku wyszukiwarki Yahoo! wyswietlane sa tylko wyniki uznane za calkowicie bezpieczne*).



➢ ***Zaawansowane*** — mozna edytowac tu ustawienia funkcji ochronnych ***AVG Security Toolbar***. Domyslne wlaczone sa obie funkcje: ***AVG Search-Shield*** i ***AVG Active Surf-Shield***.



o ***Aktualizacja*** — pozwala sprawdzic dostepnosc nowych aktualizacji ***dotyczacych Paska narzedzi AVG***

o ***Pomoc*** — pomaga znalezc odpowiednie pliki Pomocy, skontaktowac sie z ***Pomoca Techniczna AVG*** lub wyswietlic szczegóły dotyczace biezacej wersji AVG Security Toolbar.

- ***Yahoo! (pole wyszukiwarki)*** — proste i bezpieczne wyszukiwanie w sieci przy uzyciu wyszukiwarki Yahoo! Wprowadzajac wyraz lub fraze w tym polu i naciskajac przycisk ***Szukaj***, mozna rozpoczac wyszukiwanie przy uzyciu serwisu Yahoo! — niezaleznie od tego, jaka strona jest obecnie wyswietlana. Wspomniane pole zawiera takze historie poprzednich wyszukiwan. Wszystkie wyniki wyszukiwania zostana oczywiscie sprawdzone za pomoca funkcji ***AVG Search-Shield***.

- ***Przycisk AVG Active Surf-Shield*** — pozwala wlaczyc lub wylaczyc funkcje ***AVG Active Surf-Shield***.

- ***Przycisk AVG Search-Shield*** — przycisk pozwala wlaczyc lub wylaczyc funkcje ***AVG Search-Shield***.

- ***Przycisk Informacje o AVG*** — zawiera linki do waznych informacji na temat bezpieczenstwa, znajdujacych sie w witrynie firmy AVG (www.avg.com).

11. AVG Identity Protection

AVG Identity Protection jest samodzielnym skladnikiem, znanym poprzednio jako produkt Sana, który zostal wlaczony niedawno do pakietu **AVG 8.5 Anti-Virus plus Firewall**. Jest on integralna czescia instalacji AVG przeprowadzonej przy uzyciu odpowiedniego numeru licencji (*szczególowe informacje na temat wyboru odpowiedniego produktu oraz licencjonowania zawiera AVG Download Manager*).

Produkt AVG Identity Protection dostepny jest obecnie tylko w jezyku angielskim.

11.1.Zasady dzialania skladnika AVG Identity Protection

Oprogramowanie chroniace przed kradzieza tozsamosci

Technologia firmy Sana pochodzi ze znanego, behawioralnego systemu zabezpieczen Potrafi on w czasie rzeczywistym rozpoznawac zachowanie i charakter zlosliwego oprogramowania, dlatego tez moze na biezaco chronic komputery uzytkowników przed pojawiajacymi sie kazdego dnia zagrozeniami. Jak mawiaja specjalisci firmy Sana: "To natychmiastowa i stala ochrona".

11.2.Interfejs skladnika AVG Identity Protection

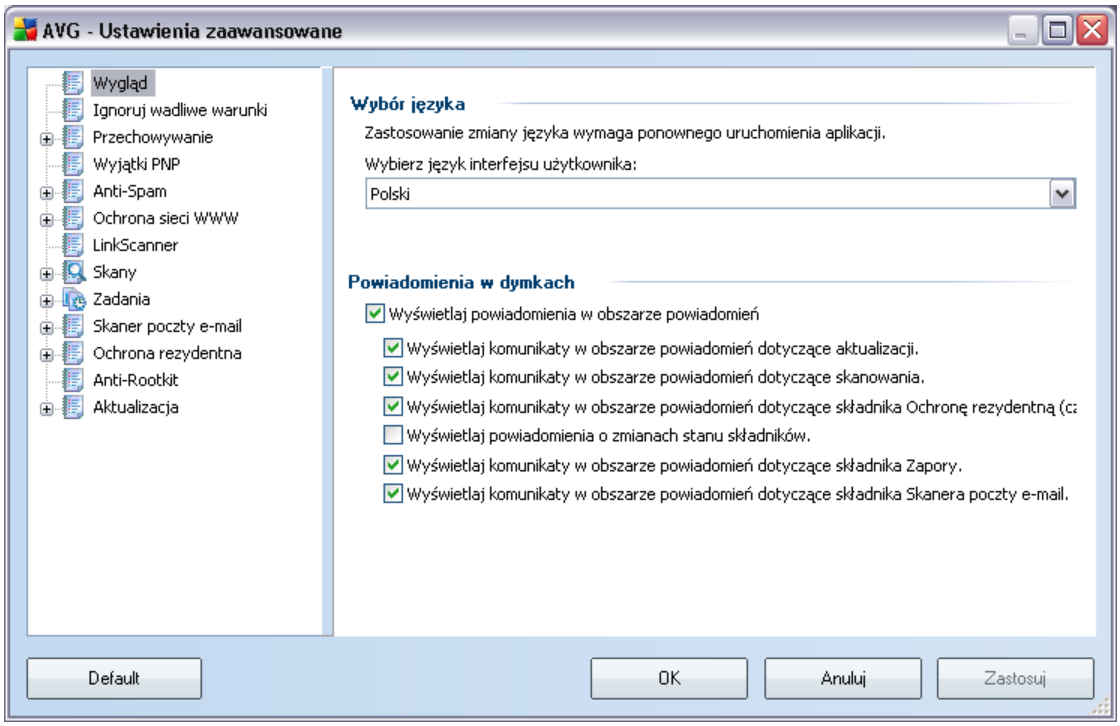
Wprowadz tekst tematu w tym miejscu.

12. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG 8.5 Anti-Virus plus Firewall** otwierane sa w nowym oknie (o nazwie ***Zaawansowane ustawienia AVG***). Okno to podzielone na dwa obszary: lewy zawiera drzewo nawigacyjne, a prawy — opcje konfiguracji programu. Wybranie skladnika, którego (*lub czesci którego*) konfiguracja ma zostac zmieniona, powoduje otwarcie okna dialogowego edycji z prawej strony.

12.1.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).
- Kliknij przycisk ***OK***, aby zamknac okno dialogowe ***Zaawansowane ustawienia AVG***.
- Zamknij interfejs uzytkownika AVG, wybierajac menu systemowego polecenie ***Plik/Zakoncz.***
- Otwórz ponownie Interfejs Uzytkownika AVG klikajac dwukrotnie ikone AVG na pasku zadan, klikajac dwukrotnie ikone AVG na pulpicie lub wybierajac menu ***Start/Wszystkie programy/AVG 8.0/Interfejs uzytkownika AVG*** (zobacz rozdzial ***Dostep do interfejsu uzytkownika***). Interfejs uzytkownika zostanie wyswietlony w nowo wybranym jezyku.

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 szczególowo 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 w obszarze powiadomien komunikaty dotyczace skanowania*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace automatycznego rozpoczecia, postepu i zakonczenia zaplanowanego skanowania;

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

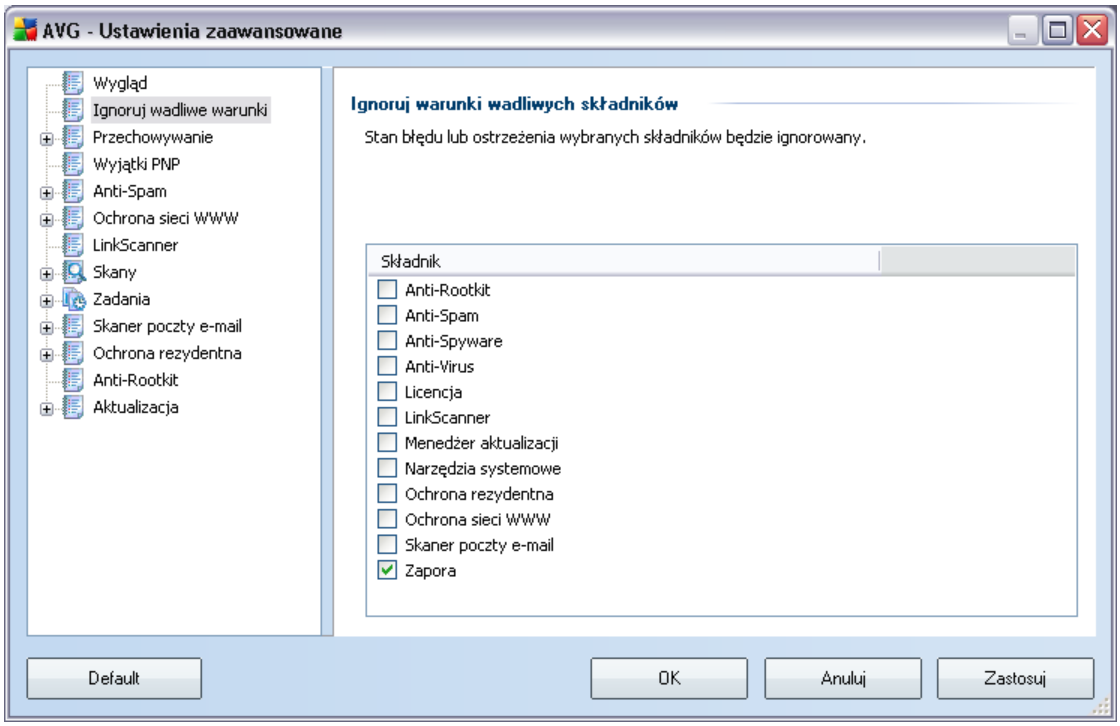
- ***Wyswietlaj powiadomienia o zmianach stanu skladników*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace aktywnosci lub nieaktywnosci skladników badz mozliwych problemów ich dotyczacych. W przypadku zglaszania stanu bledu skladnika opcja ta okresla funkcje informacyjna ikony na pasku zadan (zmiany koloru), która wskazuje na problemy z dowolnym skladnikiem systemu AVG.

- ***Wyswietlaj komunikaty w obszarze powiadomien dotyczace skladnika Firewall*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace stanu i procesów skladnika Firewall, na przyklad ostrzezenia o wlaczeniu/wylaczeniu skladnika, mozliwym blokowaniu ruchu sieciowego itp.;

- ***Wyswietlaj komunikaty w obszarze powiadomien dotyczace skladnika Skaner poczty e-mail*** — nalezy okreslic, czy maja byc wyswietlane informacje dotyczace skanowania wszystkich przychodzacych i wychodzacych wiadomosci e-mail.

12.2.Ignoruj bledny stan skladników

W oknie dialogowym ***Ignoruj wadliwe warunki 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:

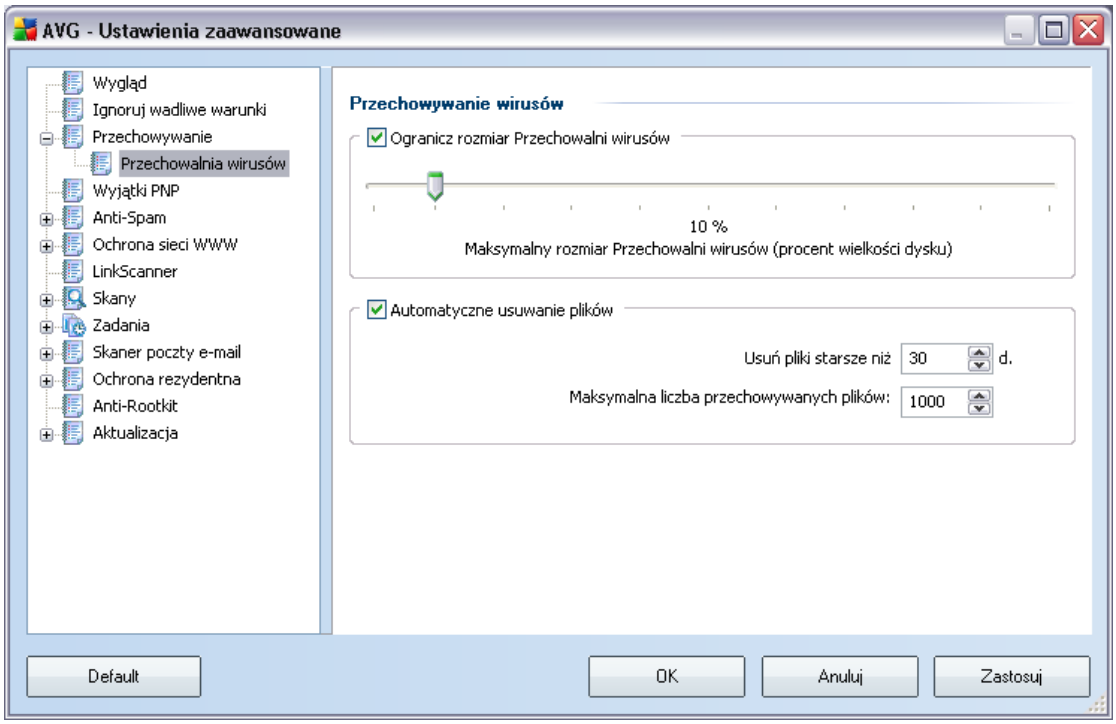
- ***ikona na pasku zadan*** — gdy wszystkie skladniki AVG dzialaja prawidlowo, wyswietlana ikona jest czterokolorowa; w przypadku bledu ikona jest wyszarzona i ma czerwony wykrzyknik,
- a opis tekstowy problemu jest widoczny w sekcji ***Informacje o stanie bezpieczenstwa*** okna glównego AVG

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 ikona jest

wyszarzona nie moze 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.

12.3.Przechowalnia wirusów



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

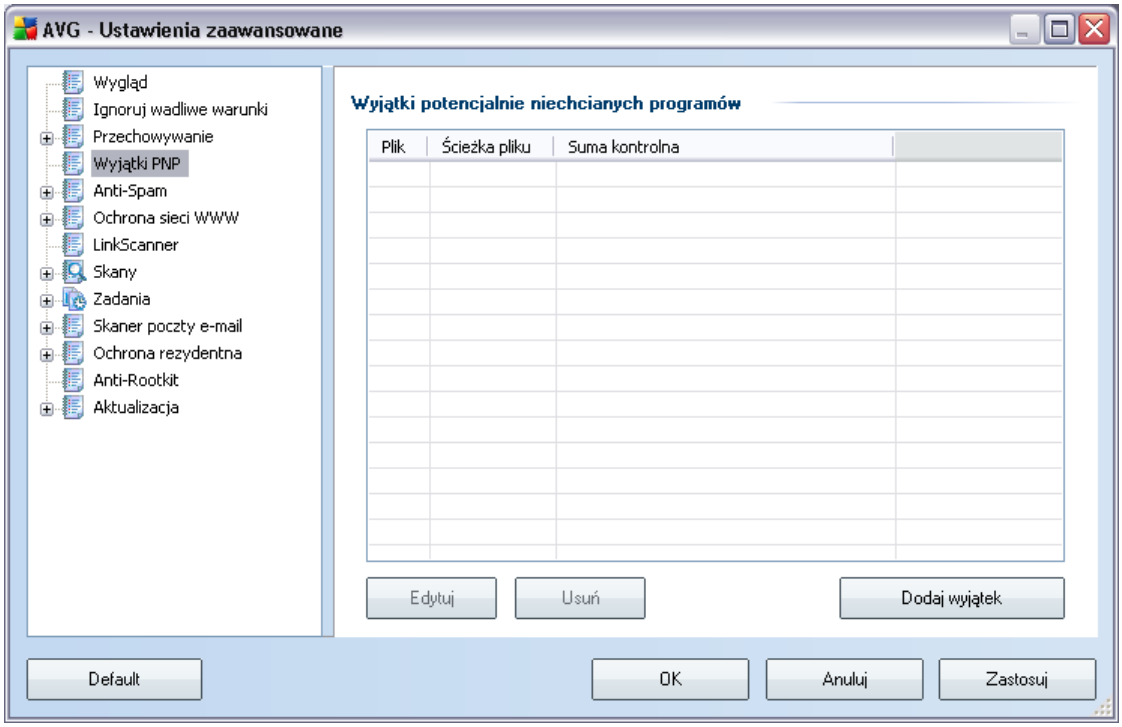
- ***Ogranicz rozmiar Przechowalni wirusów*** — za pomoca suwaka nalezy okreslic maksymalny rozmiar ***Przechowalni***. Rozmiar jest okreslany w stosunku do rozmiaru dysku lokalnego.

- ***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).

12.4.Wyjatki PNP

Oprogramowanie AVG potrafi analizowac i wykrywac pliki wykonywalne i biblioteki DLL, których obecnosc w systemie operacyjnym moze byc niepozadana. W niektórych przypadkach mozesz 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:



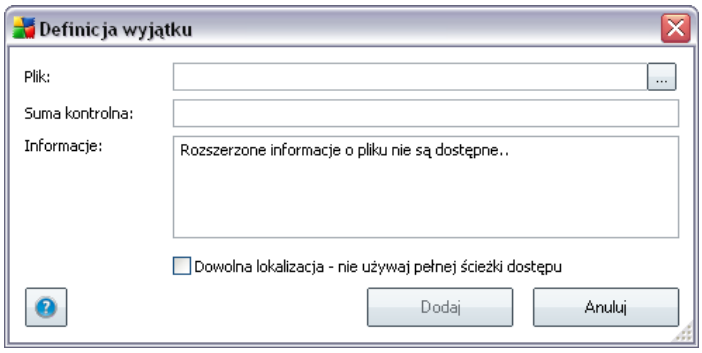
Okno ***Wyjatki potencjalnie niechcianych programów*** zawiera liste juz zdefiniowanych i aktualnie obowiazujacych wyjatków potencjalnie niechcianych programów. Wyjatki mozna edytowac, usuwac i dodawac.

Przyciski kontrolne

- ***Edytuj*** — otwiera okno edycji (*identyczne jako 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:



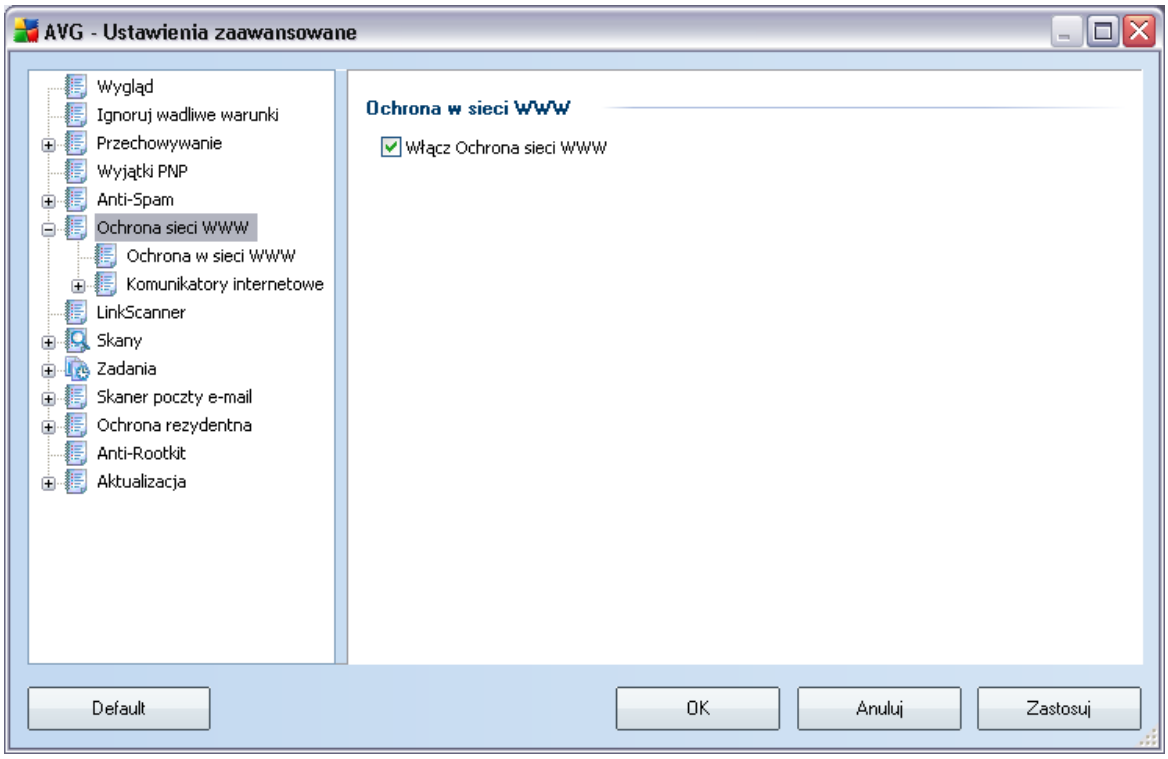
  - ***Plik*** — nalezy podac pelna sciezke do pliku, który ma byc oznaczony jako wyjatek.

  - ***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.

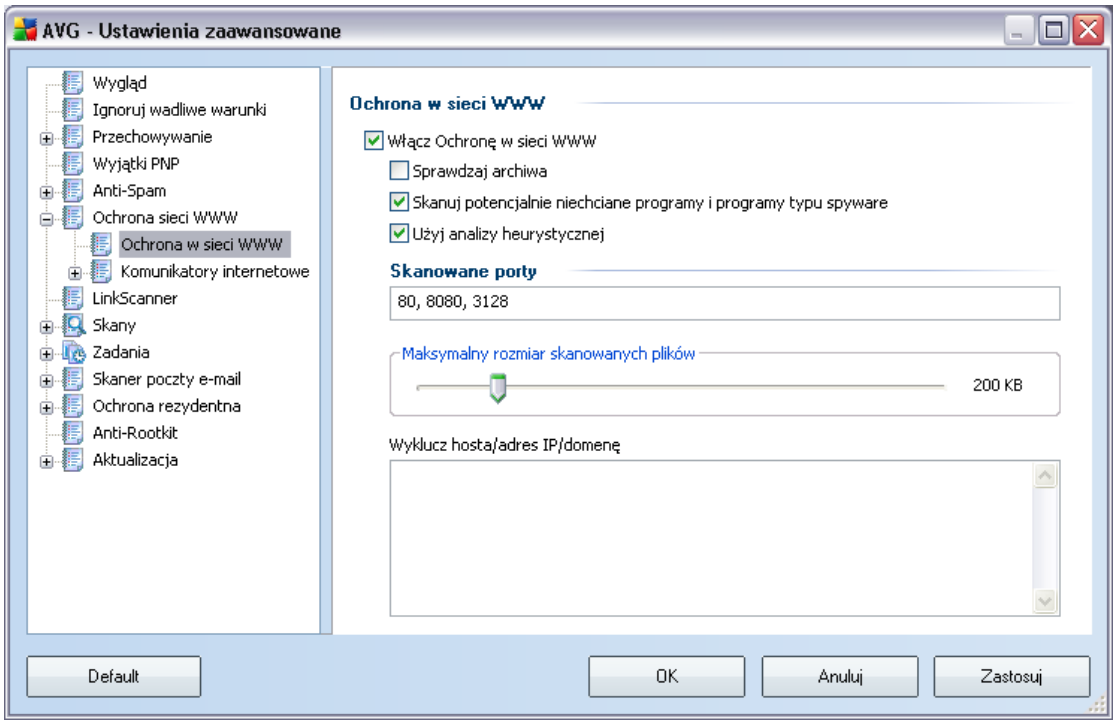
12.5.Ochrona sieci WWW



W oknie ***Ochrona sieci WWW*** mozna wlaczyc lub wylaczyc caly skladnik ***Ochrona sieci WWW*** (*domyslnie jest wlaczony*). Szczególowe ustawienia tego skladnika dostepne sa w kolejnych oknach dostepnych z poziomu drzewa opcji.

W dolnej czesci okna mozna wybrac sposób informowania o wykrytych zagrozeniach: za pomoca zwyklych okien dialogowych, powiadomien w dymkach lub ikony na pasku zadan.

12.5.1.Ochrona WWW



W oknie dialogowym ***Ochrona w sieci WWW*** mozna edytowac konfiguracje tego skladnika dotyczaca skanowania zawartosci witryn. Interfejs edycji pozwala konfigurowac nastepujace opcje:

- ***Ochrona w sieci WWW*** — potwierdza, ze skladnik ***Ochrona sieci WWW*** ma skanowac zawartosc stron WWW. Jesli ta opcja jest wlaczona (*domyslnie*), mozna wlaczyc lub wylaczyc nastepujace elementy:
    - ***Skanuj wewnatrz archiwów*** — skanowanie ma obejmowac takze archiwa zawarte na wyswietlanych stronach WWW. .
    - ***Skanuj potencjalnie niechciane programy i oprogramowanie szpiegujace*** — skanowanie ma obejmowac potencjalnie niechciane programy (*pliki wykonywalne, które moga byc programami szpiegujacymi lub reklamowymi*) zawarte na wyswietlanych stronach WWW oraz oprogramowanie szpiegujace.
    - ***Uzyj heurystyki*** — skanowanie zawartosci wyswietlanych stron ma wykorzystywac analize heurystyczna (*dynamiczna emulacje instrukcji*

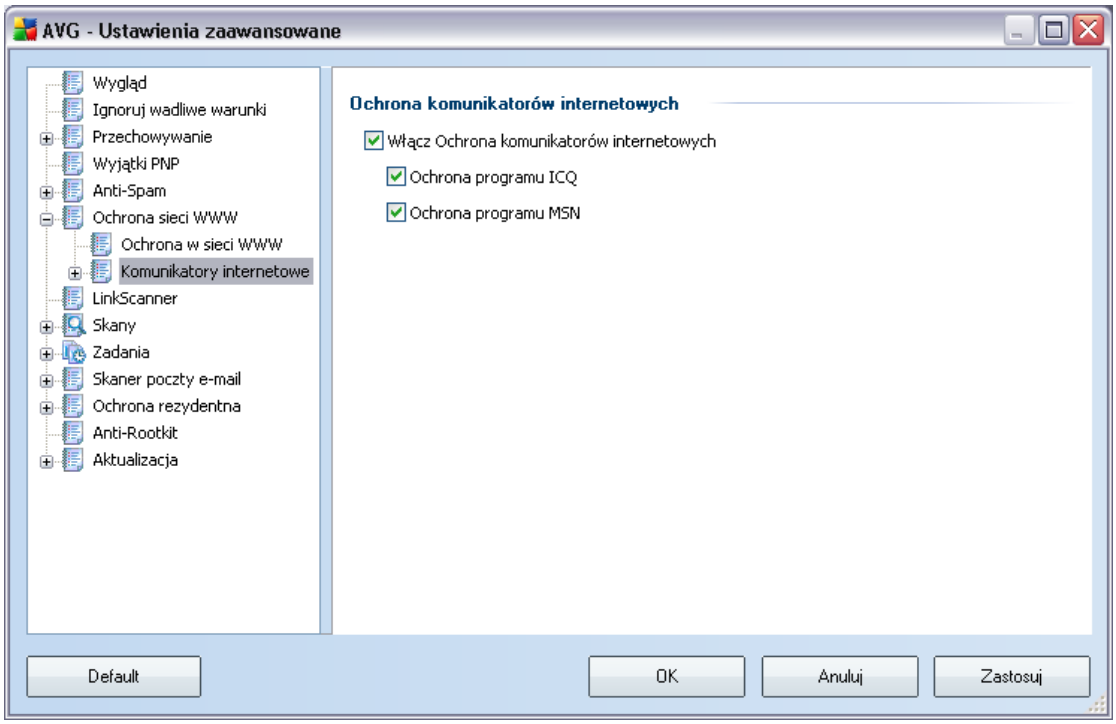
skanowanego obiektu w wirtualnym srodowisku).

- ***Skanowane porty*** — to pole zawiera liste standardowych numerów portów http. Jesli konfiguracja komputera rózni sie od standardowej, mozna zmienic numery portów zgodnie z potrzebami.

- ***Maksymalny rozmiar skanowanych plików*** — jesli wyswietlana strona zawiera pliki, mozna skanowac ich zawartosc jeszcze przed pobraniem na twardy dysk. Poniewaz jednak skanowanie obszernych plików zajmuje dluzszy czas, otwieranie stron WWW moze zostac znacznie spowolnione. Za pomoca tego suwaka mozna okreslic maksymalny rozmiar plików, które maja byc skanowane przez skladnik ***Ochrona sieci WWW***. Nawet jesli pobierany plik jest wiekszy od wybranego limitu i nie zostanie przeskanowany przez skladnik Ochrona sieci WWW, ochrona jest nadal aktywna: jesli plik jest zainfekowany, skladnik ***Ochrona rezydentna*** natychmiast to wykryje.

- ***Wyklucz hosta/adres IP/domene*** — w polu mozna wpisac dokladna nazwe serwera (*host, adres IP, adres IP z maska lub adres URL*) lub domene, które nie powinny byc skanowane przez skladnik ***Ochrona sieci WWW***. Wykluczac nalezy tylko hosty, co do których istnieje absolutna pewnosc, ze nie stanowia zagrozenia.

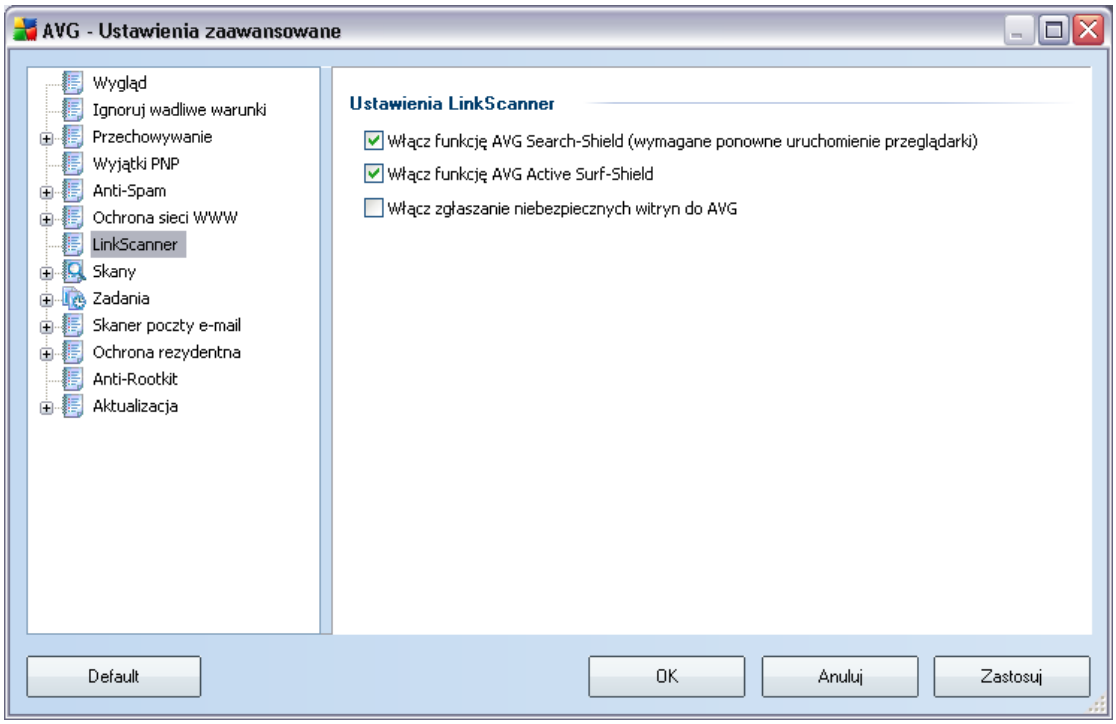
12.5.2.Komunikatory internetowe



W oknie ***Ochrona komunikatorów internetowych*** mozna edytowac ustawienia skladnika ***Ochrona sieci WWW***, dotyczace monitorowania plików przesylanych za posrednictwem komunikatorów. Obecnie obslugiwane sa trzy komunikatory: ***ICQ***, ***MSN*** i ***Yahoo*** — jesli Ochrona sieci WWW ma sprawdzac, czy komunikacja danego komunikatora jest bezpieczna, nalezy zaznaczyc odpowiednie pole wyboru.

Aby szczególowo okreslic zaufane i blokowane kontakty, przejdz do okna ***ICQ — Zaawansowane*** lub ***MSN — Zaawansowane*** (w Ustawieniach zaawansowanych AVG) i wypelnij ***biala liste*** (*uzytkowników, którzy beda mogli przesylac wiadomosci*) oraz ***czarna liste*** (*uzytkowników, którzy maja byc blokowani*).

12.6.LinkScanner



Okno ***Ustawienia LinkScanner*** umozliwia wlaczenie/wylaczenie dwóch podstawowych funkcji skladnika ***LinkScanner***:

- ***Wlacz funkcje AVG Search-Shield*** — (*domyslnie wlaczona*): Skanuje wszystkie linki pojawiajace sie w wynikach wyszukiwania witryn Google, Yahoo! oraz MSN, a nastepnie obok kazdego z nich wyswietla klasyfikacje bezpieczenstwa. Obslugiwane przegladarki to Internet Explorer i Firefox.

- ***Wlacz funkcje AVG Active Surf-Shield*** — (*domyslnie wlaczona*): aktywna (*w czasie rzeczywistym*) ochrona przed niebezpiecznymi witrynami napotykanymi w internecie. Znane zlosliwe witryny i ich niebezpieczna zawartosc blokowane sa juz w momencie otwarcia ich przez uzytkownika za pomoca przegladarki (*lub jakiejkolwiek innej aplikacji korzystajacej z protokolu HTTP*).

- ***Wlacz zglaszanie niebezpiecznych witryn do AVG*** - (*domyslnie aktywne*): Zaznacz to pole, aby wlaczyc raportowanie niebezpiecznych witryn znalezionych przy uzyciu funkcji ***Active Surf-Shield*** lub ***Search-Shield*** w celu przekazania ich do bazy danych pomagajacej chronic uzytkowników AVG.

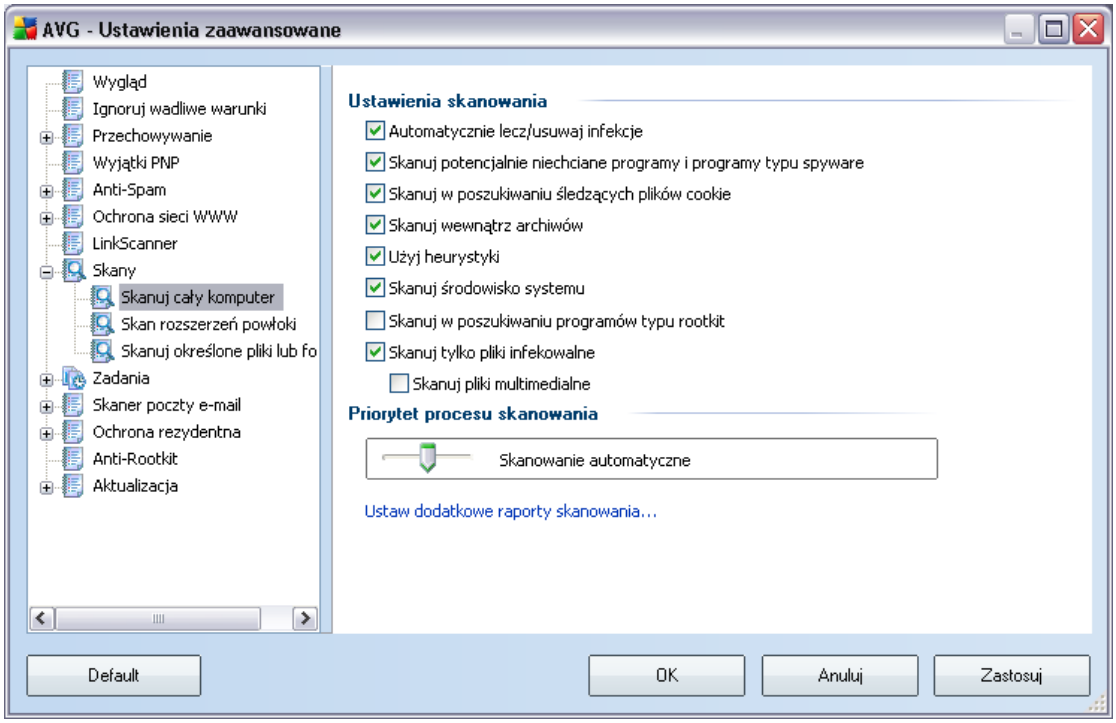
12.7.Skany

Zaawansowane ustawienia skanowania podzielone sa na trzy kategorie odnoszace sie do okreslonych typów testów zdefiniowanych przez producenta AVG:

- ***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.

12.7.1.Skan calego komputera

Opcja ***Skan calego komputera*** umozliwia edycje parametrów jednego ze wstepnie zdefiniowanych testów (***Skanu 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.

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

- ***Skanuj w poszukiwaniu plików cookie*** — ten parametr skladnika Anti-Spyware okresla, czy skanowanie ma obejmowac równiez pliki cookie (*uzywane w protokole HTTP do uwierzytelniania, sledzenia i przechowywania okreslonych informacji o uzytkowniku — np. jego preferencje dotyczace wygladu witryn i zawartosc 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.

- ***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***

- ***Skanuj tylko pliki infekowalne*** — jesli opcja zostanie wlaczona, pliki, które nie moga zostac zainfekowane, nie beda skanowane. Moga to byc np. niektóre pliki tekstowe lub niewykonywalne.

    - ***Skanuj pliki multimedialne*** — zaznaczenie tego pola umozliwi równiez

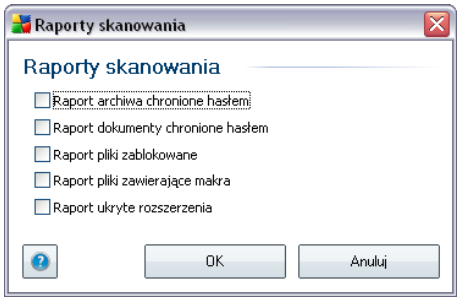
skanowanie plików multimedialnych (wideo, audio itd.). Jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej — pliki multimedialne sa dosc duze i rzadko infekowane przez wirusy.

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.

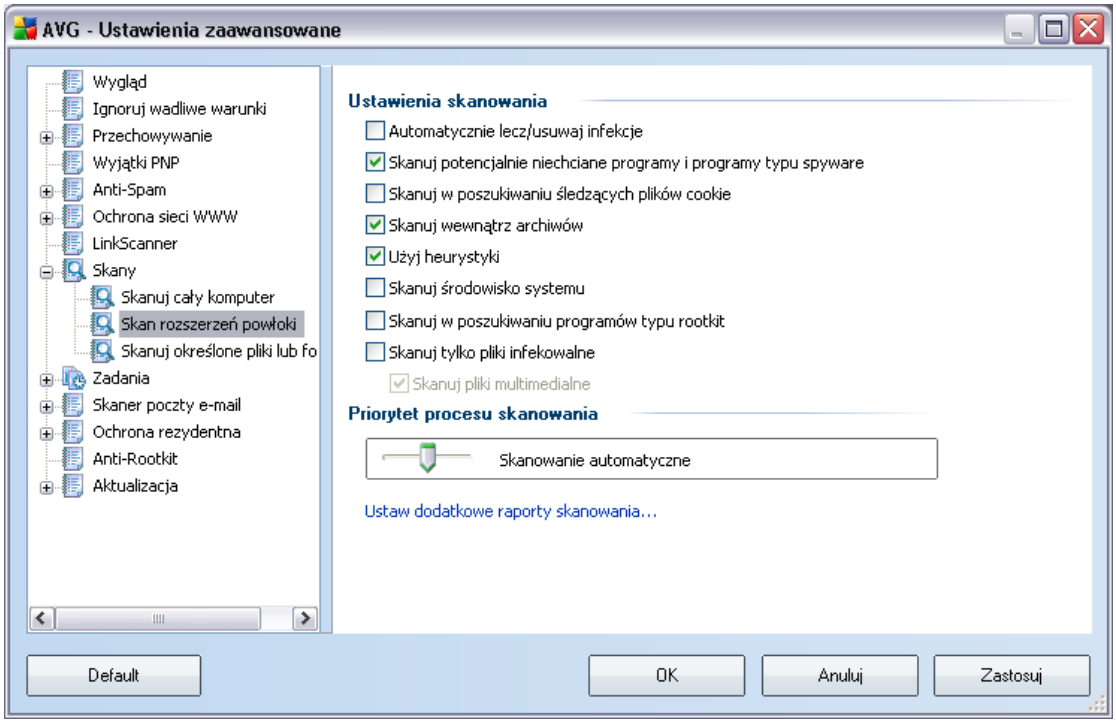
Ustaw dodatkowe raporty skanowania...

Kliknięcie linku ***Ustaw dodatkowe raporty skanowania...*** spowoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym mozna okreslic, jakie zdarzenia maja byc zglaszane:



12.7.2.Skan rozszerzenia powloki

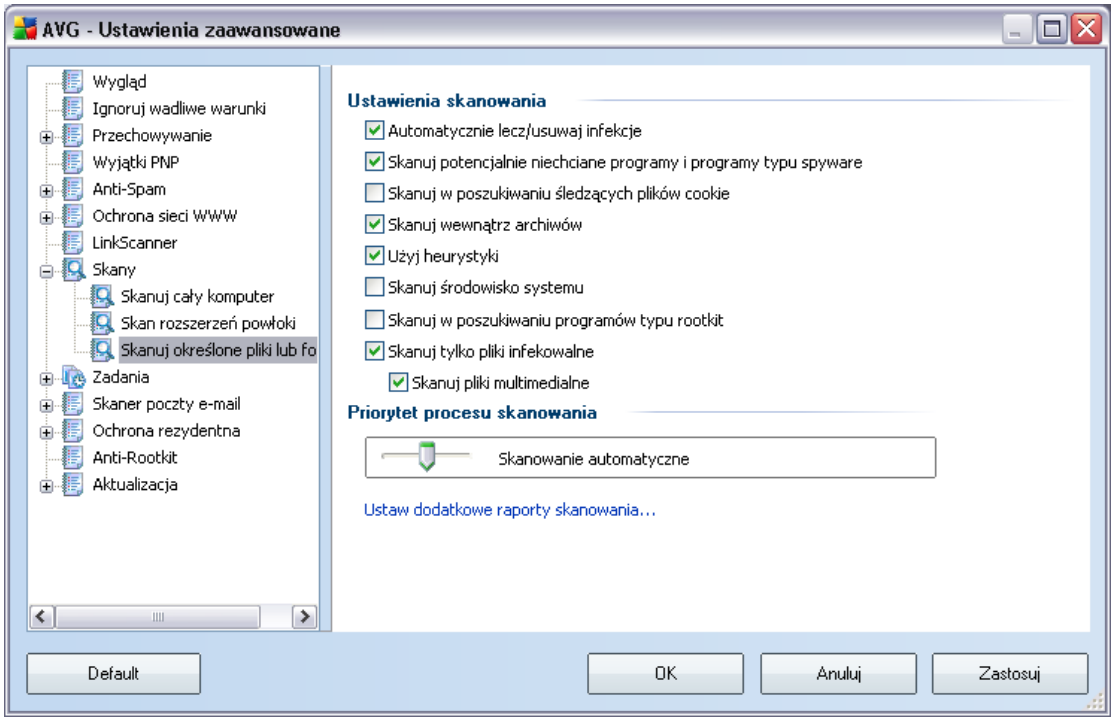
Analogicznie do ***Skanu calego komputera*** , test ***Skan rozszerzenia powloki*** takze oferuje szereg opcji silnika skanujacego, zdefiniowanych wstepnie przez dostawce oprogramowania AVG. W tym przypadku konfiguracja odnosi sie do skanowania okreslonych obiektów bezposrednio z interfejsu Eksploratora 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 testu ***Skan rozszerzenia powloki*** (***Skanowanie z poziomu Eksploratora Windows***) wybrane sa tylko najistotniejsze parametry.

12.7.3.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:

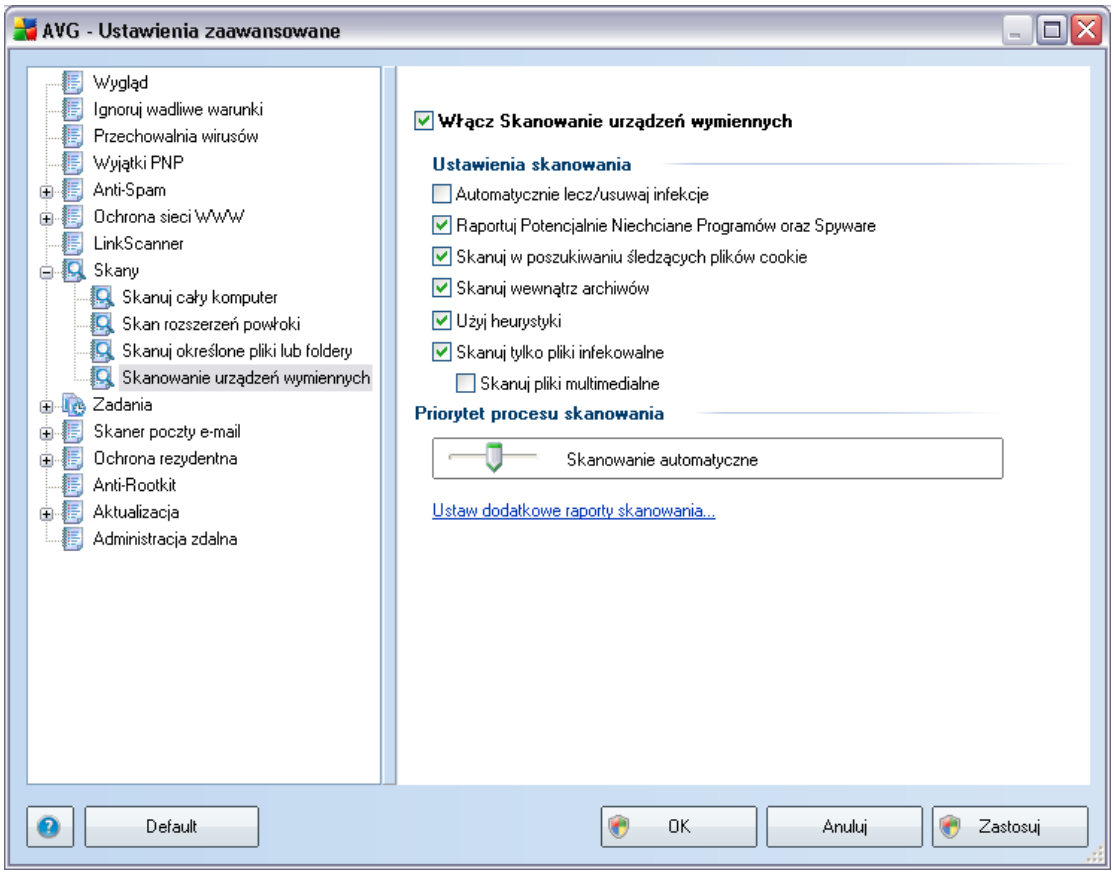


Wszystkie parametry ustawiane w tym oknie dialogowym odnosza sie tylko do obszarów wybranych do ***skanowania okreslonych plików lub folderów***! Zaznaczenie opcji ***Skanuj w poszukiwaniu programów typu rootkit*** w tym oknie konfiguracyjnym oznacza, ze wykonane zostanie tylko szybkie wyszukiwanie programów typu rootkit, czyli skanowanie w poszukiwaniu programów typu rootkit wylacznie w wybranych obszarach.

Uwaga: *Opis poszczególnych parametrów zawiera rozdzial* ***Zaawansowane ustawienia AVG / Skany / Skanowanie calego komputera***.

12.7.4.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 zawiera rozdzial* ***Zaawansowane ustawienia AVG / Skany / Skan calego komputera***.

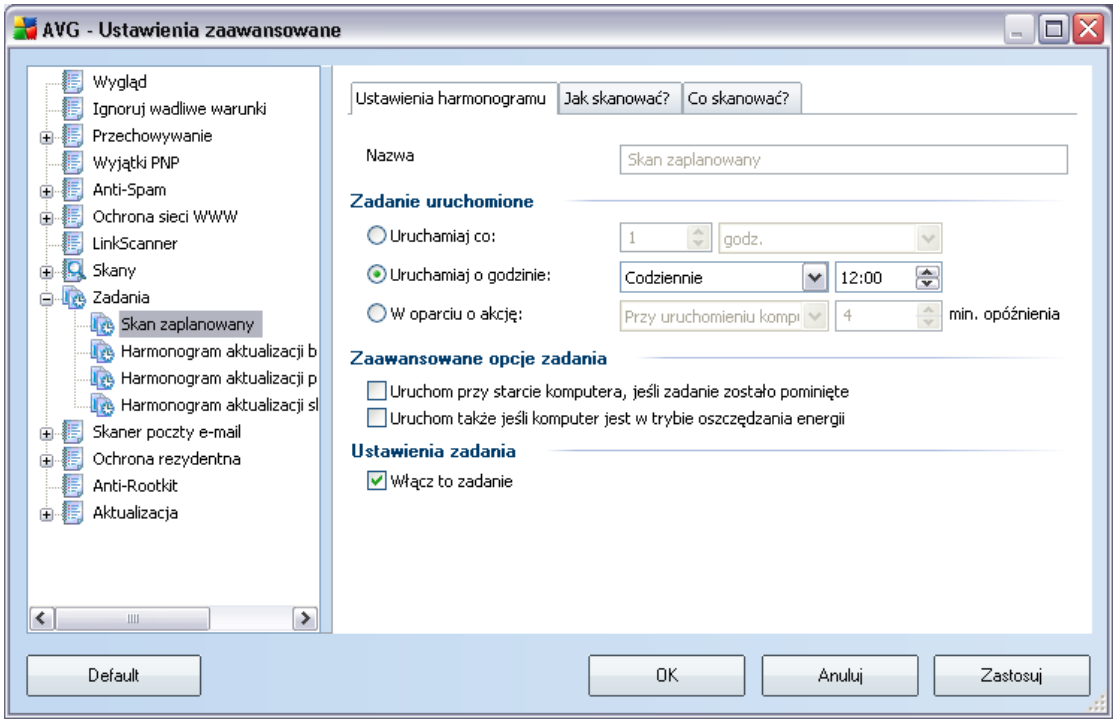
12.8.Zaplanowane zadania

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

- Skan zaplanowany
- Harmonogram aktualizacji bazy danych wirusów
- Harmonogram aktualizacji programu
- Harmonogram aktualizacji skladnika Anti-Spam

12.8.1.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.

Nastepnie nalezy nazwac nowo tworzony skan. Mozna wpisac ja 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.*

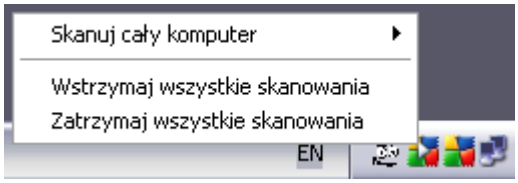
W tym samym oknie mozna szczegółowo okreslic nastepujace parametry skanowania:

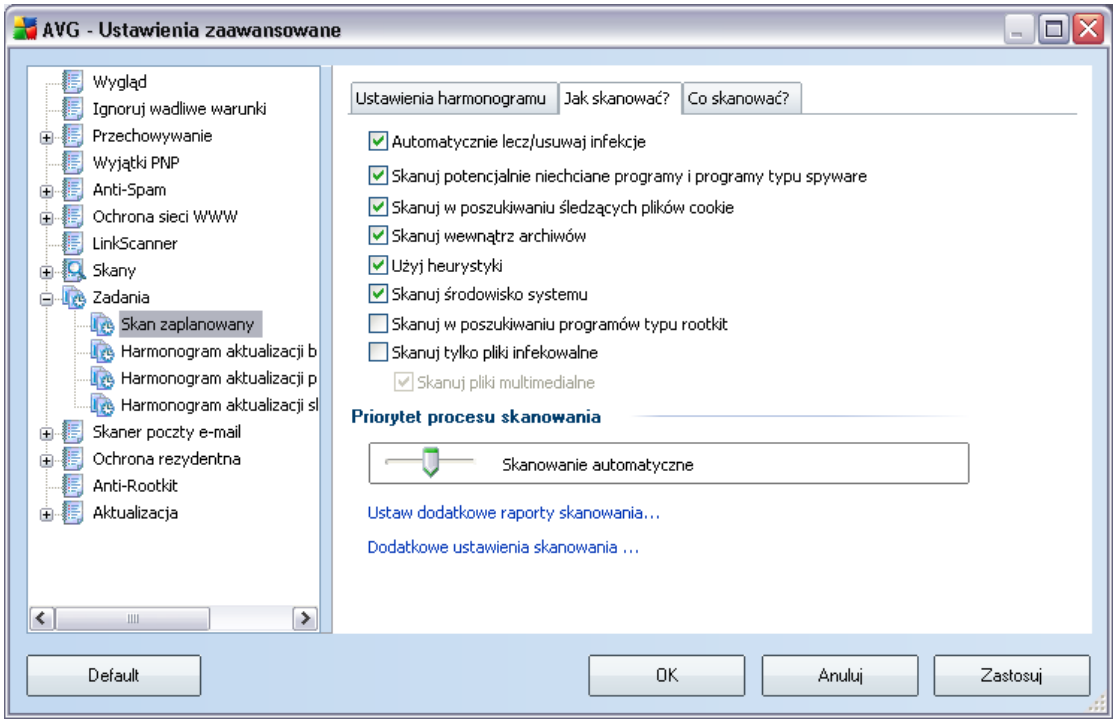
- ***Zadanie uruchomione*** — nalezy okreslic interwal przeprowadzanych testów. Skanowanie moze byc powtarzane w okreslonych odstepach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia zdefiniowanego zdarzenia (***W oparciu o akcje,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

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

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

Nastepnie pojawi sie tam nowa ikona AVG (*kolorowa, z biala strzalka — jak powyzej*), która informuje o uruchomieniu skanowania. Kliknieciе jej prawym przyciskiem myszy pozwala wyswietlic menu kontekstowe, dzieki któremu mozna wstrzymac lub zatrzymac skanowanie:





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.

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

- ***Skanuj w poszukiwaniu plików cookie*** — (*domyslnie wlaczona*) 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 jego preferencje dotyczace wygladu witryny i zawartosc koszyków w sklepach internetowych*).

- ***Skanuj wewnatrz archiwów*** — (*domyslnie wlaczona*) parametr ten okresla, czy 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.

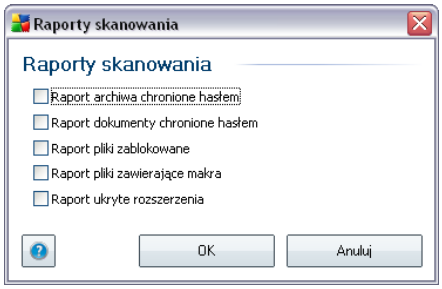
- ***Skanuj srodowisko systemu*** — (*domyslnie wlaczona*) skanowanie obejmie takze obszary systemowe komputera.

- ***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;***

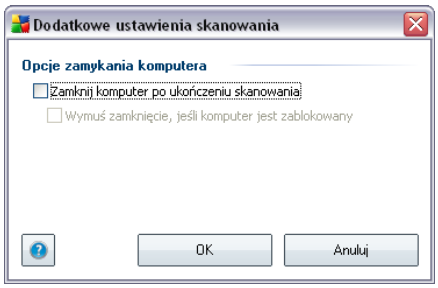
- ***Skanuj tylko pliki infekowalne***— (*domyslnie wylaczona*) jesli opcja ta zostanie wlaczona, pliki, które nie moga zostac zainfekowane, nie beda skanowane. Moga to byc np. niektóre pliki tekstowe lub niewykonywalne.

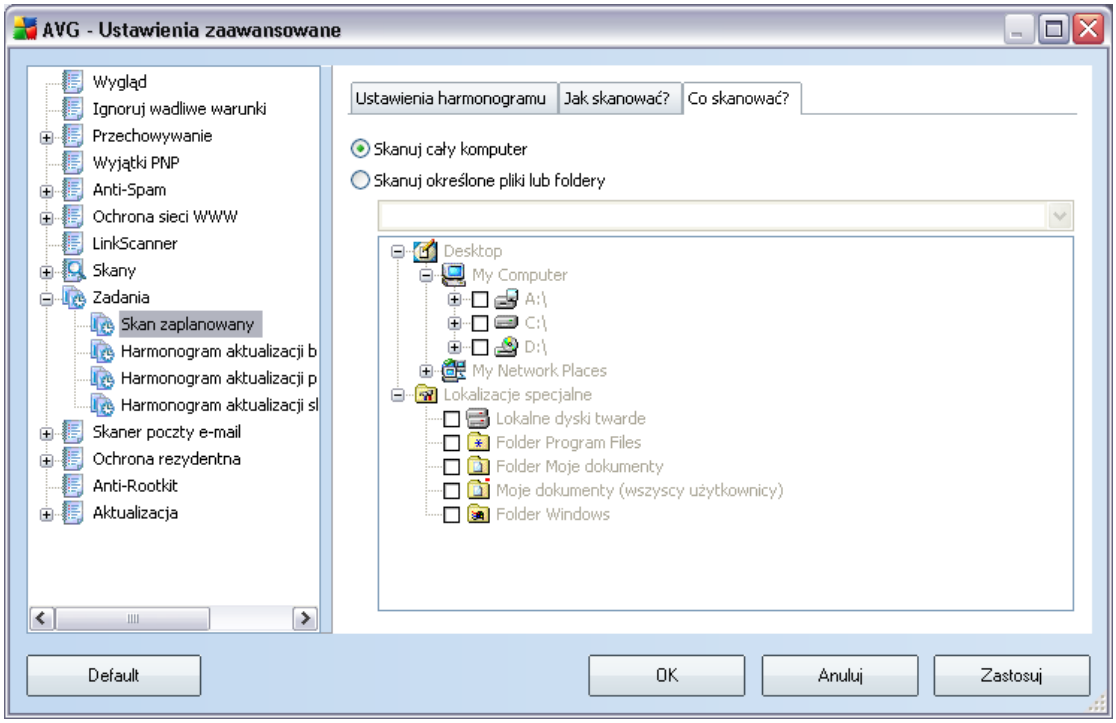
W sekcji ***Priorytet procesu skanowania*** mozna szczególowo okreslic zadana szybkosc skanowania, w zaleznosci od wykorzystania zasobów systemowych. Domyslnie wartosc tej opcji jest na srednim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jesli skanowanie ma przebiegac szybciej, 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.

Kliknięcie lacza ***Ustaw dodatkowe raporty skanowania...*** powoduje otwarcie osobnego okna dialogowego ***Raporty skanowania***, w którym mozna okreslic, co ma byc zglaszane, zaznaczajac wybrane elementy:



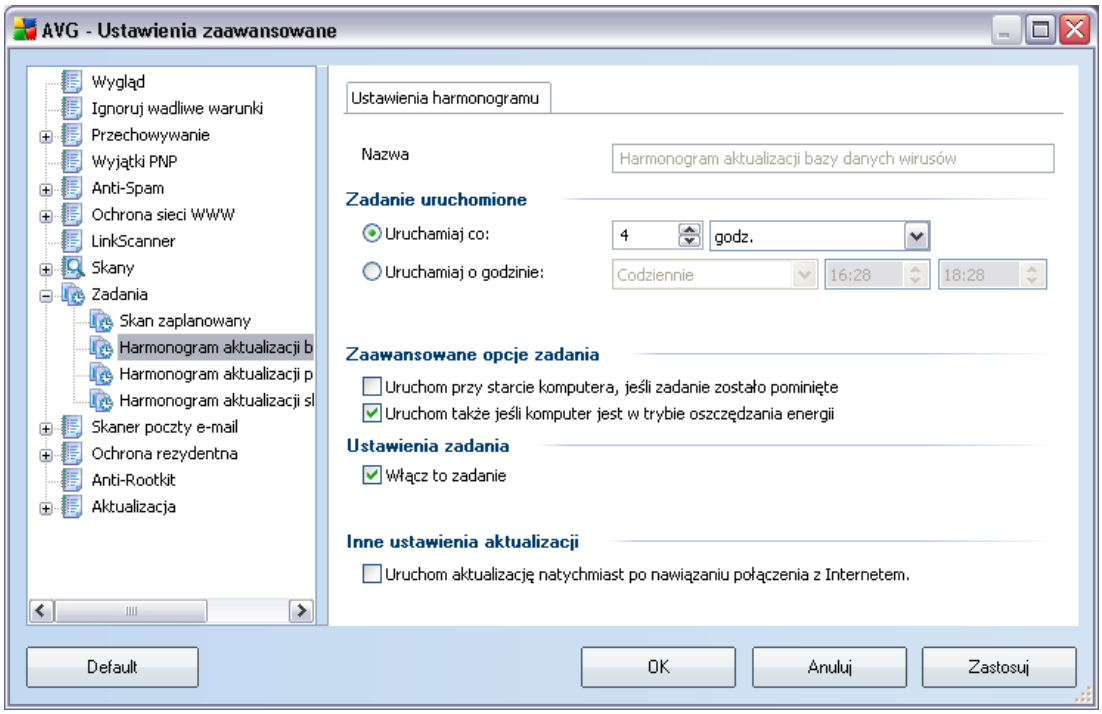
Dodatkowe ustawienia skanowania — lacze pozwala otworzyc nowe okno dialogowe ***Opcje zamykania komputera***, w którym mozna okreslic, czy komputer ma byc zamykany automatycznie po zakonczeniu procesu skanowania. Wybranie tej opcji (***Zamknij komputer po ukonczeniu skanowania***) powoduje aktywowanie nowej opcji, 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.

12.8.2.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:

Nastepnie nalezy podac nazwe utworzonego harmonogramu aktualizacji. Mozna wpisac ja w polu tekstowym obok etykiety ***Nazwa.*** Zaleca sie uzywac krótkich, opisowych nazw, co ulatwi rozpoznanie ich w przyszlosci przez innych uzytkowników.

- ***Zadanie uruchomione*** — nalezy okreslic interwal dla planowanych aktualizacji bazy 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***).

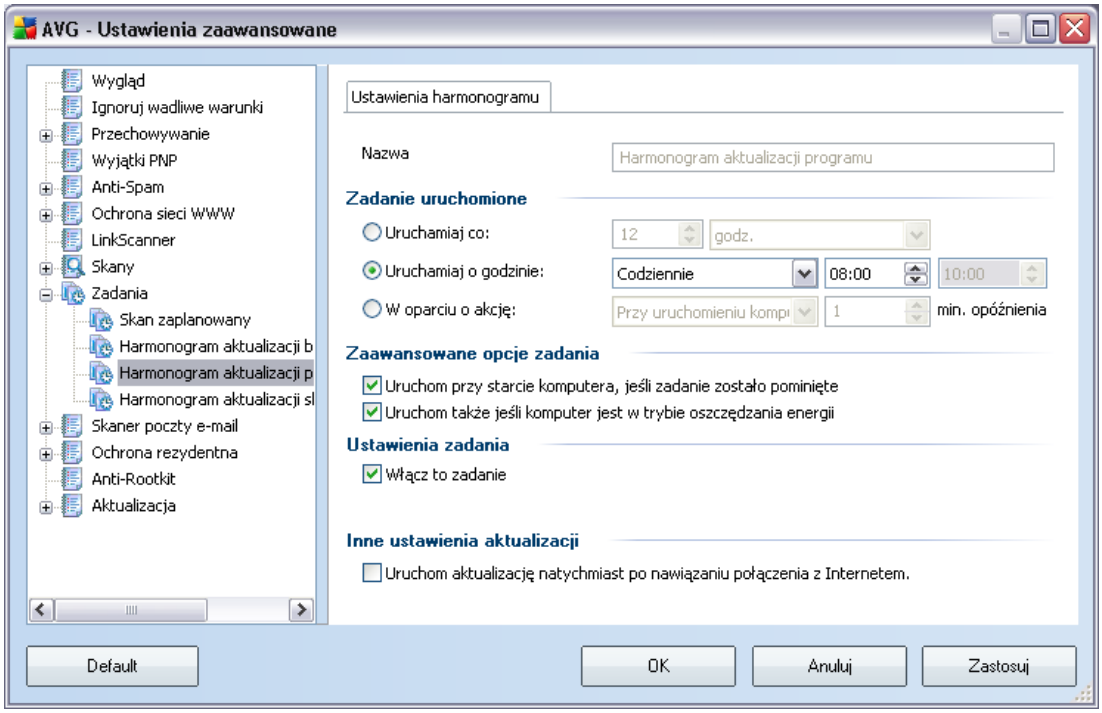
- ***Zaawansowane opcje zadania*** — ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer

pracuje w trybie oszczedzania energii lub jest wylaczony.

- ***Inne ustawienia aktualizacji*** — zaznaczenie tej opcji pozwala wlaczyc ponowne uruchomianie aktualizacji programu natychmiast po usunieciu ewentualnych problemów z polaczeniem internetowym.

Po rozpoczeciu zaplanowanego zadania, nad ikona AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wyglad***).

12.8.3.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.

Nastepnie nalezy podac nazwe utworzonego harmonogramu aktualizacji programu AVG. Mozna wpisac ja w polu tekstowym obok etykiety ***Nazwa.*** Zaleca sie uzywac krótkich, opisowych nazw, co ulatwi rozpoznanie ich w przyszlosci przez innych uzytkowników.

- ***Zadanie uruchamiane*** — nalezy w tym miejscu okreslic interwal dla

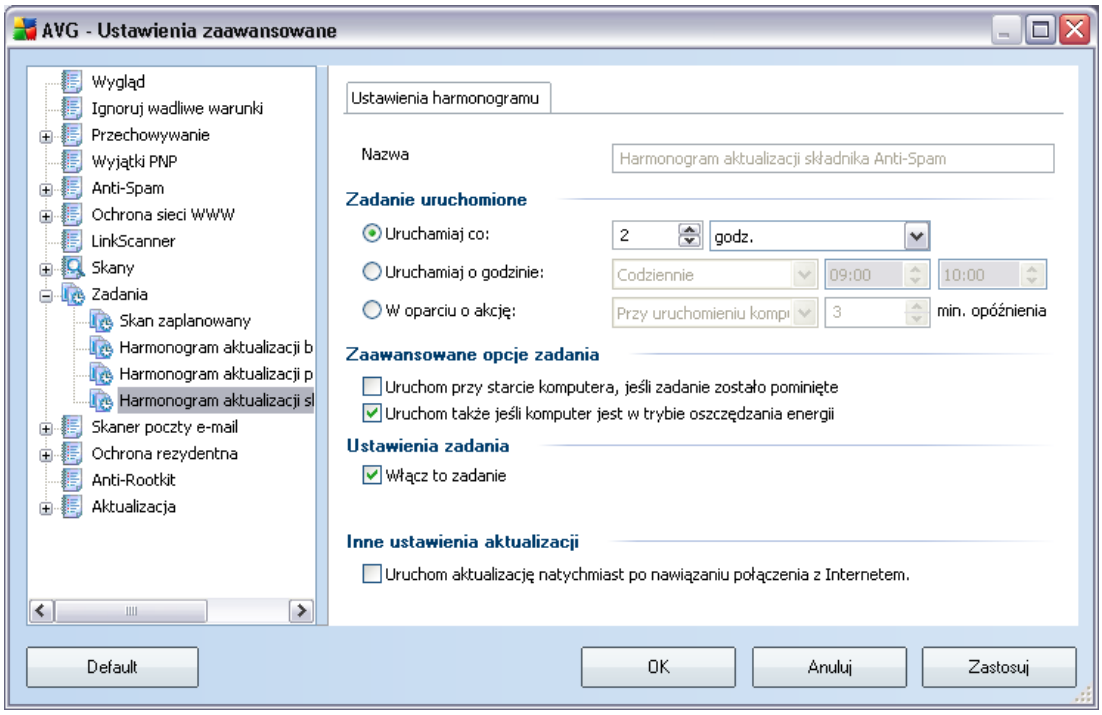
planowanych aktualizacji programu głównego. Aktualizacja moze byc powtarzana w okreslonych odstepach czasu (***Uruchamiaj co***) lub o zadanej godzinie (***Uruchamiaj o okreslonej godzinie***), a takze na skutek wystapienia zdefiniowanego zdarzenia (***W oparciu o akcje, np. uruchomienie komputera***).

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

- ***Inne ustawienia aktualizacji*** — zaznaczenie tej opcji pozwala wlaczyc ponowne uruchomianie aktualizacji programu natychmiast po usunieciu ewentualnych problemów z polaczeniem internetowym.

Po rozpoczeciu zaplanowanego zadania, nad ikona AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wyglad***).

12.8.4.Harmonogram aktualizacji skladnika Anti-Spam



Na karcie ***Ustawienia harmonogramu*** mozna odznaczyc pole ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana aktualizacje skladnika ***Anti-Spam i wlaczyc***

ja ponownie dopiero gdy zajdzie taka potrzeba.

Podstawowe opcje planowania aktualizacji skladnika ***Anti-Spam*** opisano w interfejsie ***Menedzera aktualizacji***. W niniejszym oknie mozna ustawic szczególowe parametry harmonogramu:

Nastepnie nalezy nazwac tworzony harmonogram aktualizacji skladnika ***Anti-Spam***. Wpisz zadana nazwe w polu tekstowym obok etykiety ***Nazwa.*** Zaleca sie uzywac krótkich, opisowych nazw, co ulatwi rozpoznanie ich w przyszlosci przez innych uzytkowników.

- ***Zadanie uruchomione*** — nalezy okreslic interwal dla planowanych aktualizacji skladnika ***Anti-Spam*** . Aktualizacja skladnika ***Anti-Spam*** 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***).

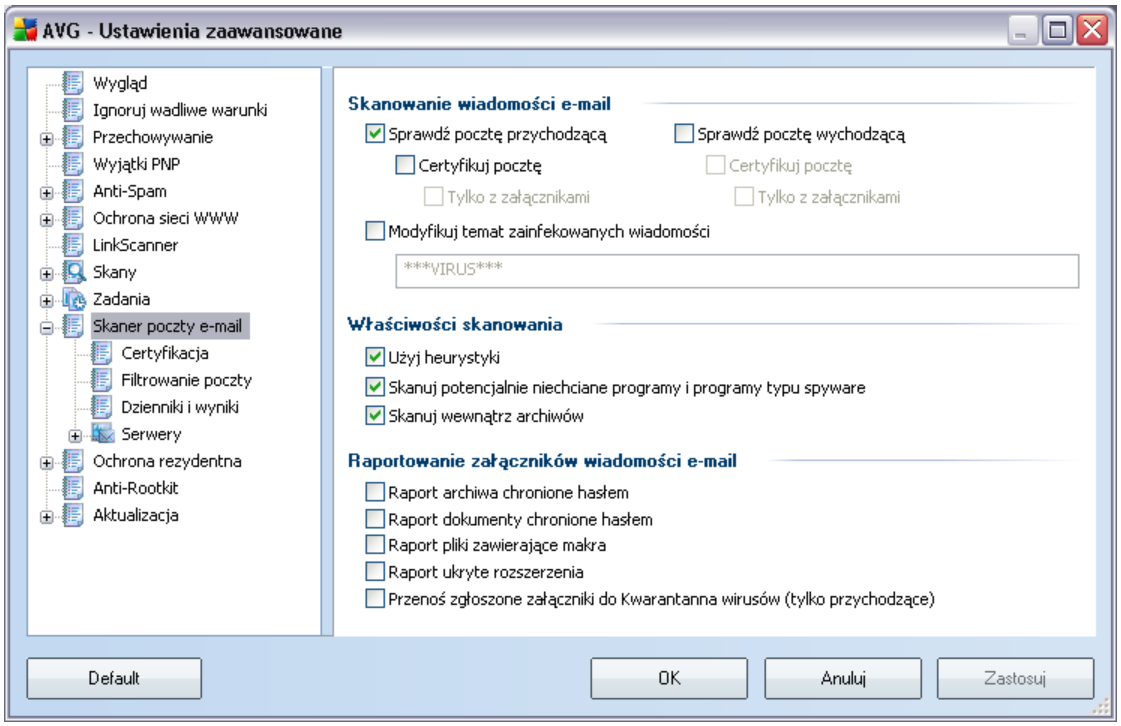
- ***Zaawansowane opcje zadania*** — ta sekcja umozliwia zdefiniowanie warunków uruchamiania aktualizacji skladnika ***Anti-Spam*** w czasie, gdy komputer pracuje w trybie oszczedzania energii lub jest wylaczony.

- ***Ustawienia zadania*** — w tej sekcji mozna odznaczyc opcje ***Wlacz to zadanie***, aby tymczasowo wylaczyc zaplanowana aktualizacje skladnika ***Anti-Spam*** lub, w razie potrzeby, ponownie ja wlaczyc.

- ***Inne ustawienia aktualizacji*** — zaznaczenie tej opcji pozwala wlaczyc ponowne uruchomianie aktualizacji skladnika ***Anti-Spam*** natychmiast po usunieciu ewentualnych problemów z polaczeniem internetowym.

Po rozpoczeciu zaplanowanego zadania, nad ikona AVG na pasku systemowym wyswietlone zostanie odpowiednie powiadomienie (*przy domyslnej konfiguracji zastosowanej w sekcji **Ustawienia zaawansowane/Wyglad*)*.

12.9.Skaner poczty e-mail



Okno ***Skaner poczty e-mail*** podzielone jest na trzy sekcje:

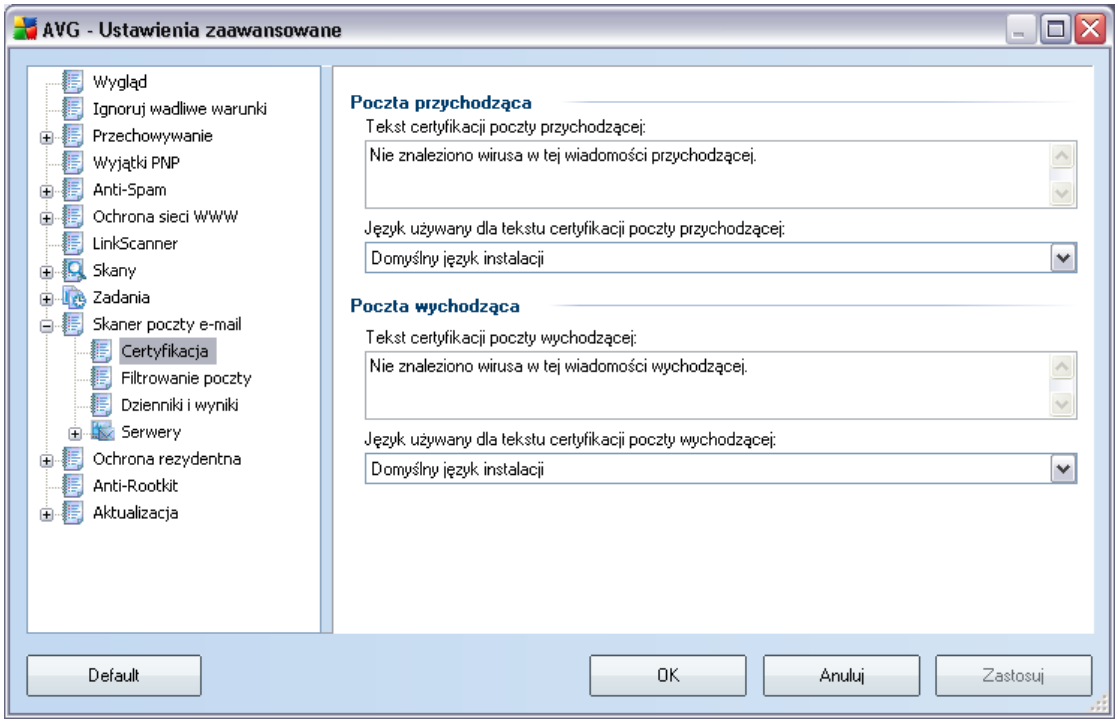
- ***Skanowanie poczty e-mail*** — w sekcji tej mozna okreslic, czy maja byc skanowane wiadomosci przychodzace i wychodzace, a takze czy certyfikacja ma obejmowac wszystkie wiadomosci, czy tylko te z zalacznikami (certyfikacja *nie jest dostepna w formacie HTML/RTF*). Ponadto, mozna okreslic, czy program AVG ma modyfikowac temat wiadomosci potencjalnie zawierajacych wirusy. W tym celu nalezy zaznaczyc pole ***Modyfikuj temat zainfekowanych wiadomosci*** i ewentualnie zmienic tekst w polu obok (*domyslnie jest to ***WIRUS****).

- ***Wlasciwosci skanowania*** — nalezy okreslic, czy podczas skanowania ma bys stosowana analiza heurystyczna (***Uzyj heurystyki***), czy system AVG ma również szukac potencjalnie niechcianych programów (***Skanuj potencjalnie niechciane programy***), a takze czy skanowane maja byc tez archiwa (***Skanuj wewnatrz archiwów***).

- ***Raportowanie zalaczników e-mail*** — nalezy okreslic, czy system ma powiadamiac poczta e-mail o archiwach zabezpieczonych haslem,

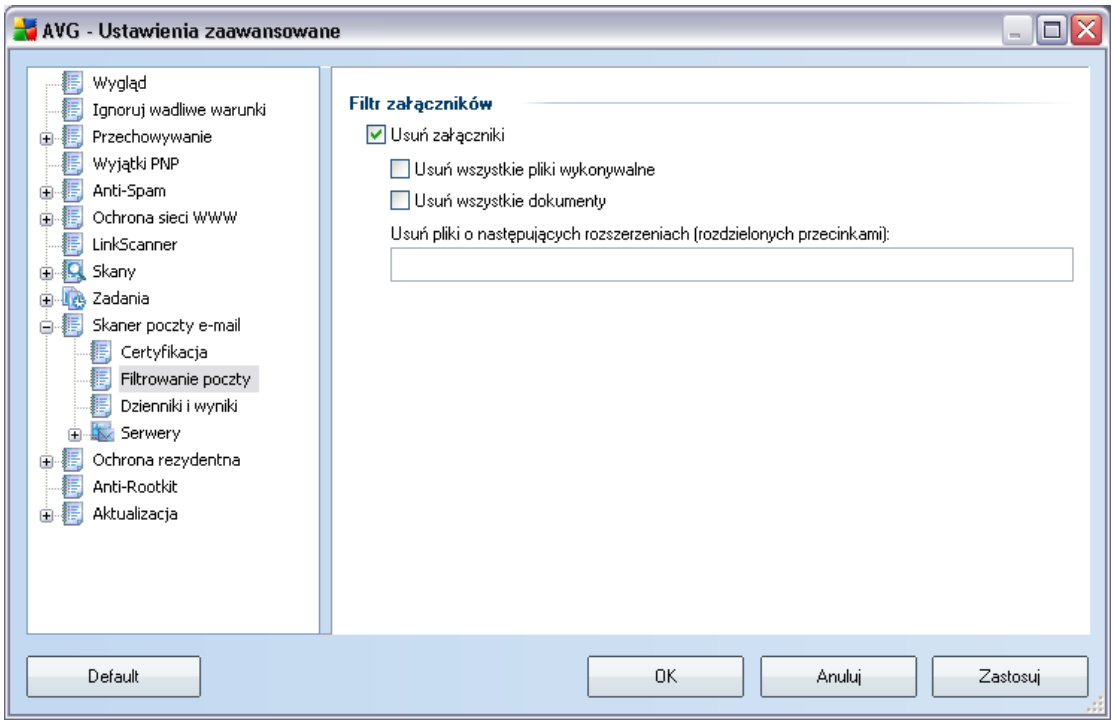
dokumentach zabezpieczonych haslem, plikach zawierajacych makra i/lub plikach o ukrytych rozszerzeniach, które zostana wykryte jako zalaczniki do skanowanych wiadomosci e-mail. Nalezy takze okreslic, czy w przypadku wykrycia takiej wiadomosci podczas skanowania zainfekowany obiekt ma zostac przeniesiony do ***Kwarantanny wirusów***.

12.9.1.Certyfikacja



W oknie ***Certyfikacja*** mozna szczególowo okreslic tresc certyfikatu oraz jego jezyk. Ustawienia te nalezy wprowadzic osobno dla ***wiadomosci przychodzacych*** i ***wychodzacych***.

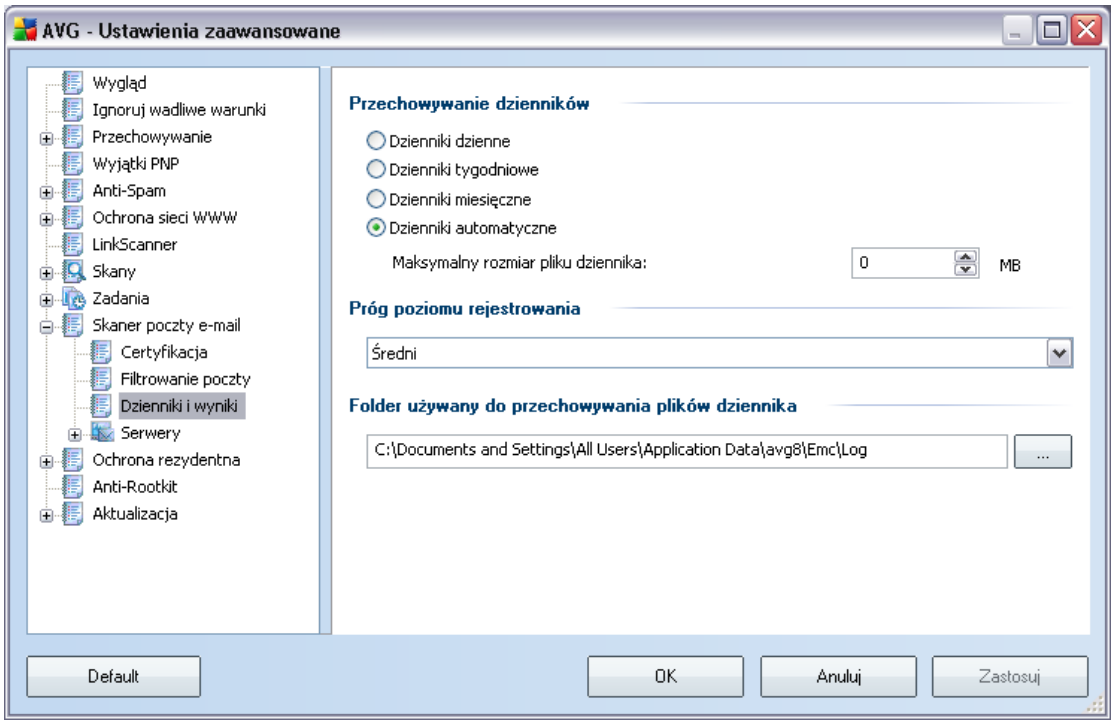
12.9.2.Filtrowanie poczty



W oknie ***Filtr zalaczników*** mozna ustawiac parametry skanowania zalaczników e-mail. Opcja ***Usun zalaczniki*** jest domyslnie wylaczona. Jesli zostanie wlaczona, wszystkie zalaczniki wiadomosci zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, beda automatycznie usuwane. Aby okreslic typy zalaczników, które maja byc usuwane, nalezy zaznaczyc odpowiednia opcje:

- ***Usun wszystkie pliki wykonywalne*** — usuwane beda wszystkie pliki *.exe.
- ***Usun wszystkie dokumenty*** — usuwane beda wszystkie pliki *.doc.
- ***Usun pliki o nastepujacych rozszerzeniach*** — usuwane beda wszystkie pliki o zdefiniowanych rozszerzeniach.

12.9.3.Dzienniki i Wyniki

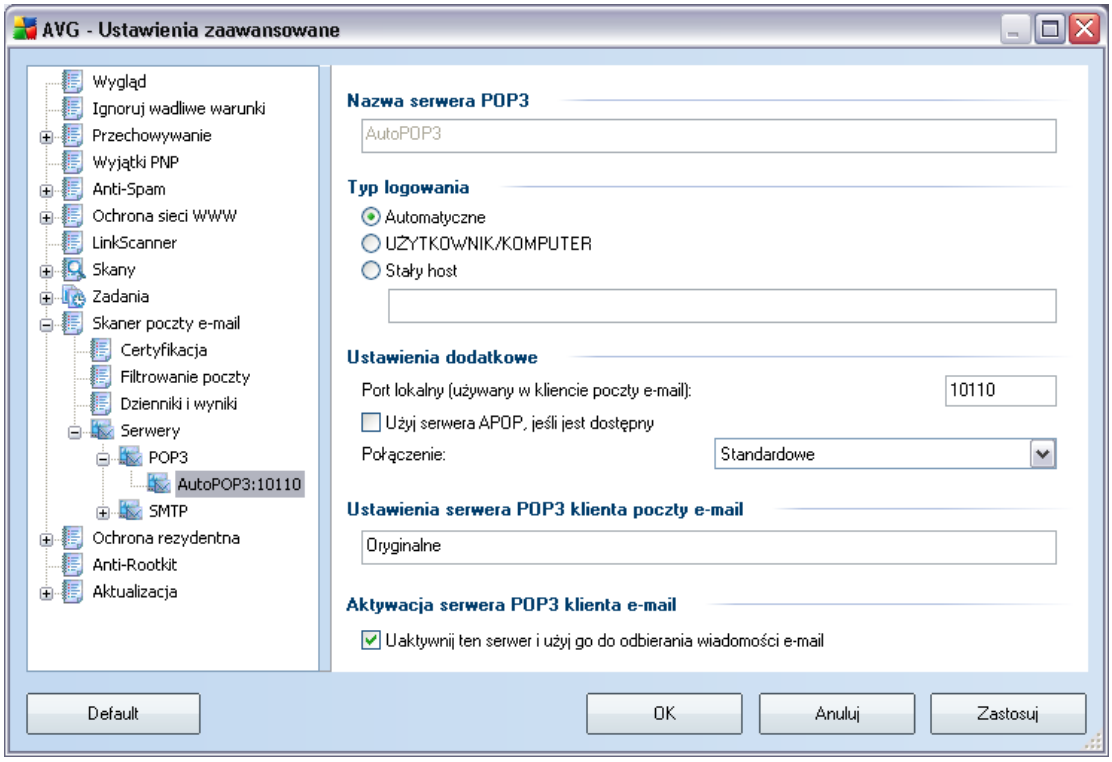


W oknie ***Dzienniki i wyniki*** mozna okreslic parametry przechowywania wyników skanowania poczty e-mail. Okno to podzielone jest na dwa obszary:

- ***Przechowywanie dzienników*** — pozwala zdecydowac, czy informacje o skanowaniu poczty e-mail maja byc rejestrowane codziennie, co tydzien, co miesiac itd.; mozna tu takze okreslic maksymalny rozmiar pliku dziennika (*w MB*).
- ***Próg poziomu rejestrowania*** — domyslnie ustawiony jest poziom sredni; mozna wybrac nizszy (*rejestrowanie podstawowych informacji o polaczeniu*) lub wyzszy (*rejestrowanie calego ruchu*).
- ***Folder uzywany do przechowywania plików dziennika*** — pozwala okreslic, gdzie maja znajdowac sie pliki dziennika.

12.9.4.Serwery

W sekcji ***Serwery*** edytowac mozna parametry wirtualnych serwerów ***Skanera poczty e-mail*** lub zdefiniowac nowy (klikajac przycisk ***Dodaj nowy serwer***).



W tym oknie dialogowym (dostepnym z menu ***Serwery / POP3***) mozna zdefiniowac (na potrzeby ***Skanera poczty e-mail***) nowy serwer poczty przychodzacej, korzystajacy z protokolu POP3:

- ***Nazwa serwera POP3*** — nalezy wpisac nazwe serwera lub zachowac domyslna nazwe AutoPOP3.
- ***Typ logowania*** — definiuje metode okreslania serwera pocztowego dla wiadomosci przychodzacych:
  - Automatyczne — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail.
  - UZYTKOWNIK/KOMPUTER — najprostsza i najczesciej uzywana metoda ustalania docelowego serwera pocztowego jest metoda proxy. Stosujac te metode, jako czesc loginu uzytkownika nalezy podac jego nazwe lub adres (lub takze port), oddzielajac ja znakiem /. Na przyklad dla konta uzytkownik1 na serwerze pop.domena.com z numerem portu 8200 nalezy stosowac login uzytkownik1/pop.domena.com:8200.

- Staly host — po wybraniu tej opcji program bedzie zawsze korzystal z serwera okreslonego w tym miejscu. Nalezy podac adres lub nazwe serwera pocztowego. Login uzytkownika pozostaje niezmieniony. Jako nazwy mozna uzyc nazwy domeny (na przyklad pop.acme.com) lub adresu IP (na przyklad 123.45.67.89). Jesli serwer pocztowy uzywa niestandardowego portu, mozna okreslic go po dwukropku zaraz za nazwa serwera (na przyklad pop.domena.com:8200). Standardowym portem protokolu POP3 jest 110.

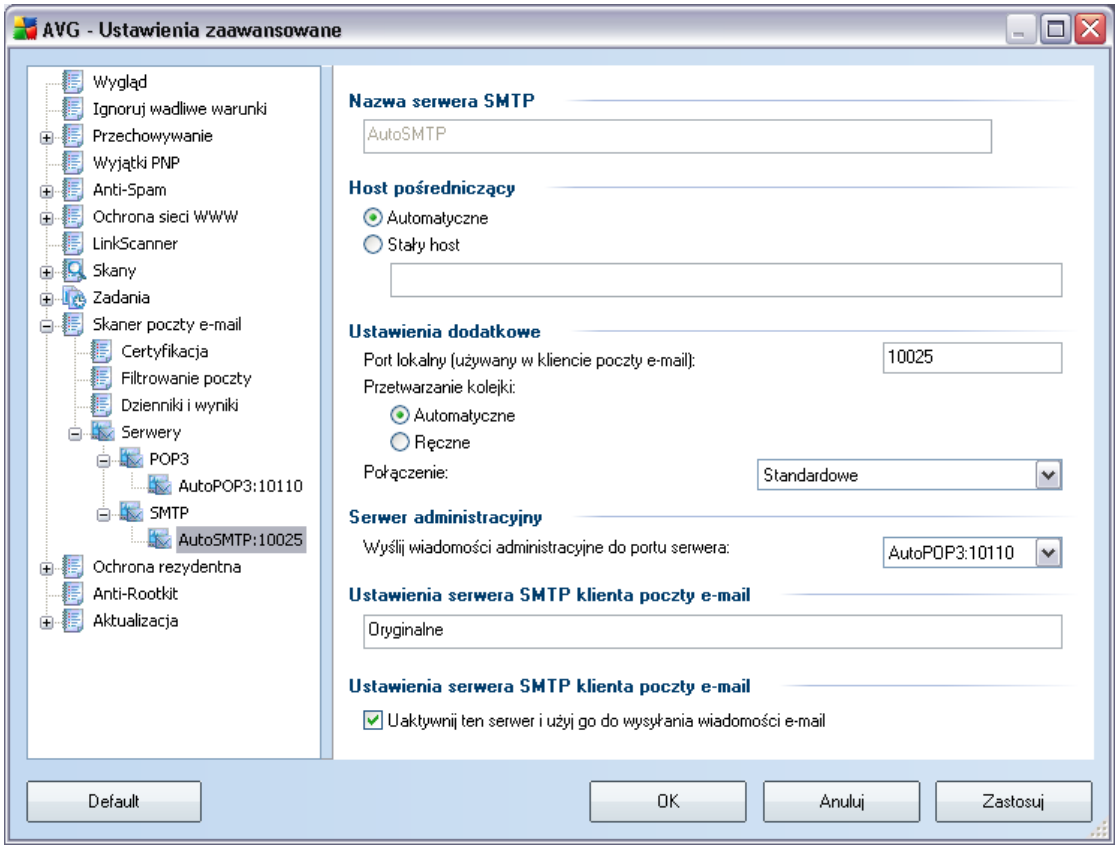
- ***Ustawienia dodatkowe*** — pozwalaja zdefiniowac bardziej szczególowe parametry:

  - Port lokalny — okresla port nasluchu dla aplikacji pocztowej. Ten sam port nalezy nastepnie okreslic w kliencie poczty jako port docelowy serwera POP3.

  - Uzyj serwera APOP, jesli jest dostepny — opcja zapewnia bezpieczniejsze logowanie na serwerze pocztowym. Gwarantuje to, ze ***Skaner poczty e-mail*** bedzie uzywal alternatywnej metody przekazywania hasla uzytkownika, polegajacej na wysylaniu go w formie zaszyfrowanej, która korzysta ze zmiennego klucza nadeslanego przez serwer. Funkcja ta dostepna jest tylko wtedy, gdy obsluguje ja docelowy serwer pocztowy.

  - Polaczenie — z menu rozwijanego nalezy wybrac rodzaj uzywanego polaczenia (zwykle/SSL/domyslne SSL). Jesli zostanie wybrane polaczenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostepna jest tylko wtedy, gdy obsluguje ja docelowy serwer pocztowy.

- ***W obszarze Aktywacja serwera POP3 klienta e-mail*** — znajduja sie informacje dotyczace poprawnych ustawien klienta poczty e-mail (tak, aby wszystkie wiadomosci przechodzily przez ***Skaner poczty e-mail***). Informacje te stanowia podsumowanie odpowiednich parametrów okreslonych w calej konfiguracji AVG.



W tym oknie dialogowym (dostepnym z menu ***Serwery / SMTP***) mozna zdefiniowac (na potrzeby ***Skanera poczty e-mail***) nowy serwer poczty przychodzacej, korzystajacy z protokolu SMTP:

- ***Nazwa serwera SMTP*** — nalezy podac nazwe serwera lub zachowac domyslna (AutoSMTP).
- ***Host posredniczacy*** — definiuje metode okreslania serwera pocztowego dla wiadomosci wychodzacych:
  - Automatyczne — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail
  - Staly host — po wybraniu tej opcji program bedzie zawsze korzystal z serwera okreslonego w tym miejscu. Nalezy podac adres lub nazwe serwera pocztowego. Jako nazwy mozna uzyc domeny (na przyklad

smtp.domena.com) lub adresu IP (na przyklad 123.45.67.89). Jesli serwer pocztowy uzywa niestandardowego portu, mozna okreslic go po dwukropku zaraz za nazwa serwera (np. smtp.acme.com:8200). Standardowym portem protokolu SMTP jest port 25.

- ***Ustawienia dodatkowe*** — pozwalaja zdefiniowac bardziej szczególowe parametry:

o Port lokalny — okresla port nasluchu dla aplikacji pocztowej. Ten sam port nalezy nastepnie okreslic w aplikacji pocztowej jako port komunikacji SMTP.

o Przetwarzanie kolejki — okresla zachowanie ***Skanera poczty e-mail*** podczas przetwarzania zadan wysylania wiadomosci:

➢ Automatycznie — poczta wychodzaca jest natychmiast dostarczana (wysylana) do docelowego serwera pocztowego.

➢ Reczne — wiadomosci sa umieszczane w kolejce wiadomosci wychodzacych i wysylane w późniejszym terminie.

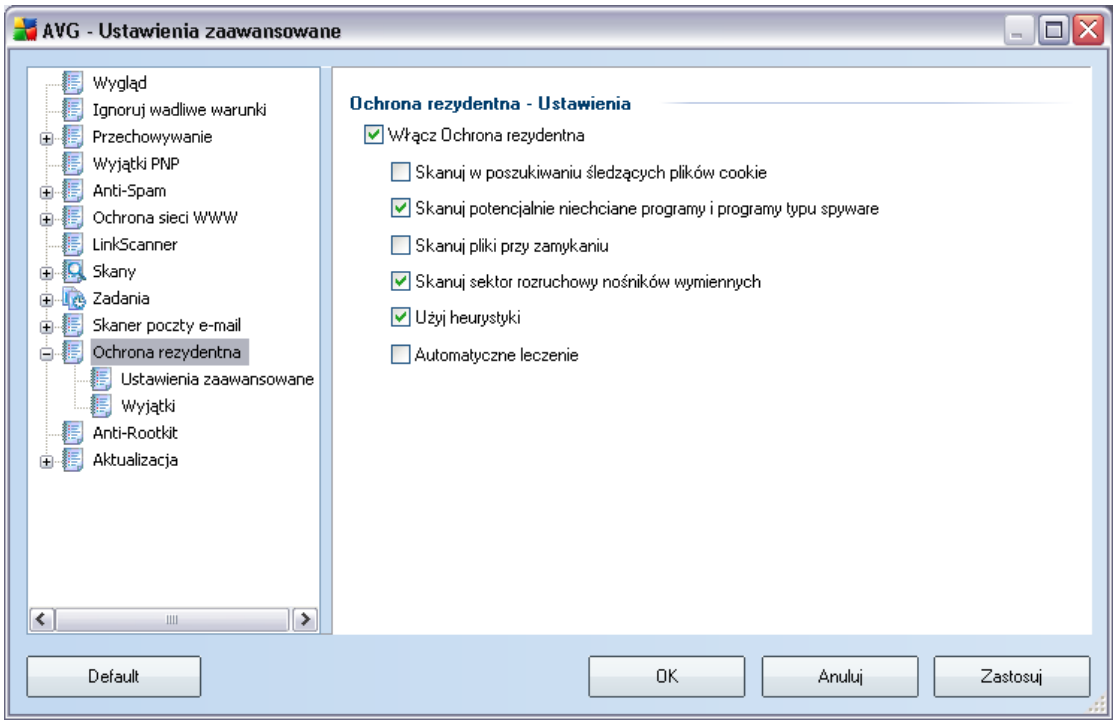
o Polaczenie — z menu rozwijanego nalezy wybrac rodzaj uzywanego polaczenia (zwykle/SSL/domyslne SSL). Jesli zostanie wybrane polaczenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostepna jest tylko wtedy, gdy obsluguje ja docelowy serwer pocztowy.

- ***Serwer administracyjny*** — zawiera numer portu serwera uzywanego do zwrotnego dostarczania raportów administracyjnych. Takie wiadomosci sa generowane, kiedy np. serwer docelowy jest niedostepny lub odrzuca wiadomosc wychodzaca.

- ***W sekcji*** Ustawienia serwera SMTP klienta poczty e-mail znajduja sie zalecenia dotyczace takiej konfiguracji klienta poczty, która umozliwi wysylanie wiadomosci do aktualnie modyfikowanego serwera. Informacje te stanowia podsumowanie odpowiednich parametrów okreslonych w calej konfiguracji AVG.

12.1. 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 pliki cookie*** — parametr 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*.)

- ***Skanuj potencjalnie niechciane programy*** — (*domyslnie wlaczona*) skanowanie w poszukiwaniu potencjalnie niechcianych programów (*plików wykonywalnych, które moga byc oprogramowaniem szpiegujacym lub reklamowym*).

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

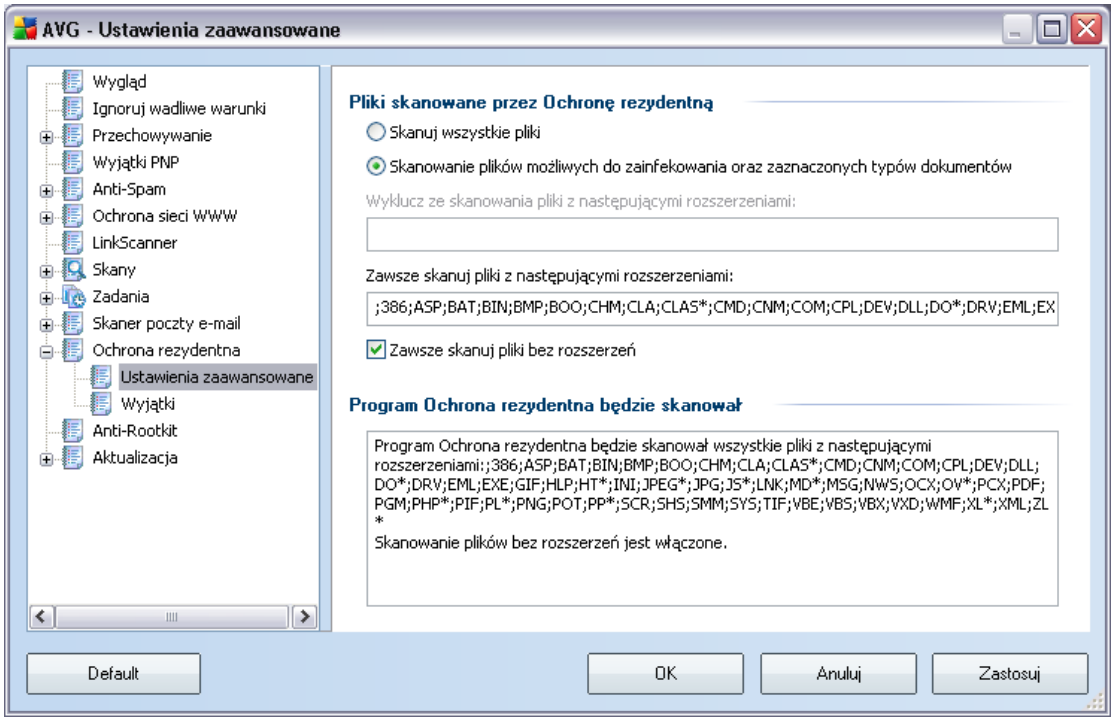
- ***Skanuj sektor rozruchowy nosników wymiennych*** — (*domyslnie wlaczona*)

- ***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).

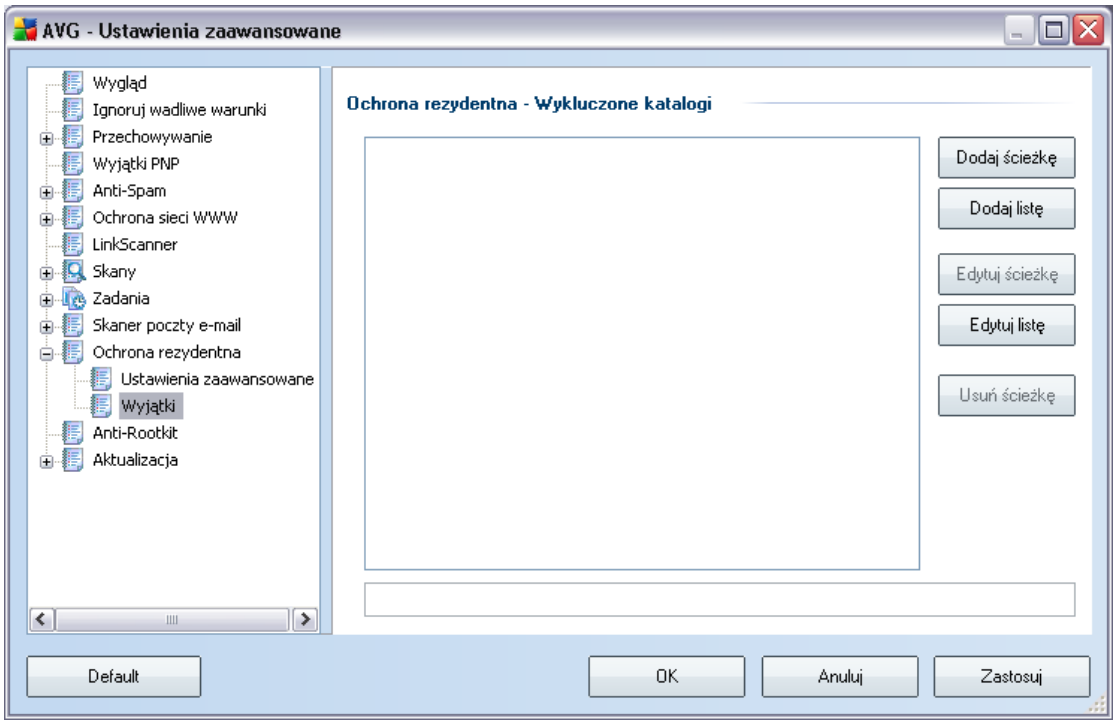
12.10.1. Ustawienia zaawansowane

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.

12.10.Wyjatki



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! Wykluczenie folderu ze skanowania funkcji ***Ochrona rezydentna*** zaczyna obowiazywac dopiero po ponownym uruchomieniu komputera!

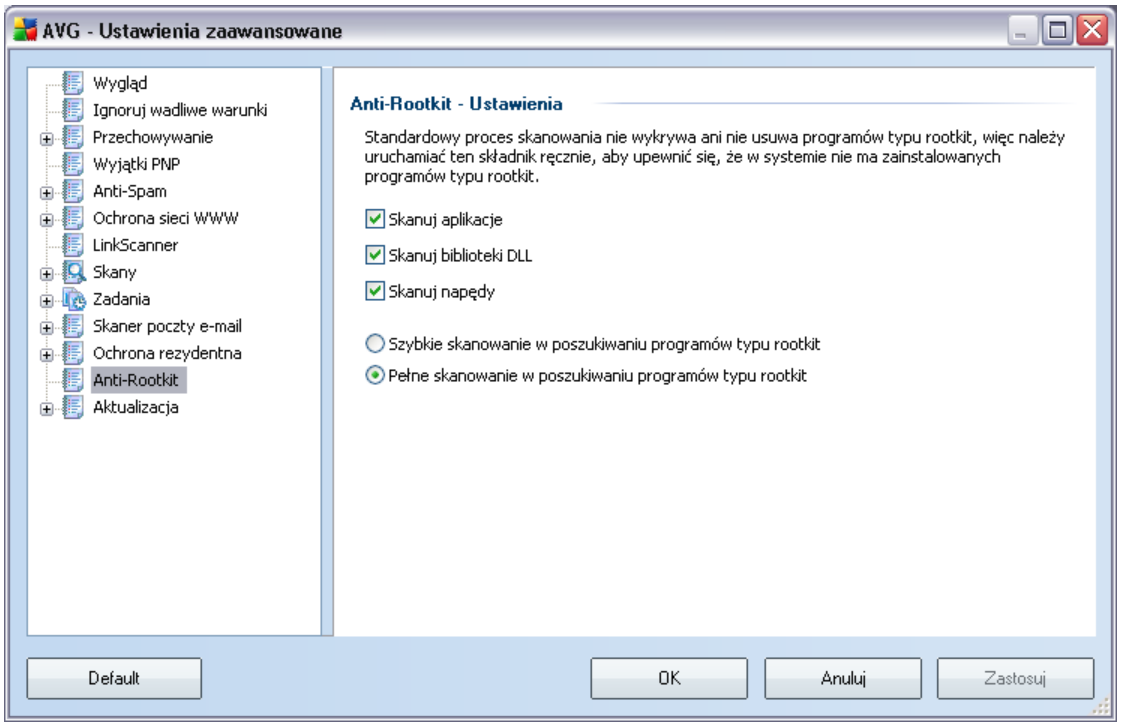
W biezacym oknie dostepne sa nastepujace przyciski kontrolne:

- ***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.

12.11 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***.

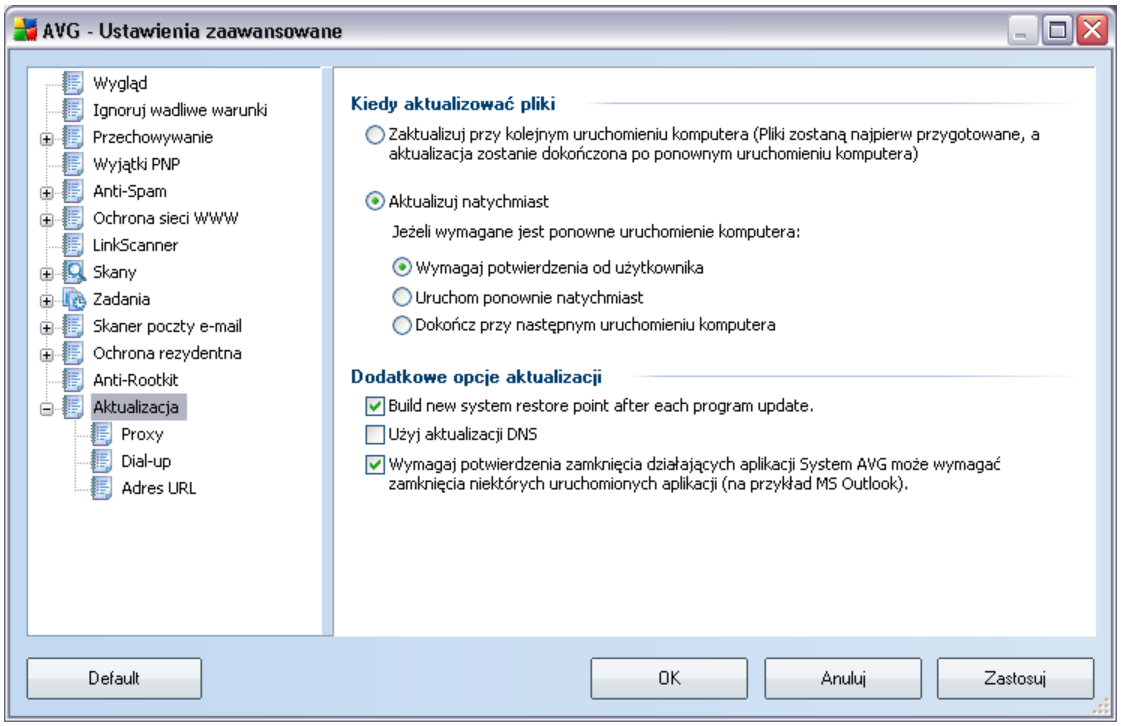
Nalezy zaznaczyc odpowiednie pola wyboru, aby okreslic obiekty, które maja byc skanowane:

- ***Skanuj aplikacje***
- ***Skanuj biblioteki DLL***
- ***Skanuj napedy***

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:.

12.11 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).

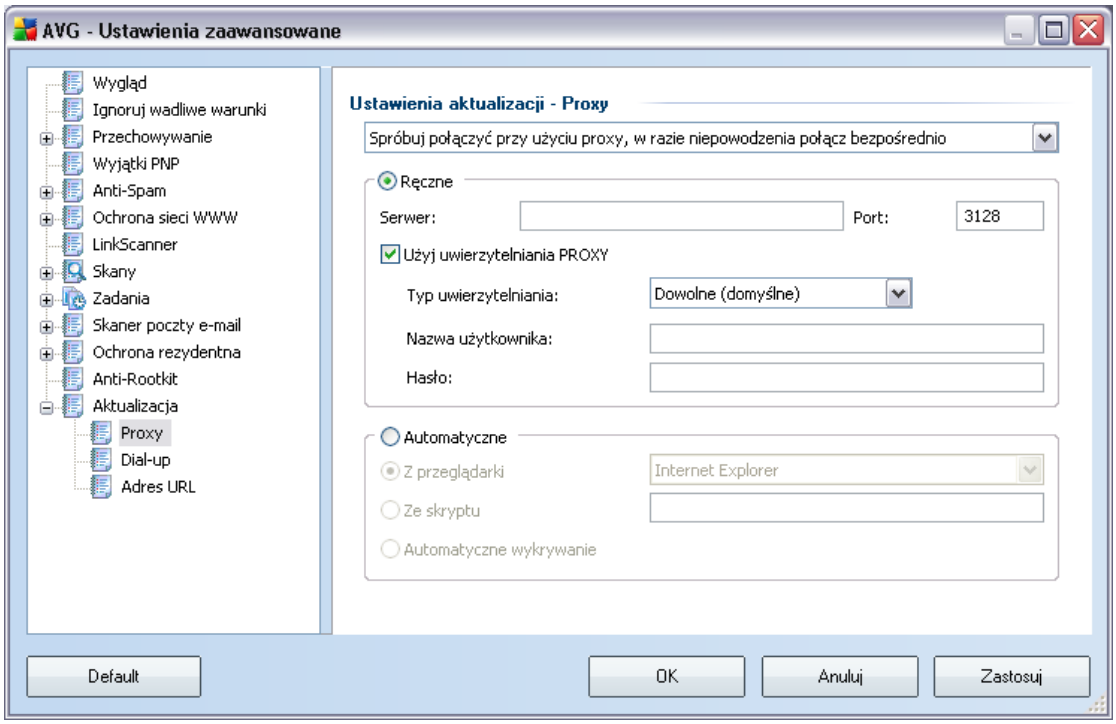
Przy pozostawienia konfiguracji domyslnej (natychmiastowe uruchomienie), mozna okreslic warunki ewentualnego restartu komputera:

- ***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 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).

Dodatkowe opcje aktualizacji

- ***Utwórz 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! Na wszelki wypadek doradzamy pozostawic to pole 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.

12.12. 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 proxy***
- ***Spróbuj polaczyc przy uzyciu proxy, w razie niepowodzenia polacz bezposrednio*** (ustawienie domyslne)

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*** — adres IP lub nazwa serwera.
- ***Port*** — 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*).

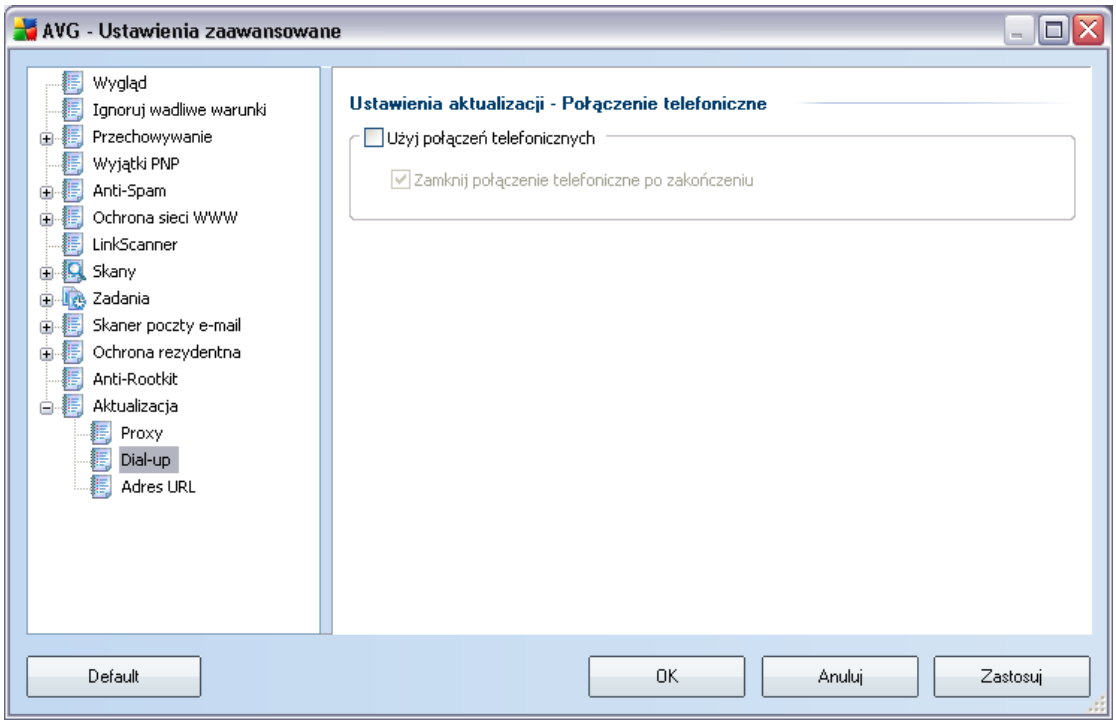
Zdarza sie, ze na serwerze proxy dla kazdego uzytkownika skonfigurowane sa odrebne reguly. Jesli serwer proxy jest skonfigurowany w ten sposób, nalezy zaznaczyc opcje ***Uzyj uwierzytelniania PROXY***, aby serwer weryfikowal nazwe uzytkownika i haslo przed nawiazaniem polaczenia.

Konfiguracja automatyczna

W przypadku wybrania konfiguracji automatycznej (*zaznaczenie opcji* ***Automatycznie*** *aktywuje odpowiednia sekcje*) nalezy wskazac, skad ma zostac pobrana konfiguracja proxy:

- ***Z przegladarki*** — konfiguracja zostanie odczytana z domyslnej przegladarki internetowej (*obslugiwane sa: Internet Explorer, Firefox, Mozilla i Opera*).
- ***Ze skryptu*** — konfiguracja zostanie odczytana z pobranego skryptu zawierajacego funkcje zwracajaca adres serwera proxy.
- ***Automatyczne wykrywanie*** — konfiguracja zostanie wykryta automatycznie bezposrednio na serwerze proxy.

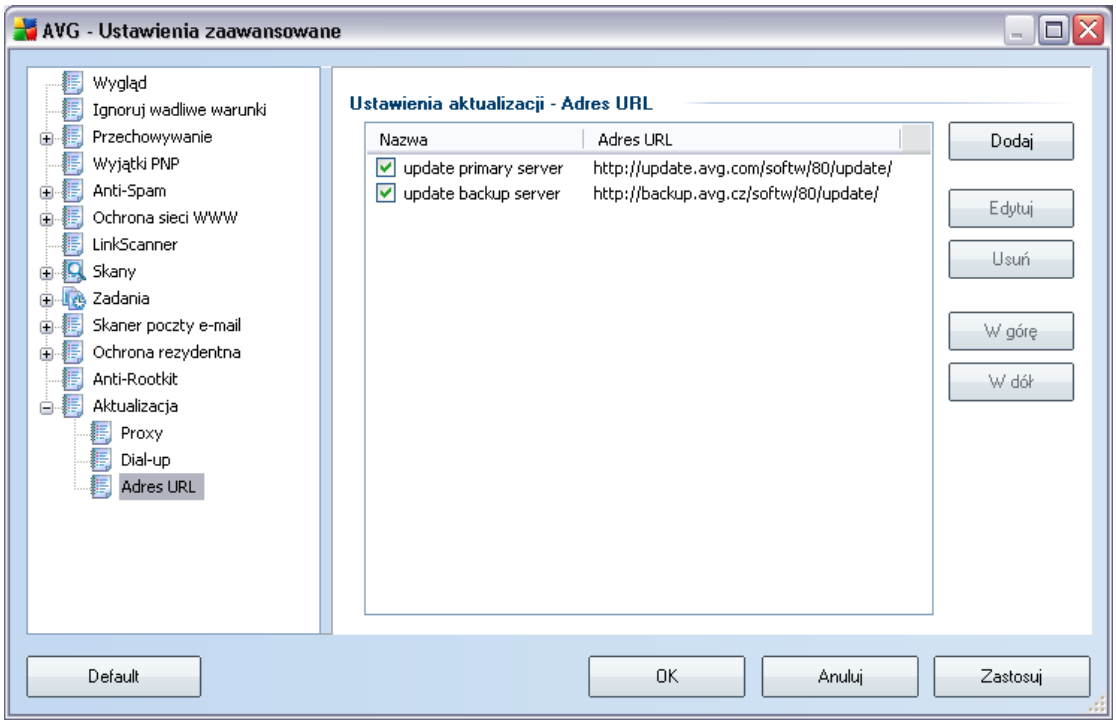
12.12.2.Polaczenie telefoniczne



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***).

12.12. 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.
- ***Domyslne*** — powoduje przywrócenie domyslnej listy adresów URL.
- ***W góre*** — przenosi wybrany adres URL o jedna pozycje w góre.
- ***W dól*** — przenosi wybrany adres URL o jedna pozycje w dól.

12.12. Zarzadzaj

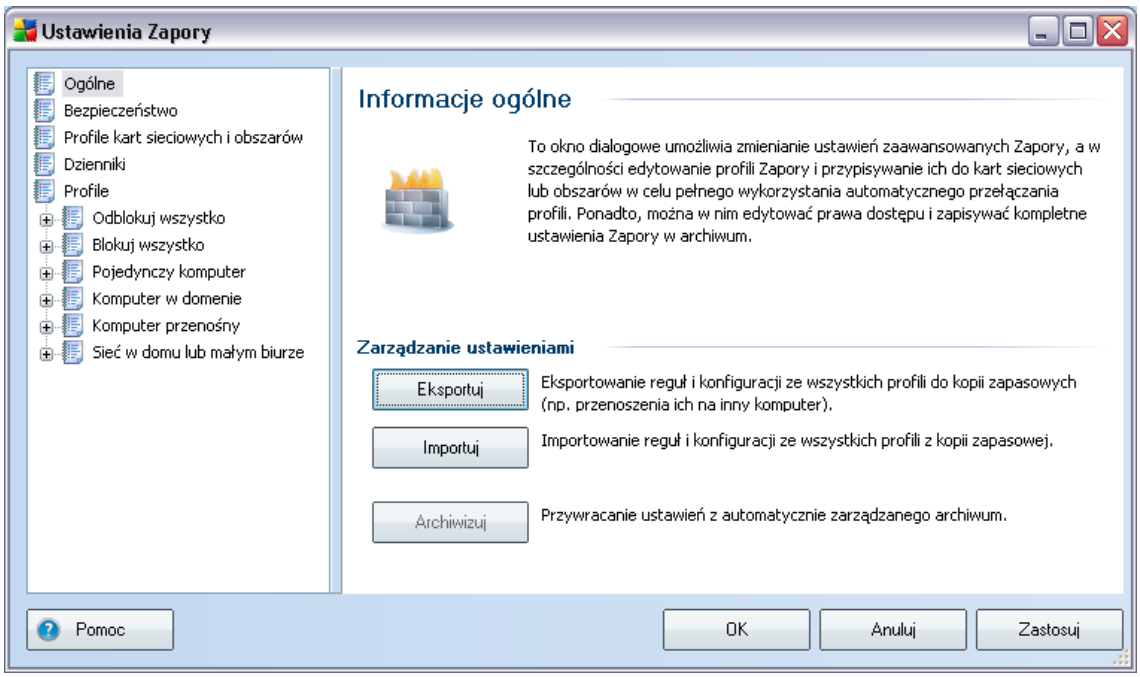
Okno dialogowe ***Zarzadzaj*** zawiera dwa przyciski:

- ***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*)

13. Ustawienia Zapory

Konfiguracja ***Zapory*** otwierana jest w nowym oknie, gdzie w kilku sekcjach mozna okreslic nawet najbardziej zaawansowane parametry tego skladnika. Edycja zaawansowanej konfiguracji powinna byc dokonywana jedynie przez fachowców i doswiadczonych uzytkowników. Zaleca sie, aby pozostali uzytkownicy zachowywali konfiguracje stworzona za pomoca ***Kreatora konfiguracji Zapory***.

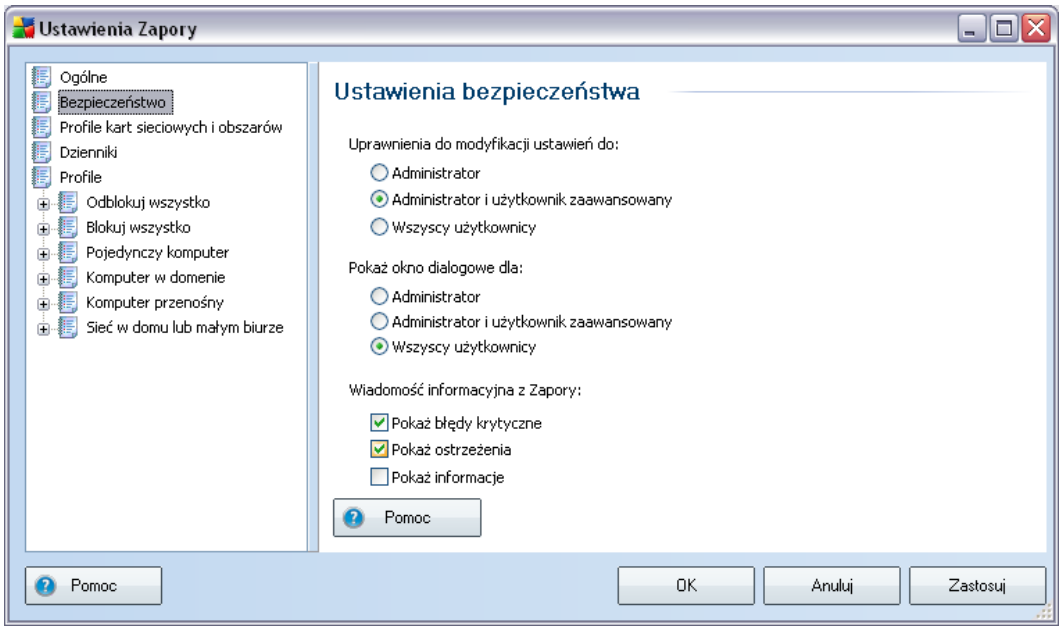
13.1.Ogólne



Na karcie ***Informacje ogólne*** mozna eksportowac/importowac lub zapisywac konfiguracje skladnika ***Firewall***:

- ***Eksport / Import*** — eksport zdefiniowanych regul i ustawien skladnika ***Firewall*** do plików kopii zapasowej albo import calego pliku kopii zapasowej.
- ***Archiwum*** — po kazdej zmianie konfiguracji skladnika ***Firewall*** cala poprzednia konfiguracja jest zapisywana w archiwum. Dostep do konfiguracji archiwalnych zapewnia przycisk ***Archiwum***. Jesli Archiwum ustawien jest puste, oznacza to, ze od momentu zainstalowania ***Zapory*** nie wprowadzono zadnych zmian w jej konfiguracji. Maksymalna liczba zapisanych konfiguracji wynosi 10. Podczas zapisywania kolejnej konfiguracji powyzej tej liczby, nadpisywana jest najstarsza z nich.

13.2.Bezpieczenstwo



W oknie ***Ustawienia bezpieczenstwa*** mozna zdefiniowac ogólne reguly zachowania ***Zapory*** niezaleznie od wybranego profilu:

- ***Pozwól modyfikowac ustawienia:*** — nalezy okreslic, kto moze zmieniac konfiguracje skladnika ***Zapora***.
- ***Pokaz okno dialogowe:*** — nalezy okreslic, komu mozna wyswietlac okna potwierdzen Zapory (*okna dialogowe z prosba o podjecie decyzji w sytuacji nieobjetej zadna regula* ***Zapory***).

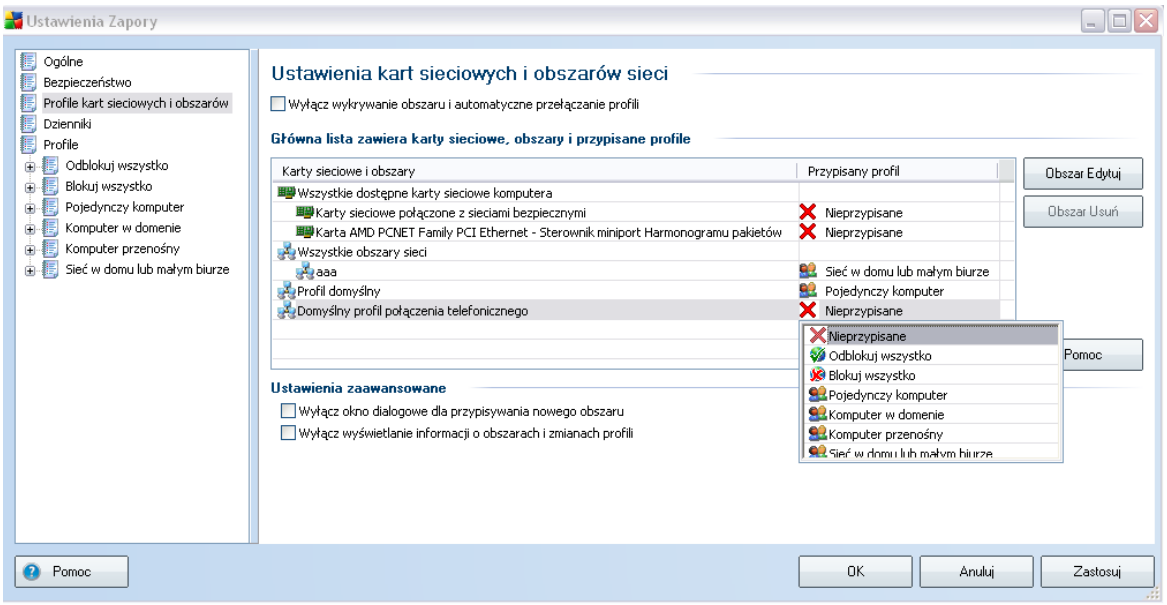
W obu wypadkach mozna przypisac konkretne uprawnienie jednej z nastepujacych grup uzytkowników:

- ***Administratorom*** — posiadaja oni calkowita kontrole nad komputerem i mozliwosc przydzielania uzytkowników do grup z okreslonymi uprawnieniami.
- ***Administratorom i uzytkownikom uprzywilejowanym*** — administrator moze przydzielic dowolnego uzytkownika do uprzywilejowanej grupy (*Uzytkownicy uprzywilejowani*) oraz okreslic uprawnienia jej czlonków.

- **Wszyscy uzytkownicy** — pozostali uzytkownicy (nie przydzieleni do zadnej konkretnej grupy).

- ***Wiadomosci informacyjne Zapory*** — nalezy okreslic, które wiadomosci generowane przez ***Zapore*** maja byc wyswietlane — zaleca sie wyswietlanie bledów krytycznych i ostrzezen, natomiast do decyzji uzytkownika pozostawia sie wyswietlanie zwyklych wiadomosci informacyjnych.

13.3.Profile kart sieciowych i obszarów



W oknie ***Ustawienia kart sieciowych i obszarów*** mozna edytowac ustawienia zwiazane z przypisywaniem zdefiniowanych profili do konkretnych kart i sieci.

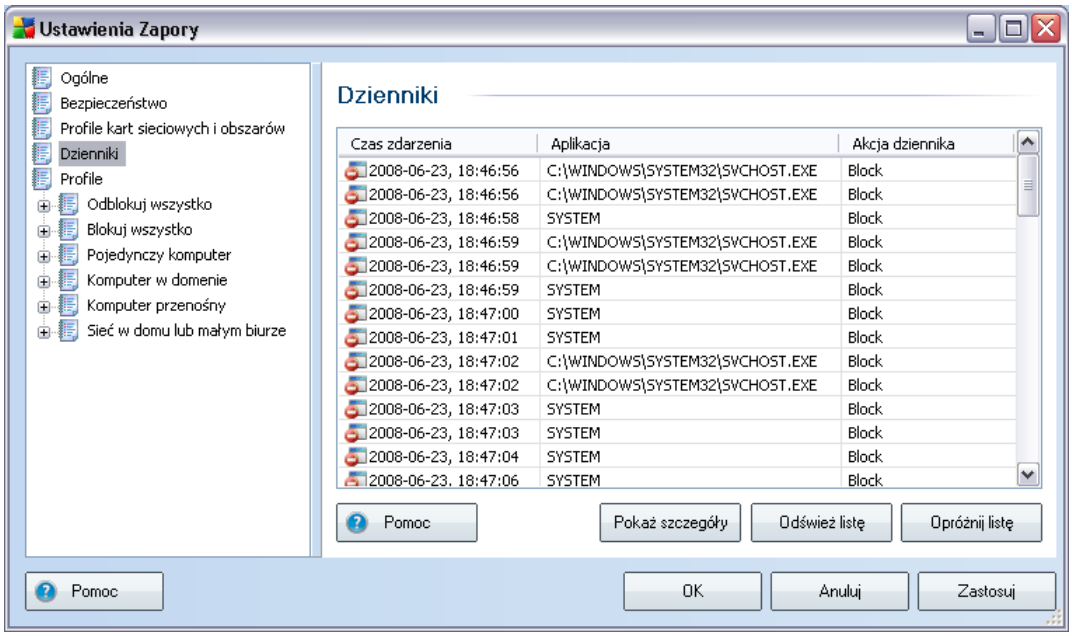
- ***Wylacz wykrywanie obszaru i automatyczne przelaczanie profili*** — do kazdej karty sieciowej (lub zdefiniowanej sieci) mozna przypisac jeden z profili Zapory. Jesli nie chcesz definiowac konkretnych profili, zostanie uzyty jeden wspólny profil zdefiniowany podczas dzialania ***Kreatora konfiguracji Zapory*** . Jesli jednak uzytkownik postanowi rozrózniac profile i przypisac je do konkretnych kart i obszarów, a nastepnie — z jakiegos powodu — postanowi tymczasowo przelaczyc to przypisanie, nalezy zaznaczyc opcje ***Wylacz wykrywanie obszaru i automatyczne przelaczanie profili***.

- ***Lista kart sieciowych, obszarów i przypisanych profili*** — na tej liscie mozna znalezc przeglad wykrytych kart i obszarów. Do kazdej karty lub sieci mozna przypisac konkretny profil z menu zdefiniowanych profili (*wszystkie*

*profile byly pierwotnie zdefiniowane w **Kreatorze konfiguracji Zapory**, ale nawet pózniej mozna utworzyc je w sekcji **Profile** ustawien Zapory*). Aby otworzyc to menu, kliknij odpowiedni element na liscie kart sieciowych i wybierz profil.

- ***Ustawienia zaawansowane*** — zaznaczenie odpowiednich opcji spowoduje wylaczenie wyswietlania komunikatu z informacjami.

13.4.Dzienniki



Okno dialogowe ***Dzienniki*** umozliwia przegladanie listy wszystkich zarejestrowanych dzialan ***Zapory***, ze szczególowym opisem odpowiednich parametrów:

- ***Czas zdarzenia*** —dokladna data i godzina wystapienia zdarzenia.
- ***Aplikacja*** — nazwa procesu, do którego odnosi sie zarejestrowane zdarzenie.
- ***Akcja*** — typ wykonanej akcji.

Dostepne sa nastepujace przyciski sterujace:

- ***Pomoc*** — otwiera okno dialogowe z powiazanymi tematami pomocy.
- ***Pokaz szczegóły*** — jesli podane parametry okaza sie niewystarczajace i

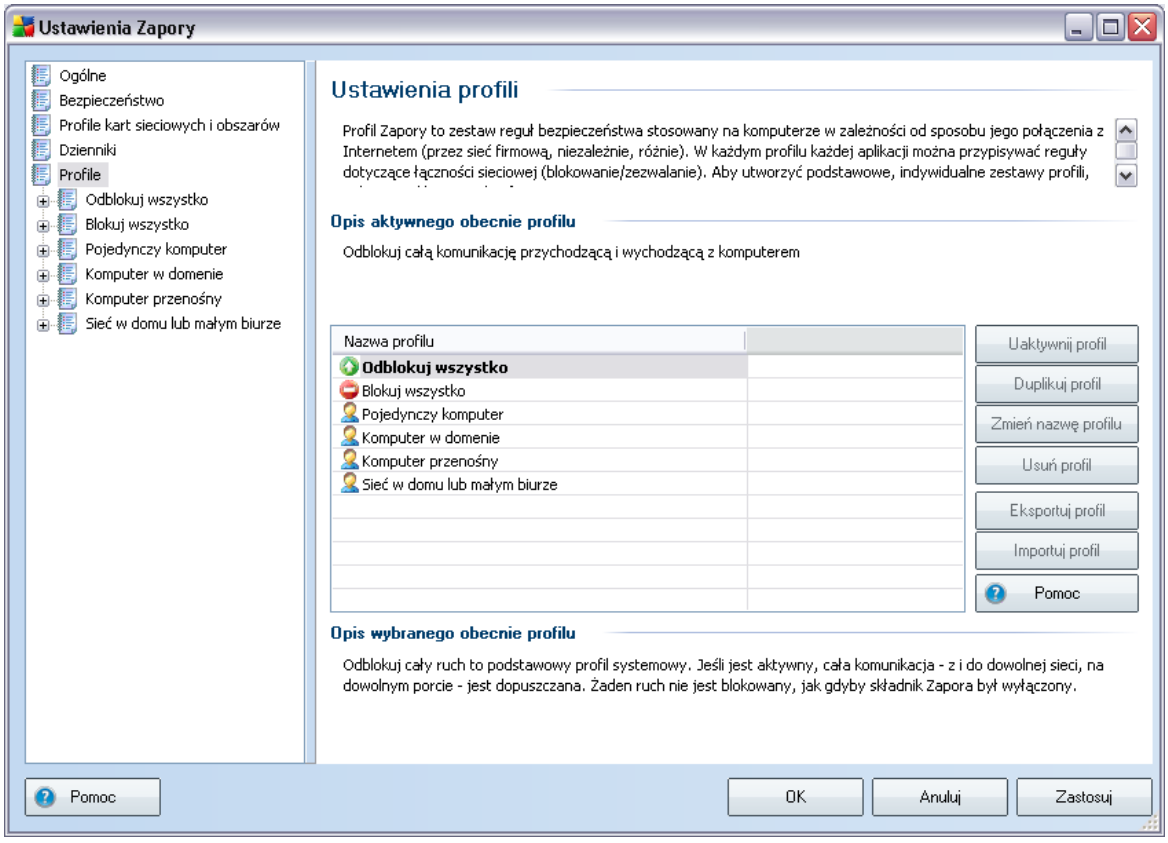
potrzeba wiecej informacji, nalezy uzyc tego przycisku, aby przelaczyc sie do zaawansowanego przegladu pliku dziennika zwierajacego dodatkowe informacje (na temat uzytkownika, identyfikatora procesu, kierunek, protokół, port zdalny/lokalny, zdalny/lokalny adres IP).

- ***Odswiez liste*** — wszystkie zarejestrowane parametry mozna uporzadkowac wedlug wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) — wystarczy kliknac odpowiedni naglówek kolumny. Nalezy uzyc przycisku ***Odswiez liste***, aby zaktualizowac aktualnie wyswietlane informacje.

- ***Opróznij liste*** — pozwala usunac wszystkie wpisy.

13.5.Profile

W oknie dialogowym ***Ustawienia profilu*** mozna znalezc liste dostepnych profili.



Wszystkie pozostale profile moga byc nastepnie edytowane w tym oknie dialogowym przy uzyciu nastepujacych przycisków sterujacych:

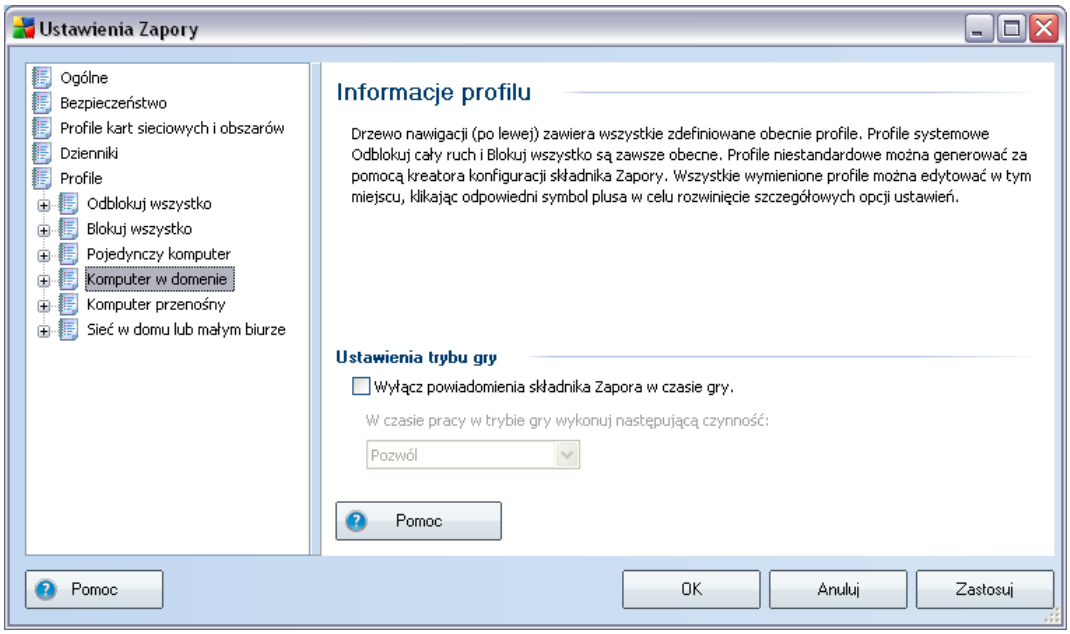
- ***Uaktywnij profil*** — przycisk ten ustawia wybrany profil jako aktywny, co oznacza, ze konfiguracja wybranego profilu bedzie uzywana przez ***Zapore*** do sterowania ruchem w sieci.
- ***Duplikuj profil*** — tworzy kopie wybranego profilu. Później bedzie mozna przeprowadzic edycje i zmienic nazwe kopii, aby utworzyc nowy profil na podstawie istniejacego.
- ***Zmien nazwe profilu*** — umozliwia zdefiniowanie nowej nazwy dla wybranego profilu.

- ***Usun profil*** — usuwa wybrany profil z listy.
- ***Eksportuj profil*** — zapisuje konfiguracje wybranego profilu w pliku, którego bedzie mozna uzyc w przyszlosci.
- ***Importuj profil*** — konfiguruje ustawienia wybranego profilu na podstawie danych zapisanych w pliku konfiguracyjnym.
- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

W dolnej czesci okna dialogowego mozna znalezc opis profilu wybranego z powyzszej listy.

Menu nawigacyjne znajdujace sie po lewej stronie zmienia odzwierciedla liste profili wyswietlona w oknie ***Profile***. Kazdy zdefiniowany profil tworzy jedna galaz nalezaca do grupy ***Profile***. Konkretne profile mozna edytowac w kolejnych oknach dialogowych (*identycznych dla wszystkich profili*).

13.5.1.Informacje o profilu



Okno ***Informacje profilu*** to pierwszy etap sekcji, w której mozna edytowac konfiguracje wybranego profilu.

Wlacz obsluge sieci maszyn wirtualnych — zaznaczenie tej pozycji pozwala

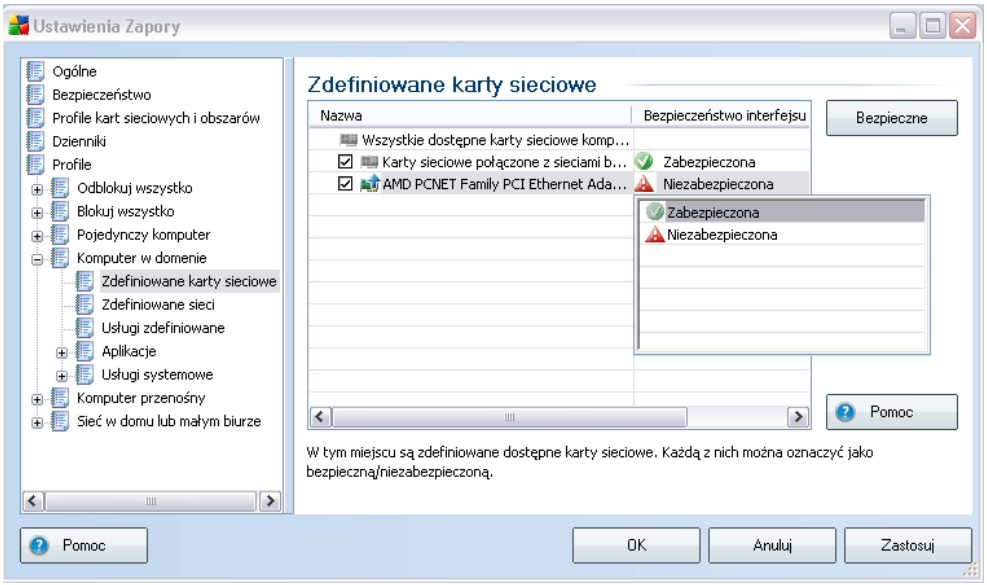
maszynom wirtualnym WMware laczyc sie bezposrednio z siecia

Ustawienia trybu gry

W sekcji ***Ustawienia trybu gry*** mozna okreslic czy komunikaty ***Zapory*** maja byc wyswietlane nawet podczas dzialania aplikacji pelnoekranowych (*sa to na ogól gry, ale dotyczy to równiez wszelkich innych aplikacji, takich jak np. prezentacje PPT*). Poniewaz takie komunikaty moga w pewnym stopniu przeszkadzac w pracy, sa one domyslnie wylaczone.

Jesli zostanie zaznaczona opcja ***Wylacz powiadomienia skladnika Zapora w czasie gry***, z menu rozwijanego znajdujacego sie ponizej nalezy wybrac akcje, która ma podjac Zapora, gdy nowa aplikacja spróbuje nawiazac polaczenie z siecia (*aby nie wyswietlac komunikatu z pytaniem o dostep*). Wszystkie takie aplikacje moga byc odblokowane lub zablokowane.

13.5.2.Zdefiniowane karty sieciowe



Okno dialogowe ***Zdefiniowane karty sieciowe*** zawiera liste wszystkich kart sieciowych wykrytych w komputerze. Kazda siec odpowiada okreslonej karcie sieciowej (aby wyswietlic liste sieci, przejdz do ekranu ***Zdefiniowane sieci***.

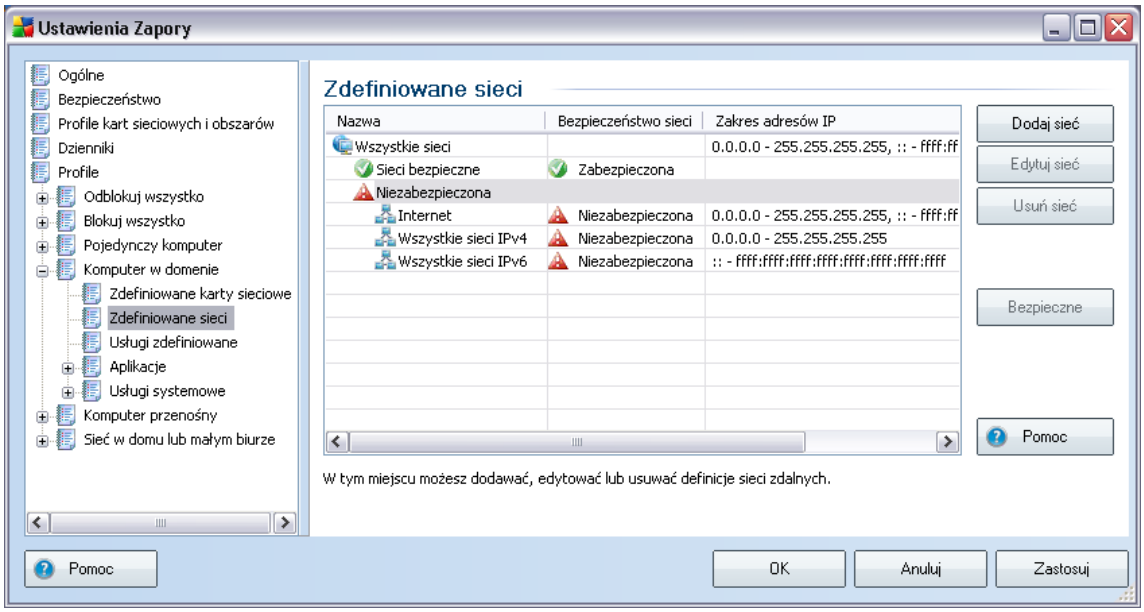
Dla kazdej wykrytej karty sieciowej wyswietlane sa nastepujace informacje:

- ***Karty sieciowe*** — zawiera liste nazw wszystkich wykrytych kart uzywanych przez komputer do laczenia sie z okreslonymi sieciami

- ***Bezpieczenstwo interfejsu*** — *domyslnie wszystkie karty sieciowe sa uwazane za niebezpieczne i tylko w przypadku pewnosci, ze dana karta sieciowa (i odpowiednia siec) jest godna zaufania, mozna przypisac jej takie ustawienie (w tym celu nalezy kliknac na liscie pozycje odpowiadajaca tej karcie i wybrac z menu kontekstowego opcje Zabezpieczona, badz kliknac przycisk* ***Bezpieczne***). Wszystkie bezpieczne karty sieciowe i odpowiadajace im sieci zostana wziete pod uwage przy przyznawaniu dostepu aplikacjom, dla których zastosowano regule Pozwól bezpiecznym

- ***Zakres adresów IP*** — kazda siec (odpowiadajaca danej karcie sieciowej) zostanie automatycznie wykryta i okreslona w formie zakresu adresów IP

13.5.3.Zdefiniowane sieci



Okno ***Zdefiniowane sieci*** zawiera liste wszystkich sieci, z którymi polaczony jest Twój komputer. Kazda siec odnosi sie do konkretnej karty sieciowej — lista wszystkich kart znajduje sie w oknie ***Zdefiniowane karty sieciowe***

Dla kazdej wykrytej sieci wyswietlane sa nastepujace informacje:

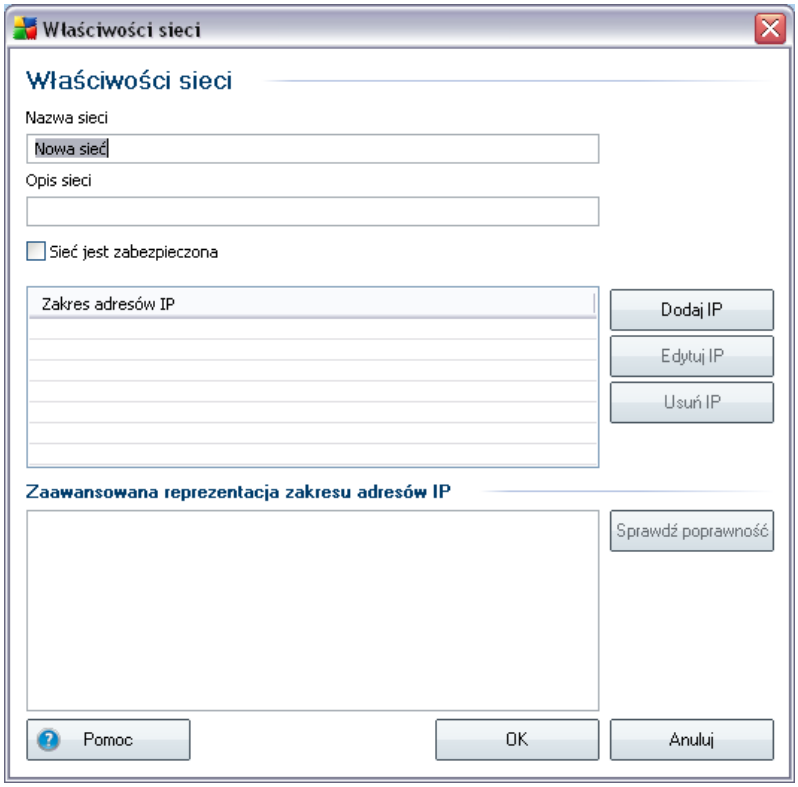
- ***Sieci*** — lista nazw wszystkich sieci, do których podlaczony jest komputer.

- ***Bezpieczenstwo sieci*** *— domyslnie wszystkie sieci uwazane sa za niebezpieczne i tylko w przypadku pewnosci, ze dana siec (i odpowiednia karta sieciowa) jest godna zaufania, mozna przypisac jej takie ustawienie (w tym celu nalezy kliknac na liscie pozycje odpowiadajaca tej sieci i wybrac z menu kontekstowego opcje Zabezpieczona, badz kliknac przycisk Bezpieczne*). Wszystkie bezpieczne karty sieciowe i odpowiadajace im sieci zostana wziete pod uwage przy przyznawaniu dostepu aplikacjom, dla których zastosowano regule Pozwól bezpiecznym

- ***Zakres adresów IP*** — kazda siec zostanie automatycznie wykryta i okreslona w formie zakresu adresów IP

Przyciski kontrolne

- ***Dodaj siec*** — otwiera okno ***Wlasciwosci sieci*** , w którym mozna edytowac parametry nowo zdefiniowanej sieci.



Nalezy wówczas okreslic ***Nazwe sieci***, podac ***Opis sieci*** i zdecydowac, czy

jest zabezpieczona. Adres sieci moze byc okreslony recznie w odrebnym oknie dialogowym otwieranym za pomoca przycisku ***Dodaj adres IP*** (mozna tez uzyc przycisków ***Edytuj adres IP***/***Usun adres IP***). W oknie tym nalezy okreslic siec, podaja zakres adresów IP lub maske.

W wypadku duzej liczby sieci, które maja byc zdefiniowane jako czesci nowo utworzonej sieci, mozna uzyc opcji ***Zaawansowana reprezentacja zakresu adresów IP***: nalezy w tym celu wpisac liste wszystkich sieci do odpowiedniego pola tekstowego (*obslugiwane sa wszystkie standardowe formaty*) i kliknac przycisk ***Sprawdz***, aby upewnic sie, ze format zostal rozpoznany. Nastepnie nalezy kliknac przycisk ***OK***, aby potwierdzic i zapisac dane.

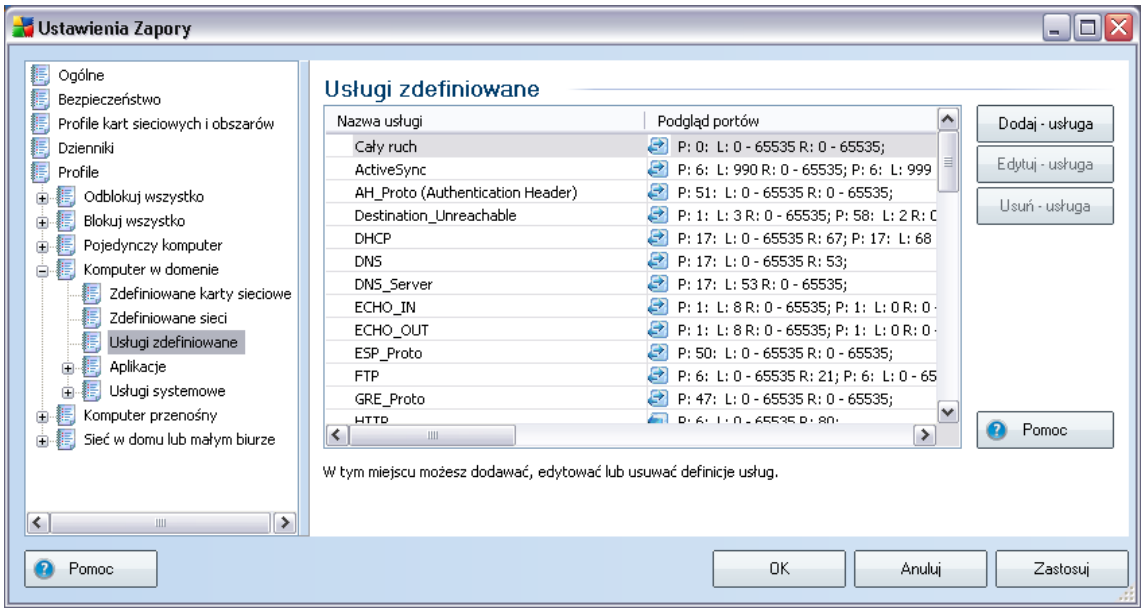
- ***Edytuj siec*** — powoduje otwarcie okna dialogowego ***Wlasciwosci sieci*** (*patrz wyzej*). w którym mozna edytowac parametry zdefiniowanej sieci (*okno to jest identyczne jak podczas dodawania nowej sieci. Zobacz opis w poprzednim akapicie*).

- ***Usun siec*** — usuwa wybrana siec z listy sieci.

- ***Oznacz jako zabezpieczona*** — domyslnie wszystkie sieci uwazane sa za niebezpieczne i tylko w przypadku pewnosci, ze dana siec (i odpowiednia karta sieciowa) jest godna zaufania, mozna przypisac jej takie ustawienie.

- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

13.5.4.Zdefiniowane uslugi



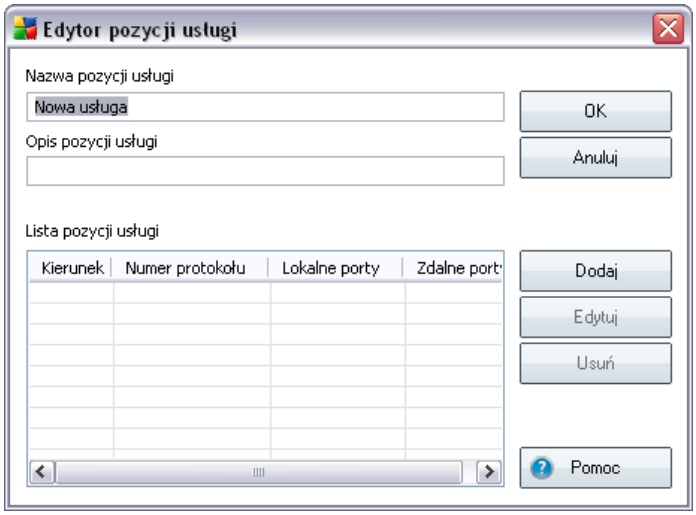
Okno dialogowe ***Uslugi zdefiniowane*** zawiera liste wszystkich uslug zdefiniowanych dla aplikacji w konfiguracji domyslnej oraz uslugi zdefiniowane wczesniej przez uzytkownika. Okno dialogowe jest podzielone na dwie kolumny:

- ***Nazwa uslugi*** — okresla nazwe uslugi.
- ***Podglad portów*** — strzalki okreslaja kierunek komunikacji (przychodzaca/ wychodzaca); podawany jest takze numer lub nazwa uzywanego protokolu (P), oraz numer lub zakres numerów uzywanych portów lokalnych (L) i zdalnych (Z).

Konkretne uslugi mozna dodawac, edytowac lub usuwac.

Przyciski kontrolne

- ***Dodaj usluge*** — powoduje otwarcie okna ***Edytor pozycji uslugi***, w którym mozna zdefiniowac parametry dodawanej uslugi.

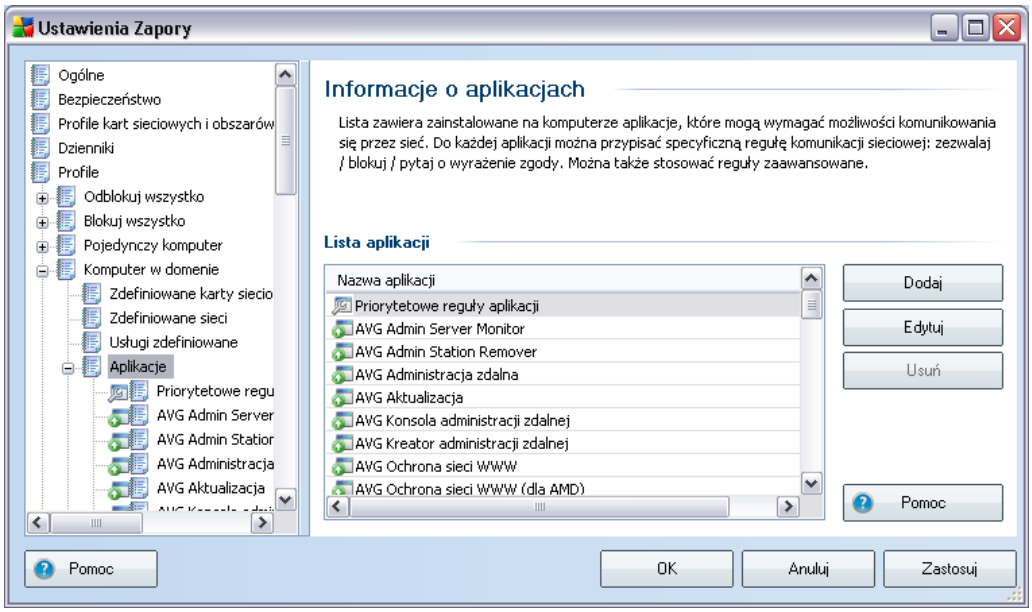


Nalezy w tym celu okreslic ***Nazwe pozycji uslugi*** oraz podac krótki ***Opis pozycji uslugi***. W sekcji ***Lista pozycji uslugi*** mozna nastepnie dodac (*a takze edytowac lub usunac*) pozycje uslugi, okreslajac nastepujace parametry:

- ***Kierunek*** — przychodzacy, wychodzacy lub w obie strony.
- ***Numer protokolu*** — typ protokolu (*nalezy wybrac z menu*).
- ***Lokalne porty*** — lista zakresów portów lokalnych.
- ***Zdalne porty*** — lista zakresów portów zdalnych.

- ***Edytuj usluge*** — powoduje otwarcie okna ***Edytor pozycji uslugi*** (*patrz wyzej*), w którym mozna edytowac parametry zdefiniowanej sieci (*okno to jest identyczne jak w przypadku dodawania nowej uslugi - zobacz opis w poprzednim akapicie*).
- ***Usun usluge*** — usuwa wybrana usluge z listy.
- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

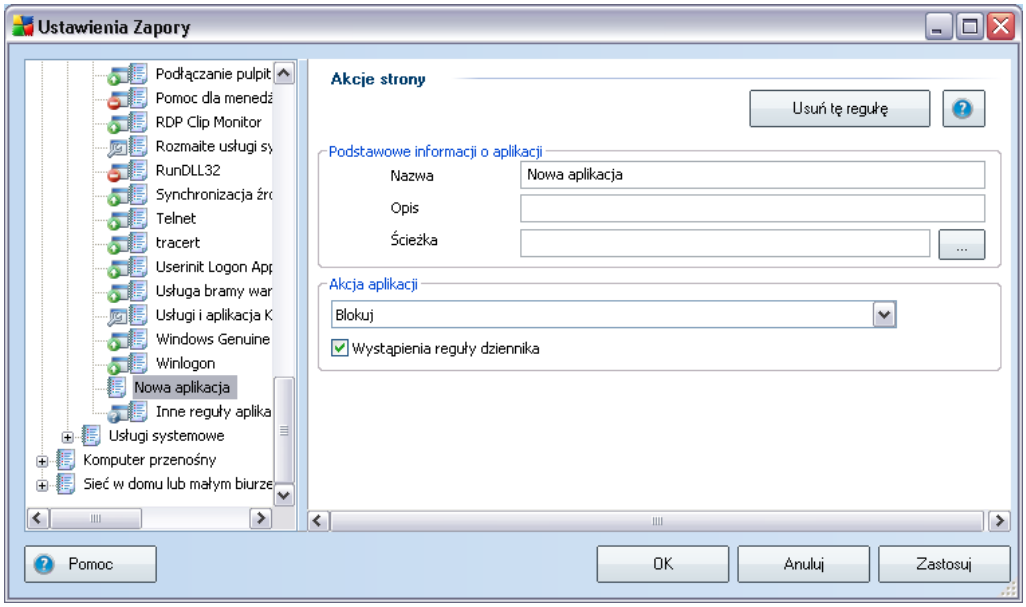
13.5.5.Aplikacje



W oknie ***Informacje o aplikacjach*** mozna znalezc przeglad wszystkich aplikacji komunikujacych sie za posrednictwem sieci, które zostaly wykryte na komputerze w czasie dzialania ***Kreatora konfiguracji Zapory*** (podczas procesu wyszukiwania w oknie ***Skanuj w poszukiwanie aplikacji internetowych*** lub w dowolnym pózniejszym momencie). Liste mozna edytowac przy uzyciu nastepujacych przycisków kontrolnych:

- ***Dodaj*** — otwiera okno sluzace do definiowania nowego zbioru regul aplikacji.
- ***Edytuj*** — otwiera okno sluzace do edytowania istniejacego zbioru regul aplikacji.
- ***Usun*** — usuwa wybrany zbiór regul z listy.
- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

Okno dialogowe sluzace do dodania nowej reguly aplikacji otwierane jest za pomoca przycisku ***Dodaj*** w sekcji ***Aplikacje*** **(**w ***ustawieniach Zapory***):



W oknie tym mozna zdefiniowac:

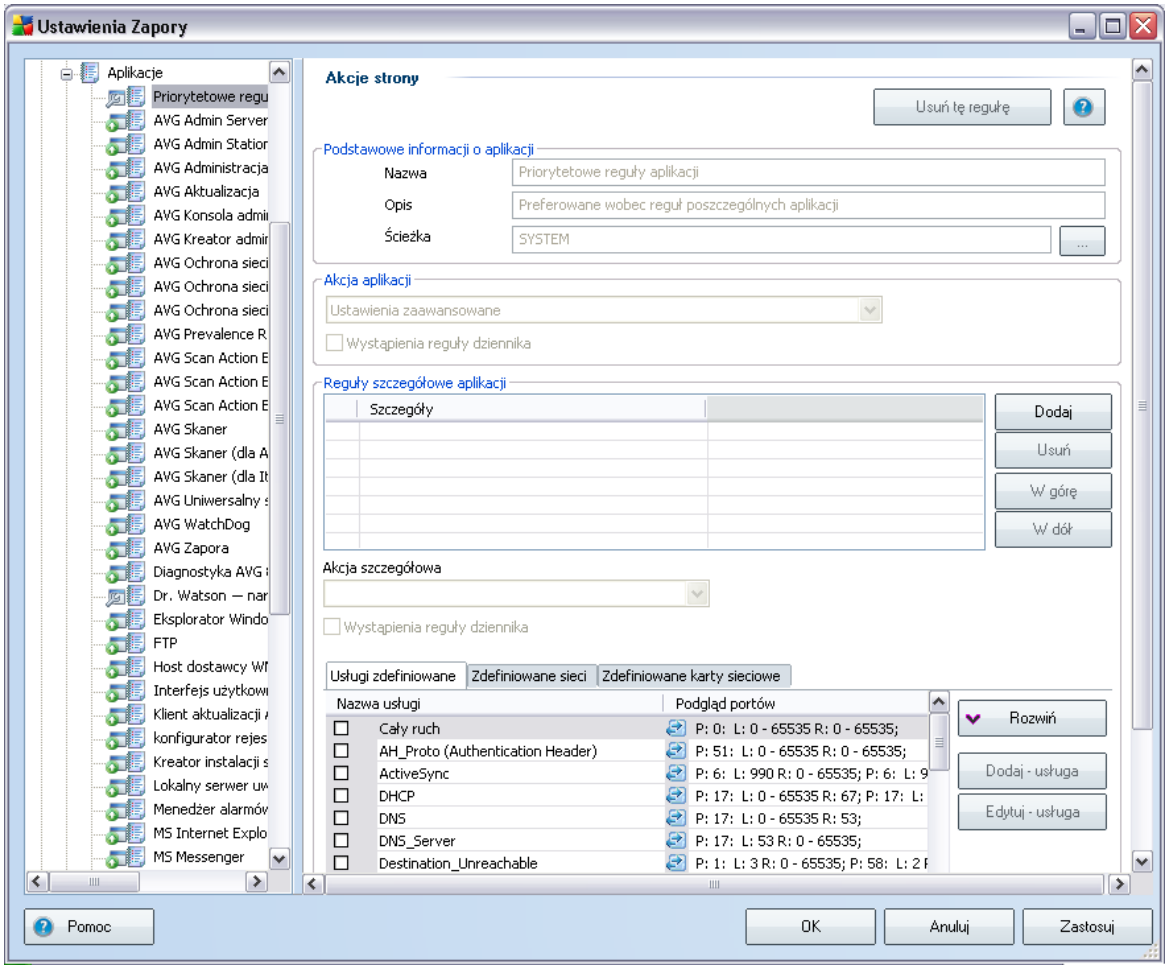
- ***Podstawowe informacji o aplikacji*** — nazwa aplikacji, jej krótki opis i lokalizacja na dysku.
- ***Akcja aplikacji*** — z menu rozwijanego mozna wybrac regule, która ma byc stosowana do danej aplikacji.
  - ***Ustawienia zaawansowane —*** opcja ta umozliwia szczególowa edycje zbioru regul obecnych w dolnej czesci okna dialogowego. *Opis tej sekcji znajduje sie w rozdziale* ***Edycja aplikacji****.*
  - ***Pozwól —*** wszelkie próby nawiazania komunikacji przez ta aplikacje beda dozwolone.
  - ***Pozwól bezpiecznym —*** aplikacja bedzie mogla komunikowac sie wylacznie z bezpiecznymi sieci (*np. polaczenia z chroniona siecia firmowa beda dozwolone, natomiast komunikacja z internetem - zablokowana*). Omówienie i opis bezpiecznych sieci znajduje sie w oknie ***Sieci***.

- ***Pytaj —*** jesli aplikacja podejmie próbe komunikacji przez siec, zostanie wyswietlony monit pytajacy uzytkownika o zgode.

- ***Blokuj —*** wszelkie próby komunikacji podejmowane przez aplikacje beda zablokowane.

- ***Rejestruj stosowanie reguly*** — nalezy zaznaczyc te opcje, jesli wszystkie akcje ***Zapory*** podejmowane w zwiazku z dana aplikacja maja byc rejestrowane w dzienniku. Wspomniane wpisy dziennika mozna znalezc w oknie ***Dzienniki***

Okno dialogowe do definiowania zbioru regul aplikacji otwiera sie za pomoca przycisku ***Edytuj*** w oknie dialogowym ***Aplikacje*** w ***ustawieniach skladnika Firewall***:



W oknie tym mozna edytowac wszystkie parametry istniejacej aplikacji:

- ***Podstawowe informacji o aplikacji*** — nazwa aplikacji, jej krótki opis i lokalizacja na dysku.
- ***Akcja aplikacji*** — z menu rozwijanego mozna wybrac regule, która ma byc stosowana do danej aplikacji.
  - ***Ustawienia zaawansowane —*** opcja ta umozliwia szczególowa edycje reguly w dolnej czesci okna.
  - ***Pozwól —*** wszelkie próby nawiazania komunikacji przez ta aplikacje beda dozwolone.

- ***Pozwól bezpiecznym —*** aplikacja bedzie mogla komunikowac sie wylacznie z bezpiecznymi sieci (*np. polaczenia z chroniona siecia firmowa beda dozwolone, natomiast komunikacja z internetem - zablokowana*). Omówienie i opis bezpiecznych sieci znajduje sie w oknie ***Sieci***.

- ***Pytaj —*** jesli aplikacja podejmie próbe komunikacji przez siec, zostanie wyswietlony monit pytajacy uzytkownika o zgode.

- ***Blokuj —*** wszelkie próby komunikacji podejmowane przez aplikacje beda zablokowane.

- ***Rejestruj stosowanie reguly*** — nalezy zaznaczyc te opcje, jesli wszystkie akcje ***Zapory*** podejmowane w zwiazku z dana aplikacja maja byc rejestrowane w dzienniku. Wspomniane wpisy dziennika mozna znalezc w oknie ***Dzienniki***

- ***Reguly szczególowe aplikacji*** — ta sekcja jest otwierana do edycji tylko wtedy, gdy uzytkownik wczesniej wybral opcje ***Ustawienia zaawansowane*** z menu rozwijanego ***Akcja aplikacji.*** Wszystkie ustawienia szczególowe (wymienione w kolumnie ***Szczegóły***) mozna edytowac przy uzyciu nastepujacych przycisków sterujacych:

  - ***Dodaj*** — pozwala utworzyc nowa regule szczególowa dla okreslonej aplikacji. Na karcie ***Szczegóły*** wyswietlany jest nowy wpis; jego parametry nalezy okreslic, wybierajac odpowiednie sieci, z którymi aplikacja moze sie komunikowac (karta ***Sieci***), karty sieciowe, których aplikacja moze uzywac (karta ***Karty sieciowe***), oraz uslugi, które aplikacji moze wykorzystywac (karta ***Nazwa uslugi***).

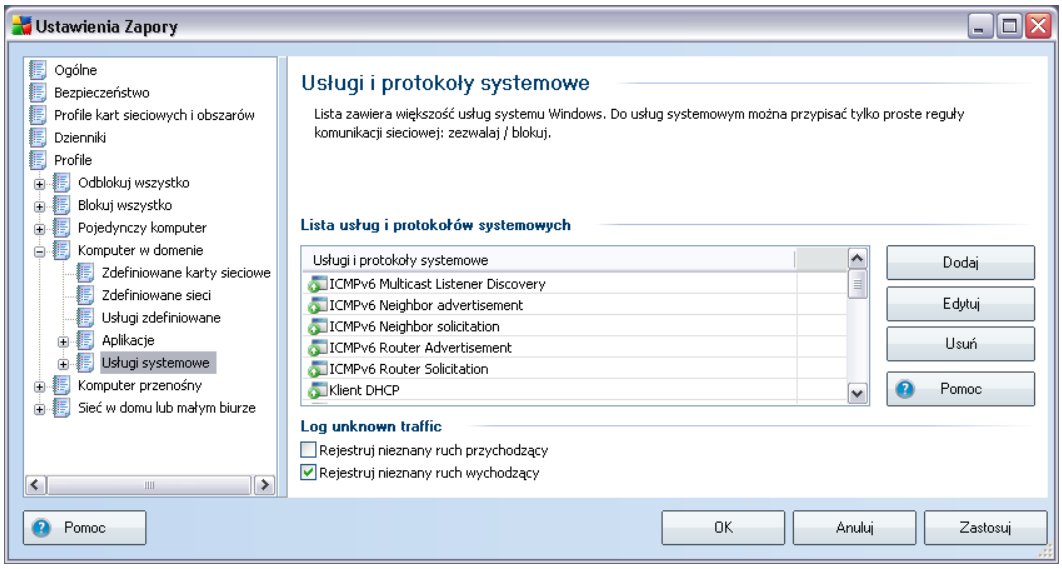
  - ***Usun*** — pozwala usunac wybrany wpis reguly szczególowej z listy.

  - ***W góre / W dól*** — reguly szczególowe sa porzadkowane wedlug priorytetu. Aby zmienic priorytet reguly szczególowej, nalezy przeniesc ja w zadane miejsce za pomoca przycisków ***W góre*** i ***W dól*** .

Kazde ustawienie szczególowe okresla ponadto, jakie beda uzywane ***zdefiniowane uslugi / zdefiniowane sieci / zdefiniowane karty sieciowe***.

13.5.6.Uslugi systemowe

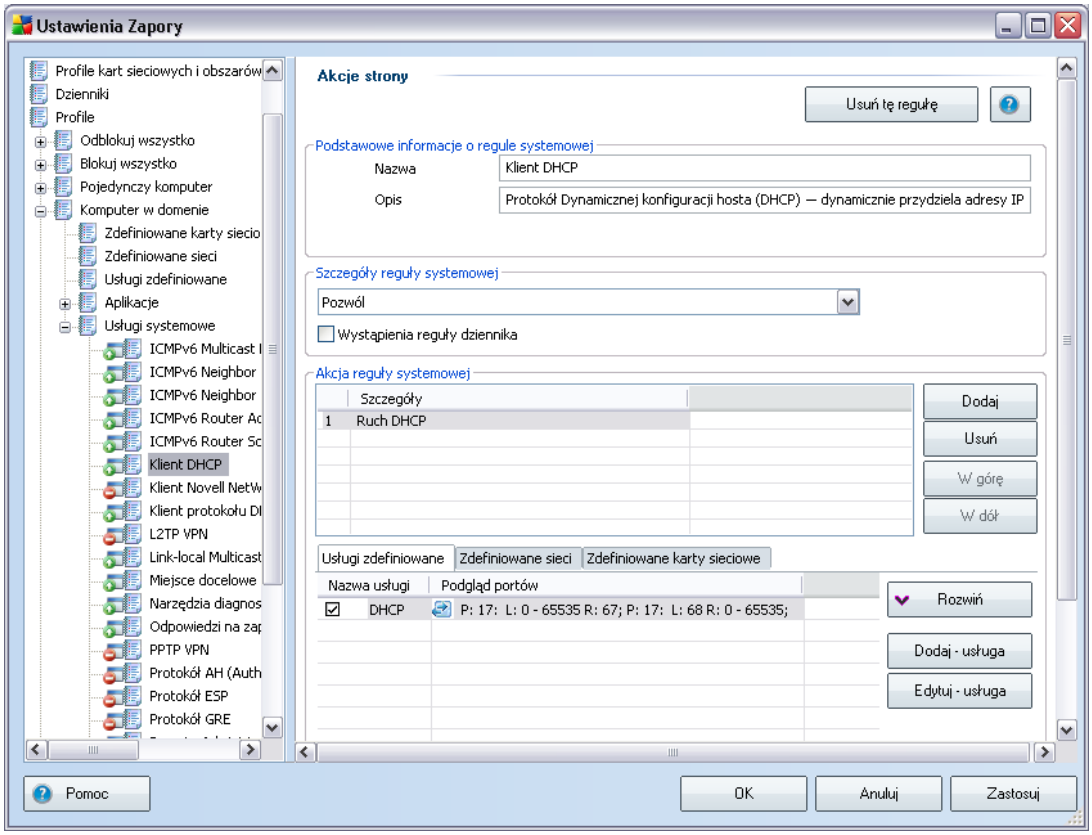
Wszelkie zmiany w konfiguracji uslug i protokolów systemowych powinny byc wprowadzane jedynie przez doswiadczonych uzytkowników.



Okno ***Uslugi i protokoly systemowe*** zawiera przeglad uslug i protokolów systemowych komunikujacych sie poprzez siec. Ponizej znajduja sie dwie opcje: nalezy je zaznaczyc, jezeli chcesz, aby rejestrowano caly nieznany ruch w obu kierunkach (*przychodzacym i wychodzacym*).

Przyciski kontrolne

- ***Dodaj/Edytuj*** — oba przyciski otwieraja to samo okno, w którym mozna edytowac parametry uslugi systemowej. Przycisk ***Dodaj*** otwiera puste okno dialogowe w trybie podstawowym (*bez sekcji ustawien zaawansowanych, która mozna otworzyc, wybierajac zaawansowane ustawienia akcji aplikacji*). Przycisk ***Edytuj*** otwiera to samo okno dialogowe wypelnione danymi dotyczacymi wybranej uslugi systemowej:



- **_Podstawowe informacji o aplikacji_** — nazwa aplikacji i jej krótki opis.

- **_Akcja aplikacji_** — z menu rozwijanego nalezy wybrac regule, która ma byc zastosowana do danej uslugi systemowej (*w porównaniu z aplikacja dla uslug systemowych sa dostepne tylko trzy akcje*):

  - **_Blokuj_** — wszelkie próby komunikacji podejmowane przez usluge systemowa beda zablokowane.

  - **_Pozwól bezpiecznym_** — usluga systemowa bedzie mogla komunikowac sie wylacznie za posrednictwem bezpiecznych sieci (*na przyklad komunikacja z chroniona siecia firmowa bedzie dopuszczona, natomiast komunikacja z internetem bedzie zablokowana*). Omówienie i opis bezpiecznych sieci znajduje sie w oknie ***Sieci***.

  - **_Pozwól wszystkim_** — wszelkie próby nawiazania komunikacji przez

usluge systemowa beda dozwolone.

- **Rejestruj stosowanie reguly** — nalezy zaznaczyc te opcje, jesli wszystkie akcje ***Zapory*** podejmowane w zwiazku z dana usluga systemowa maja byc rejestrowane w dzienniku. Wspomniane wpisy dziennika mozna znalezc w oknie ***Dzienniki***

- **Szczegóły reguly systemowej** - dla kazdej uslugi systemowej mozna okreslic bardziej szczególowe reguly w sekcji ***Reguly szczególowe aplikacji***. Wszystkie ustawienia szczególowe (wymienione na karcie ***Szczegóły***) mozna edytowac przy uzyciu nastepujacych przycisków sterujacych:

  - ***Dodaj*** — pozwala utworzyc nowa regule szczególowa dla okreslonej uslugi systemowej. Na karcie ***Szczegóły*** wyswietlany jest nowy wpis; jego parametry nalezy okreslic, wybierajac odpowiednie sieci, z którymi usluga systemowa moze sie komunikowac (karta ***Sieci***), karty sieciowe, których usluga systemowa moze uzywac (karta ***Karty sieciowe***), oraz uslugi, które usluga systemowa moze wykorzystywac (karta ***Nazwa uslugi***).

  - ***Usun*** — pozwala usunac wybrany wpis reguly szczególowej z listy.

  - ***W góre / W dól*** — reguly szczególowe sa porzadkowane wedlug priorytetu. Aby zmienic priorytet reguly szczególowej, nalezy przeniesc ja w zadane miejsce za pomoca przycisków ***W góre*** i ***W dól*** .

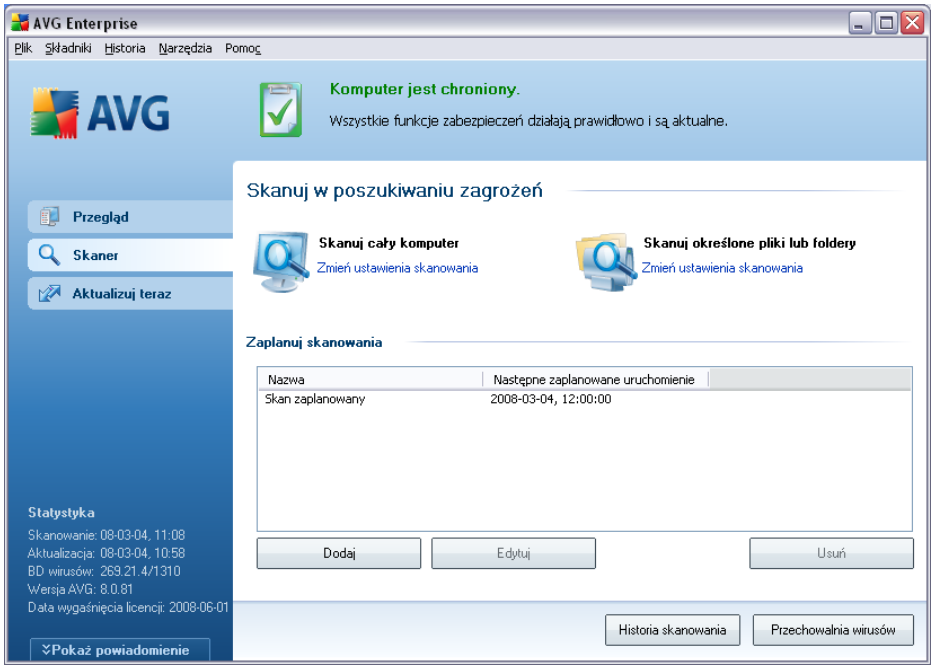
  Kazde ustawienie szczególowe okresla ponadto, jakie beda uzywane ***zdefiniowane uslugi / zdefiniowane sieci / zdefiniowane karty sieciowe***.

- ***Usun*** — usuwa z powyzszej listy wybrany wpis dotyczacy uslug systemowych.
- ***Pomoc*** — otwiera okno dialogowe z powiazanym tematem pomocy.

14. Skanowanie AVG

Skanowanie plików to podstawowa funkcja systemu **AVG 8.5 Anti-Virus plus Firewall**. Mozliwe jest uruchamianie testów na zadanie lub planowanie ich okresowego przeprowadzania o odpowiednich porach.

14.1.Interfejs skanowania



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

- Przeglad wstepnie zdefiniowanych skanów — dwa typy testów (zdefiniowane przez dostawce oprogramowania AVG) sa gotowe do uzycia na zadanie lub wedlug utworzonego planu;
- 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.

14.2.Wstepnie zdefiniowane testy

Jedna z glównych funkcji programu AVG 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.

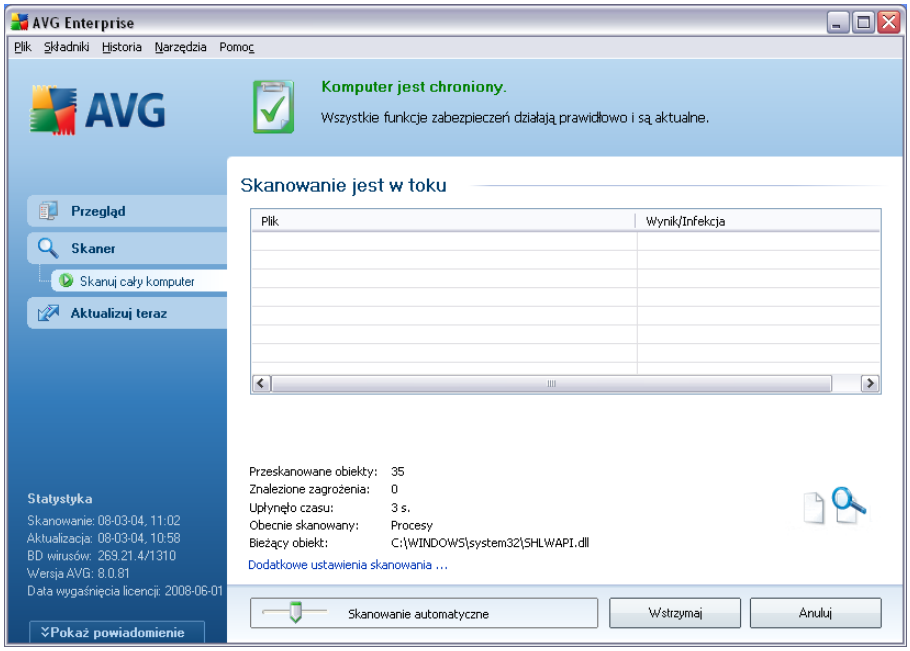
System **AVG 8.5 Anti-Virus plus Firewall**oferuje dwa typy skanowania zdefiniowane wstepnie przez AVG:

14.2.1.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.

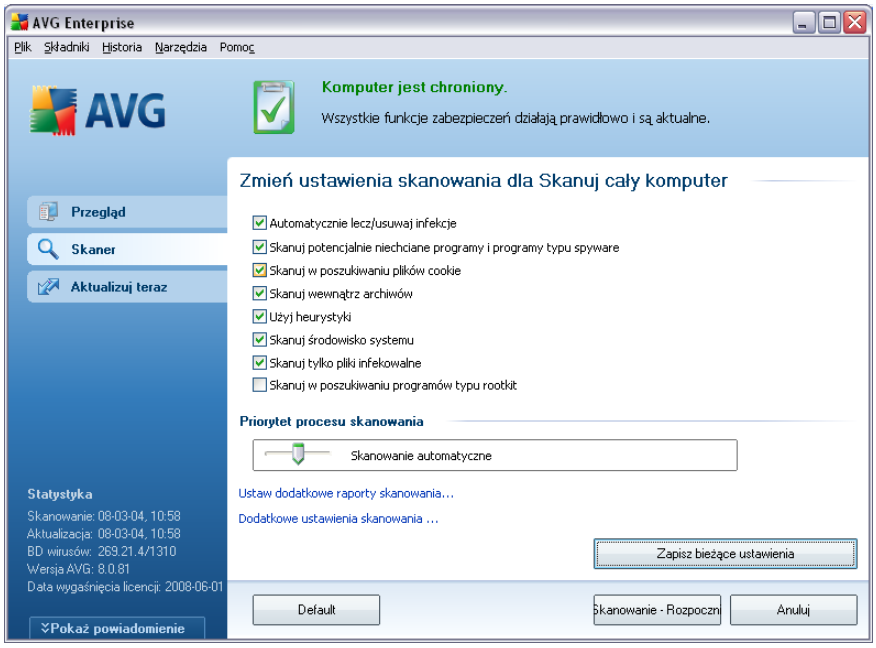
Uruchamianie skanowania

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



Edycja konfiguracji skanowania

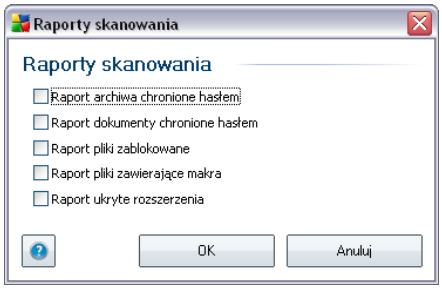
Zdefiniowane wstepne ustawienia domyslne testu ***Skan calego komputera*** mozna edytowac. Kliknieciе lacza ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***zmiany ustawien dla skanowania calego komputera***. ***Zaleca sie nie zmieniac ustawien domyslnych, jesli nie jest to konieczne!***



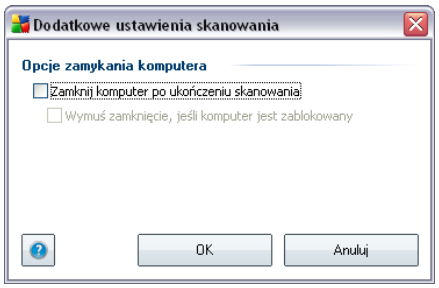
- ***Parametry skanowania*** — na liscie parametrów skanowania mozna wlaczac/ wylaczac okreslone parametry w zaleznosci od potrzeb. Wiekszosc parametrów jest domyslnie wlaczona i automatycznie uzywana podczas skanowania.

- ***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 (*przydatna, gdy komputer jest w czasie skanowania uzywany, 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*** — lacze pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic, co ma byc zglaszane:



- ***Dodatkowe ustawienia skanowania*** — lacze 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 opcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).



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 bedzie mozna zapisac jako konfiguracje domyslna, która bedzie uzywana we wszystkich zdefiniowanych w przyszlosci Skanach calego komputera.

14.2.2.Skan okreslonych plików lub folderów

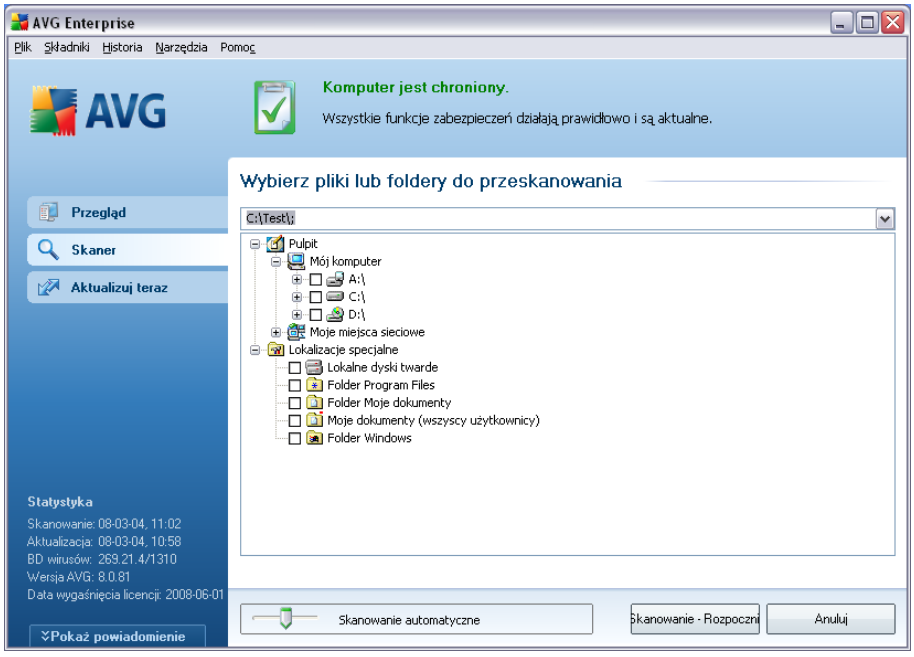
Skan okreslonych plików lub folderów — skanowane sa tylko wskazane obszary komputera (wybrane foldery, a takze dyski twarde, pamieci USB, plyty CD itd).. Postep skanowania w przypadku wykrycia wirusów i ich traktowania jest taki sam jak przy skanowaniu calego komputera: kazdy znaleziony wirus jest leczony lub przenoszony do ***Kwarantanny***. Skanowanie okreslonych plików lub folderów moze posluzyc do utworzenia wlasnych testów i planowania ich zgodnie z wlasnymi potrzebami.

Uruchamianie skanowania

Skanowanie okreslonych plików lub folderów mozna uruchomic bezposrednio w interfejsie skanowania, klikajac ikone skanowania. Wyswietlone zostanie nowe okno dialogowe ***Wybierz pliki lub foldery do przeskanowania***. W drzewie dysków komputera nalezy wybrac foldery, 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: nalezy wprowadzic znak minus „**-**” przed jego nazwe w wygenerowanej sciezce (*patrz ilustracja*). Aby wykluczyc caly folder ze skanowania, nalezy uzyc parametru „!”.

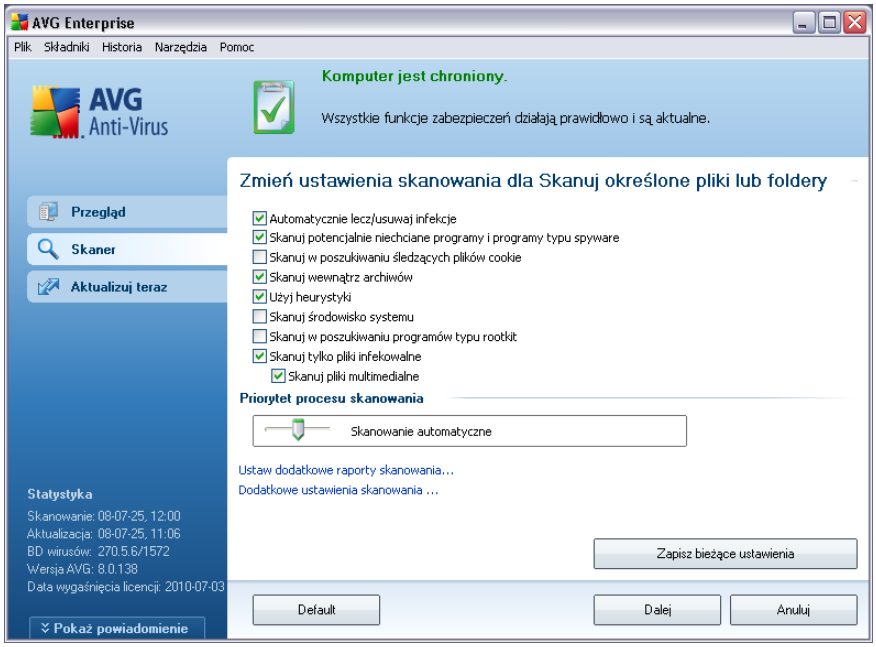
Na koniec, aby uruchomic skanowanie, nalezy nacisnac przycisk ***Rozpocznij skanowanie***; proces skanowania jest w zasadzie taki sam jak skanowanie calego komputera.



Edycja konfiguracji skanowania

Zdefiniowane wstepne ustawienia domyslne testu ***Skan okreslonych plików lub***

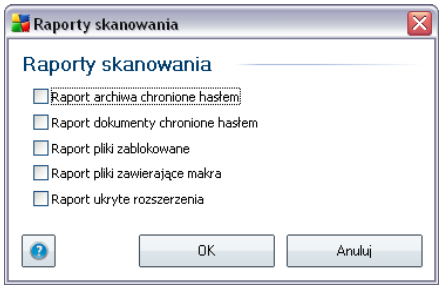
folderów mozna edytowac. Klikniecie lacza ***Zmien ustawienia skanowania*** powoduje otwarcie okna dialogowego ***zmiany ustawien dla skanowania okreslonych plików lub folderów***. ***Zaleca sie nie zmieniac ustawien domyslnych, jesli nie jest to konieczne!***



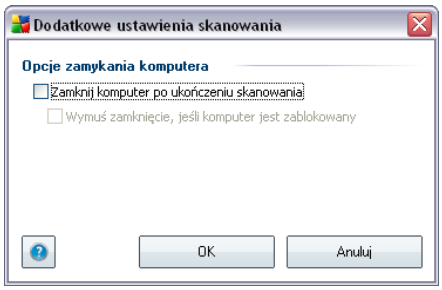
- ***Parametry skanowania*** — na liscie parametrów skanowania mozna wlaczac/ wylaczac okreslone parametry w zaleznosci od potrzeb (*szczególowy opis tych ustawien zawiera rozdzial Zaawansowane ustawienia AVG / Skany·/ Skanowanie okreslonych plików lub folderów*).

- ***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 (*przydatna, gdy komputer jest w czasie skanowania uzywany, 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*** — lacze pozwala otworzyc nowe okno dialogowe ***Raporty skanowania***, w którym mozna okreslic, co ma byc zglaszane:



- ***Dodatkowe ustawienia skanowania*** — lacze 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 opcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (***Wymus zamkniecie, jesli komputer jest zablokowany***).

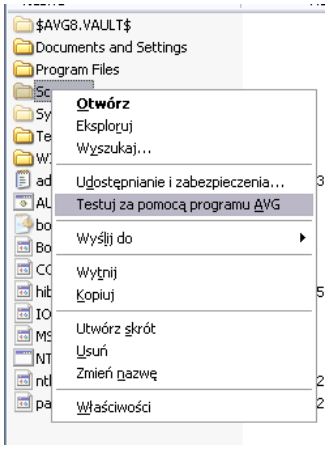


Ostrzezenie: *Ustawienia te sa identyczne jak domyslne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale* ***Skanowanie AVG / Planowanie skanowania / Jak skanowac****.*

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*).

14.3.Skan z poziomu eksploratora systemu Windows

Oprócz wstepnie zdefiniowanych testów obejmujacych caly komputer lub wybrane obszary, system AVG 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.

14.4.Skan z poziomu wiersza polecen

AVG 8.5 Anti-Virus plus Firewall oferuje mozliwosc uruchamiania skanowania z wiersza polecenia. Opcji tej mozna uzywac na przyklad na serwerach lub w czasie tworzenia skryptu wsadowego, który ma byc uruchamiany po uruchomieniu komputera. Uruchamiajac skanowanie z wiersza polecenia, mozna uzywac wiekszosci parametrów dostepnych w graficznym interfejsie uzytkownika AVG.

Aby uruchomic skanowanie z wiersza polecenia, nalezy wykonac nastepujace polecenie w folderze, w którym zainstalowano system:

- ***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*** dla skanowania 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:***

Skanuj pliki w

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 szczegółowe informacje na temat opcji zawiera przeglad parametrów wiersza polecenia.

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

Skanowanie z wiersza polecenia uruchamiane za pomoca interfejsu graficznego

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

Poniewaz okno to jest dostepne tylko w trybie awaryjnym Windows, jego szczegółowy opis zawiera plik pomocy dostepny bezposrednio z okna.

14.4.1.Parametry skanowania z wiersza polecen

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

- ***/SCAN*** Skanuj okreslone pliki lub foldery /SCAN=sciezka;sciezka (np. /SCAN=C:\;D:\)

- ***/COMP*** Skanuj caly komputer

- ***/HEUR*** Uzyj analizy heurystycznej
- ***/EXCLUDE*** Nie skanuj sciezki lub plików
- ***/@*** Plik polecenia /nazwa pliku/
- ***/EXT*** Skanuj te rozszerzenia /na przyklad EXT=EXE,DLL/
- ***/NOEXT*** Nie skanuj tych rozszerzen /na przyklad NOEXT=JPG/
- ***/ARC*** Sprawdzaj archiwa
- ***/CLEAN*** Usuwaj automatycznie
- ***/TRASH*** Przenies zainfekowane pliki do Kwarantanny
- ***/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

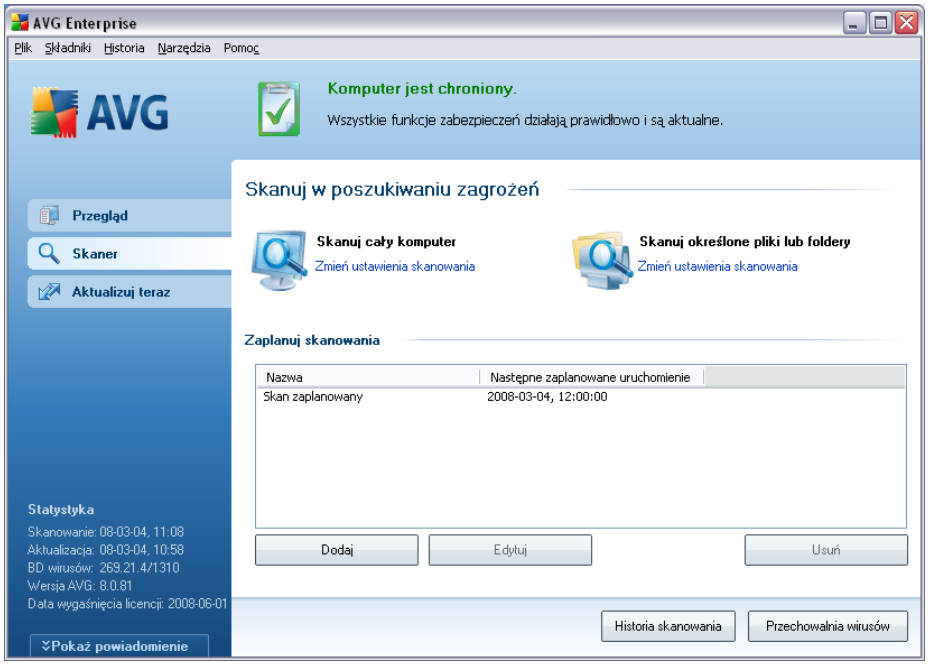
- ***/PRIORITY*** Ustaw priorytet skanowania /Niski, Auto, Wysoki/ (zobacz:·Ustawienia zaawansowane / Skany)
- ***/SHUTDOWN*** Zamknij komputer po ukonczeniu skanowania
- ***/FORCESHUTDOWN*** Wymus zamkniecie komputera po ukonczeniu skanowania
- ***/ADS*** Skanuj alternatywne strumienie danych (tylko NTFS)

14.5.Planowanie skanowania

System **AVG 8.5 Anti-Virus plus Firewall** pozwala uruchomic skanowanie na zadanie uzytkownika (np. 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***:



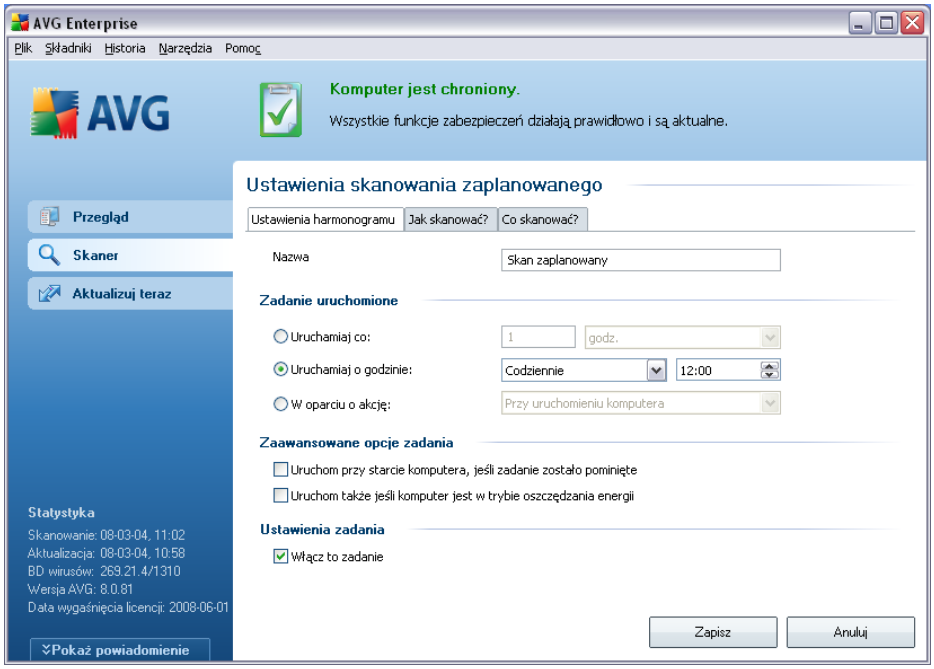
Przyciski kontrolne harmonogramu

We wspomnianej sekcji znajduja sie nastepujace przyciski kontrolne:

- ***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 testów. Klikniecie przycisku spowoduje usuniecie wybranej pozycji z listy. Usuwac mozna jedynie testy zdefiniowane przez uzytkownika; nie da sie usunac domyslnego ***Skanu zaplanowanego*** .

14.5.1.Ustawienia harmonogramu

Aby zaplanowac regularne przeprowadzanie testów, nalezy wprowadzic odpowiednia konfiguracje w ***ustawieniach skanów zaplanowanych***. Okno to podzielone jest 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. Mozna wpisac ja 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.

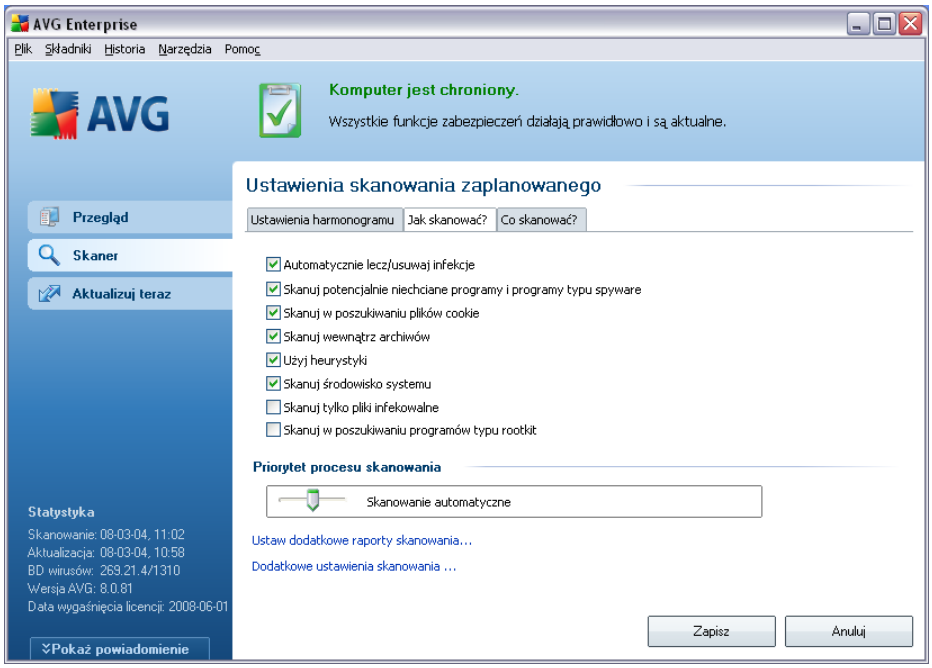
Przyciski kontrolne konfiguracji harmonogramu

Na wszystkich trzech zakladkach okna z ***ustawieniami skanów zaplanowanych*** (***Ustawienia harmonogramu***, ***Jak skanowac?*** i ***Co skanowac?***) dostepne sa dwa przyciski kontrolne. Ich dzialanie jest takie samo na kazdej zakladce:

- ***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 wprowadzone na wszystkich kartach, nalezy kliknac ten przycisk.

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

14.5.2.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*** — (*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.

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

- ***Skanuj w poszukiwaniu sledzacych plików cookie*** — (*domyslnie wlaczona*) 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 wlaczona*) parametr ten okresla, czy skanowanie ma obejmowac pliki 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;***

  - ***Skanuj tylko pliki infekowalne***— (*domyslnie wylaczona*) jesli opcja ta zostanie wlaczona, pliki, które nie moga zostac zainfekowane, nie beda skanowane. Moga to byc np. niektóre pliki tekstowe lub niewykonywalne.

W sekcji ***Priorytet procesu skanowania*** mozna szczególowo okreslic zadana szybkosc 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 tej mozna smialo uzywac wtedy, gdy komputer jest wlaczony, ale nikt na nim nie pracuje*). Mozna równiez obnizyc wykorzystanie zasobów, co przedluzy jednoczesnie czas skanowania.

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 konfiguracji harmonogramu

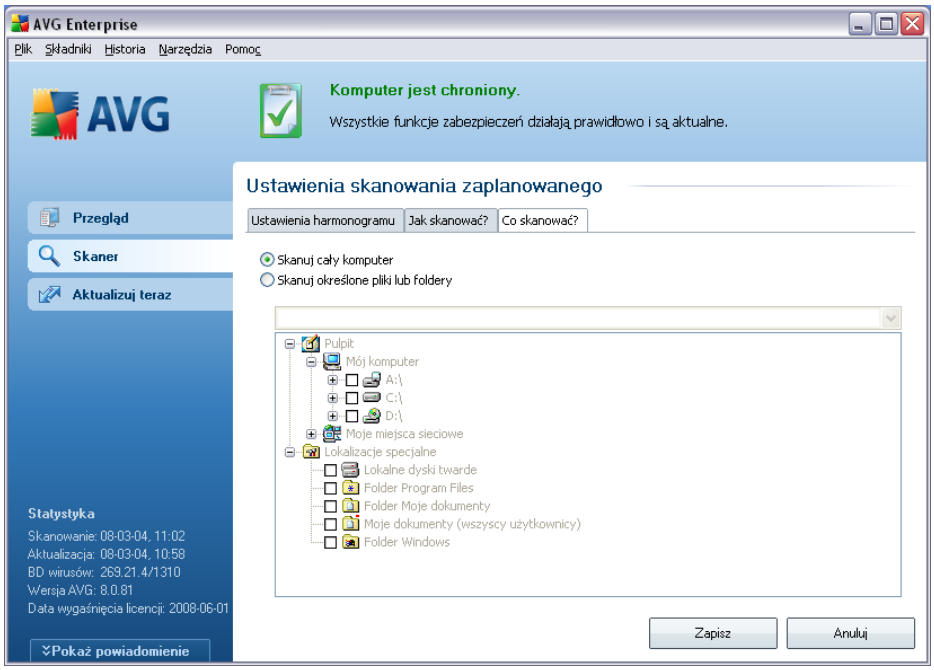
Na wszystkich trzech kartach okna z ***konfiguracja skanu zaplanowanego*** (

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 wprowadzone na wszystkich kartach, nalezy kliknac ten przycisk.

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

14.5.3.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

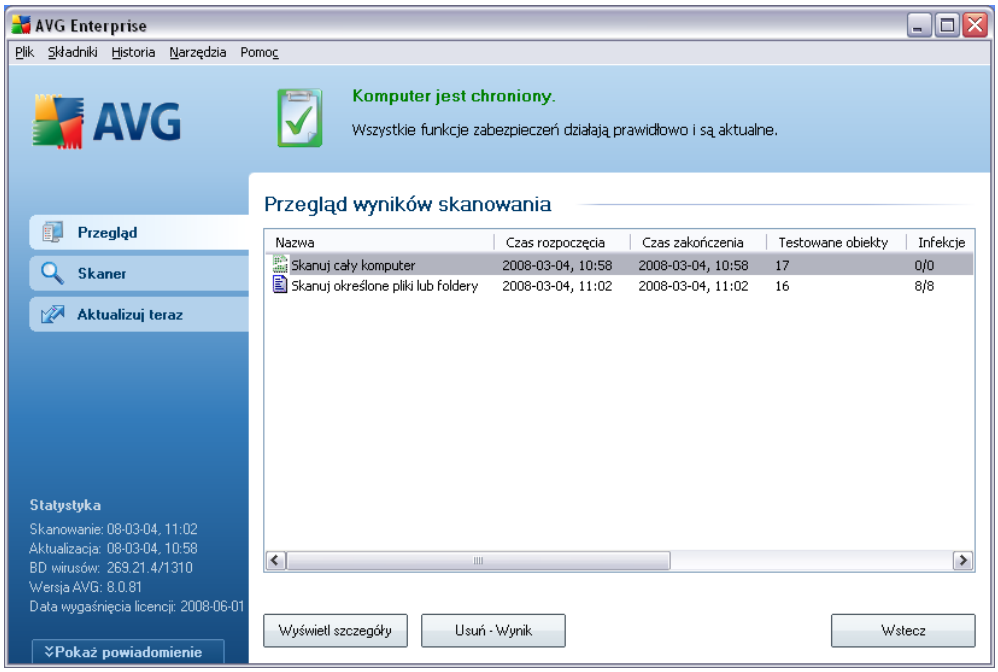
Na wszystkich trzech zakladkach okna z ***ustawieniami skanów zaplanowanych*** (***Ustawienia harmonogramu***, ***Jak skanowac?*** ***i Co skanowac?***) dostepne sa dwa

przyciski kontrolne. Dzialanie tych przycisków jest takie samo na kazdej zakladce:

- ***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 wprowadzone na wszystkich kartach, nalezy kliknac ten przycisk.

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

14.6.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 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 kliknieciu 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.

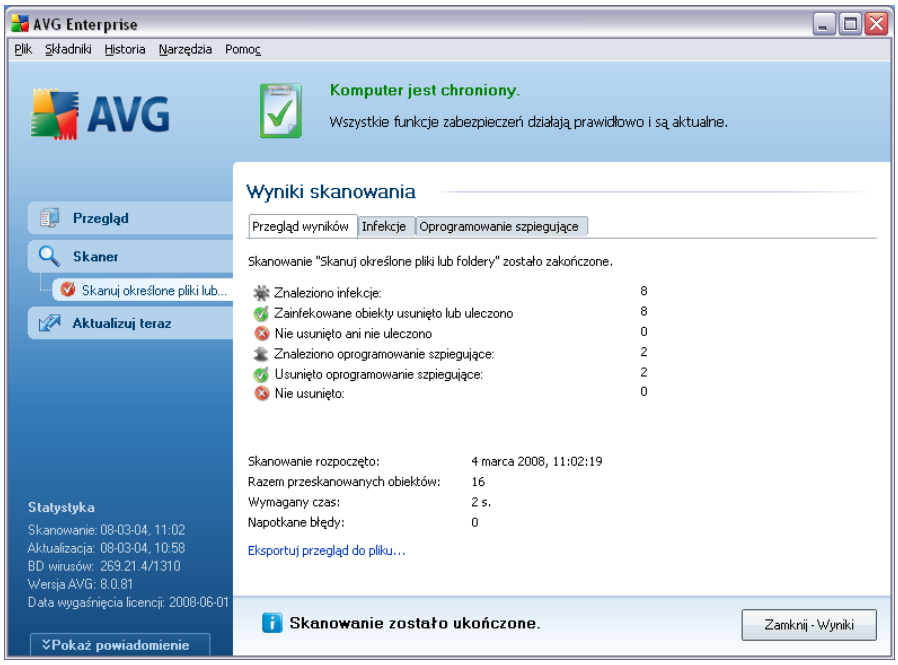
14.7.Szczegóły wyników skanowania

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 karta zawiera komunikat ostrzegawczy.

14.7.1.Karta "Przeglad wyników"



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

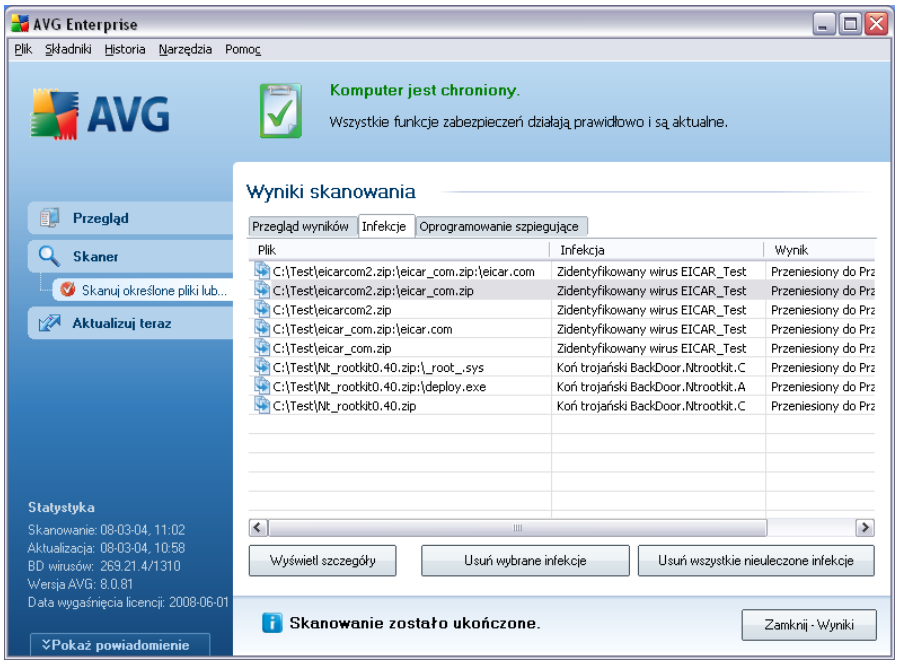
- wykrytych infekcjach wirusowych/programach szpiegujacych
- usunietychinfekcjach wirusowych/programach szpiegujacych
- liczbie infekcji wirusowych/programów szpiegujacych, których nie udalo sie usunac ani wyleczyc.

Ponadto, znajduja sie tu informacje o dacie i dokladnej godzinie uruchomienia testu, lacznej liczbie przeskanowanych obiektów, czasie trwania oraz liczbie napotkanych bledów.

Przyciski kontrolne

Okno to zawiera tylko jeden przycisk kontrolny. Kliknięcie przycisku ***Zamknij wyniki*** powoduje powrót do ***Przegladu wyników skanowania***.

14.7.2.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:

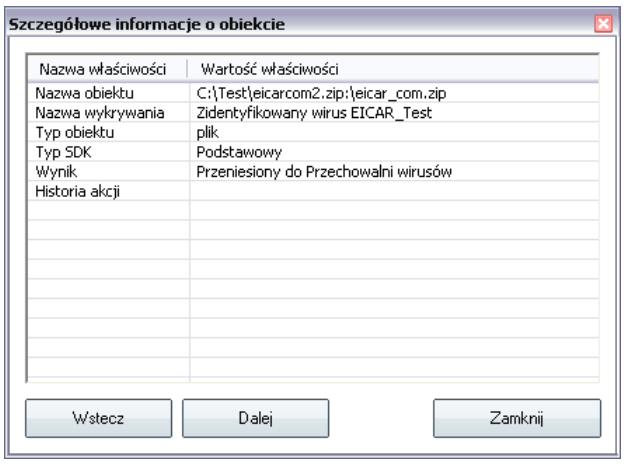
- ***Plik*** — pelna sciezka do oryginalnej lokalizacji zainfekowanego obiektu.
- ***Infekcje*** — nazwa wykrytego wirusa (*szczególowe informacje na temat wirusów zawiera Encyklopedia Wirusów dostepna online*).
- ***Wynik*** — okresla biezacy stan zainfekowanego obiektu, który wykryto podczas skanowania:
    - ***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 ze ***szczególowymi informacjami o wyniku testu***:



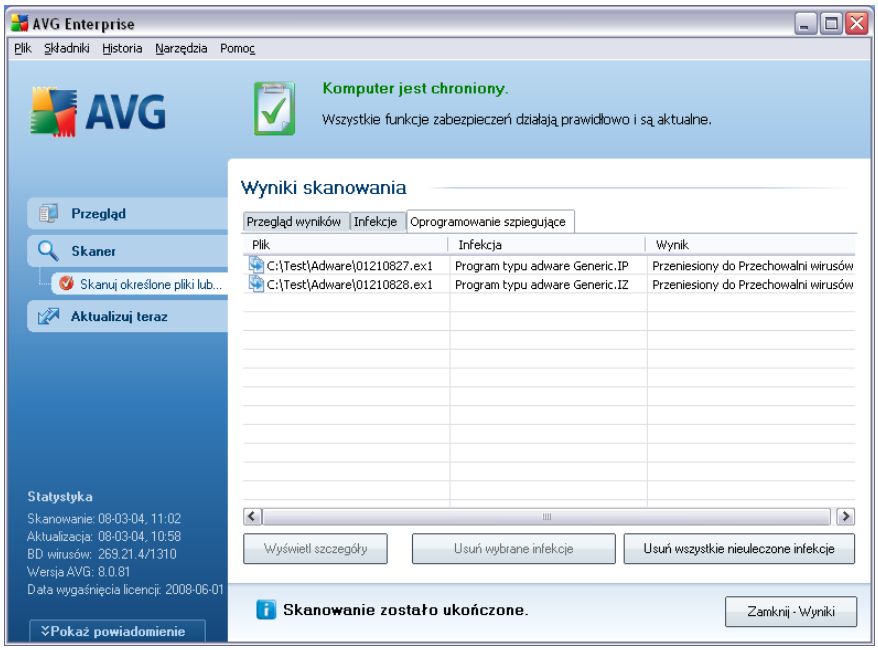
Mozna w nim znalezc informacje o lokalizacji wykrytego pliku (***Nazwa wlasciwosci***). Przyciski ***Wstecz*** i ***Dalej*** sluza do nawigacji miedzy pozycjami listy. Przycisk ***Zamknij*** zamyka okno.

- ***Usun wybrane infekcje*** — pozwala przeniesc wybrane obiekty do ***Przechowalni wirusów.***

- ***Usun wszystkie niewyleczone pliki*** — pozwala usunac wszystkie znalezione obiekty, których nie mozna wyleczyc ani przeniesc do ***Przechowalni wirusów.***

- ***Zamknij wyniki*** — powoduje zamkniecie szczególowych wyników i powrót do okna ***Przeglad wyników skanowania***.

14.7.3.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*).

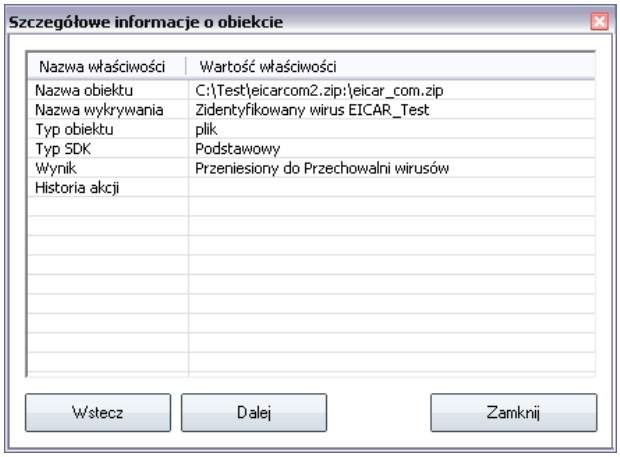
- ***Wynik*** — okresla biezacy stan obiektu, który wykryto podczas skanowania:

- ***Zainfekowany*** — zainfekowany obiekt zostal wykryty i pozostawiony w oryginalnej lokalizacji (np. jesli wylaczono opcje automatycznego leczenia w szczegółowych 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 ***szczegółowymi informacjami o wyniku testu***:



Mozna w nim znalezc informacje o lokalizacji wykrytego pliku (***Nazwa wlasciwosci***). Przyciski ***Wstecz*** i ***Dalej*** sluza do nawigacji miedzy pozycjami listy. Przycisk ***Zamknij*** zamyka okno.

- ***Usun wybrane infekcje*** — pozwala przeniesc wybrane obiekty do ***Przechowalni wirusów.***
- ***Usun wszystkie niewyleczone pliki*** — pozwala usunac wszystkie znalezione obiekty, których nie mozna wyleczyc ani przeniesc do ***Przechowalni wirusów.***
- ***Zamknij wyniki*** — powoduje zamkniecie szczególowych wyników i powrót do okna ***Przeglad wyników skanowania***.

14.7.4.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.

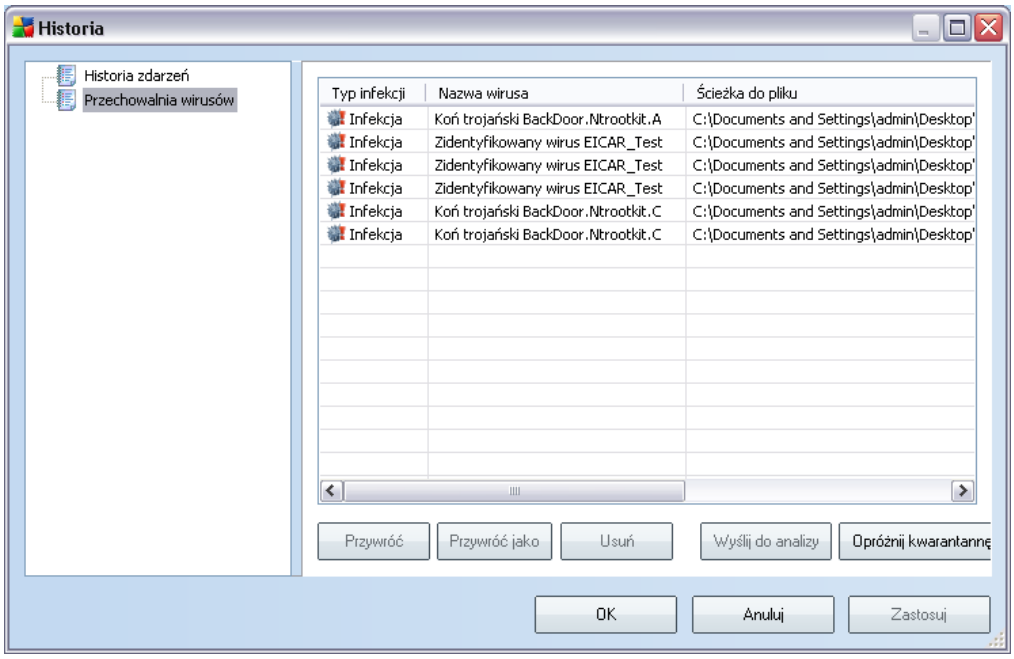
14.7.5.Karta "Programy typu rootkit"

Na karcie·***Programy typu rootkit*** zawiera informacje na temat programów typu rootkit wykrytych podczas skanowania. Jego struktura jest w zasadzie taka sama jak ***karty Infekcje*** i ***karty Oprogramowanie szpiegujace***.

14.7.6.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. Wszystkie dane na tej karcie maja jedynie znaczenie informacyjne.

14.8.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 wybranie 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:

- ***Typ infekcji*** — klasyfikuje obiekty wedlug poziomu 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***.
- ***Wyslij do analizy*** — wysyla podejrzany plik do szczególowej analizy w laboratorium wirusów firmy AVG.
- ***Opróznij kwarantanne*** - usuwa bezpowrotnie cala zawartosc ***Przechowalni wirusów*** .

15. Aktualizacje AVG

15.1.Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

- ***Aktualizacja definicji*** zawiera uzupelnienia niezbedne do zapewnienia niezawodnej ochrony antywirusowej i antyspamowej. 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.

15.2.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.

15.3.Proces aktualizacji

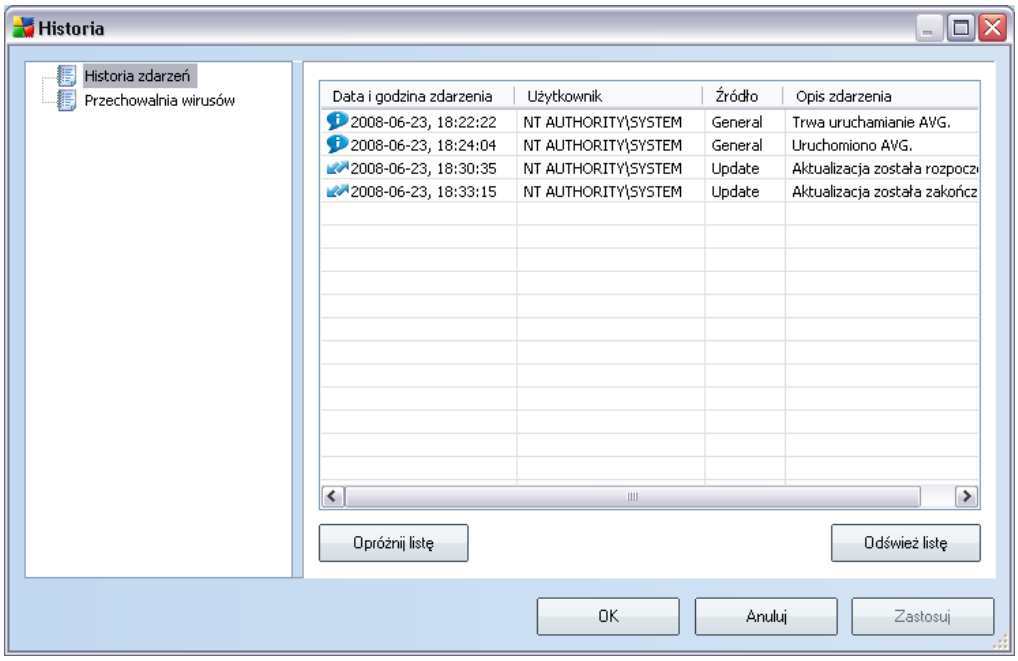
Aktualizacje mozna uruchamiac na zadanie, gdy sa potrzebne, klikajac link ***Aktualizuj teraz*** . Link ten jest zawsze dostepny w glównym oknie interfejsu uzytkownika AVG. Mimo to, zaleca sie regularne aktualizowanie systemu, zgodnie z harmonogramem, który mozna edytowac za pomoca Menedzera aktualizacji.

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 otwierane jest okno ***Aktualizacja*** , w którym mozna sledzic przedstawiony graficznie postep aktualizacji oraz przegladac szereg parametrów (

rozmiar pliku aktualizacyjnego, ilosc odebranych danych, szybkosc i czas pobierania itd.).

***Uwaga**: Przed zaktualizowaniem programu AVG tworzony jest punkt odtwarzania systemu. W przypadku niepowodzenia aktualizacji i awarii systemu operacyjnego mozna odtworzyc pierwotna konfiguracje systemu, uzywajac tego punktu. Aby uzyc tej opcji, nalezy wybrac kolejno: Start / Wszystkie Programy / Akcesoria / Narzedzia systemowe / Odtwarzanie systemu. Zalecane tylko doswiadczonym uzytkownikom!*

16. Historia zdarzen



Do interfejsu ***Historii zdarzen*** mozna dostac sie poprzez menu glówne ***Historia/ Dziennik historii zdarzen***. Okno to zawiera podsumowanie najwazniejszych wydarzen, które wystapily w czasie pracy systemu **AVG 8.5 Anti-Virus plus Firewall**. ***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.

17. FAQ i Pomoc Techniczna

W przypadku jakichkolwiek problemów z oprogramowaniem AVG (w kwestiach handlowych lub technicznych) prosimy skorzystac z sekcji ***FAQ*** dostepnej pod adresem 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***.