



# AVG 9 Anti-Virus plus Firewall

## Podrecznik uzytkownika

### **Wersja dokumentu 90.21 (3.2.2010)**

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

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

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

W produkcie zastosowano biblioteki do kompresji zlib, Copyright (c) 1995-2002 Jean-loup Gailly i Mark Adler. Ten produkt wykorzystuje biblioteki do kompresji libbzip2. Copyright (c) 1996-2002 Julian R. Seward.

## Spis treści

<b>1. Wprowadzenie</b>	<b>7</b>
<b>2. Wymagania instalacyjne AVG</b>	<b>8</b>
2.1 Obsługiwane systemy operacyjne	8
2.2 Minimalne i zalecane wymagania sprzętowe	8
<b>3. Opcje instalacji systemu AVG</b>	<b>9</b>
<b>4. AVG Download Manager</b>	<b>10</b>
4.1 Wybór języka	10
4.2 Test połączenia	11
4.3 Ustawienia proxy	12
4.4 Pobieranie plików instalacyjnych	13
<b>5. Proces instalacji systemu AVG</b>	<b>14</b>
5.1 Uruchamianie instalacji	14
5.2 Umowa licencyjna	15
5.3 Sprawdzanie stanu systemu	15
5.4 Wybieranie typu instalacji	16
5.5 Uaktywnienie licencji AVG	16
5.6 Instalacja niestandardowa — Folder docelowy	18
5.7 Instalacja niestandardowa — Wybór składników	19
5.8 Pasek narzędzi AVG Security Toolbar	20
5.9 Zamknij otwarte aplikacje	21
5.10 Instalowanie systemu AVG	22
5.11 Zaplanowanie regularnych skanów i aktualizacji	23
5.12 Wybór typu komputera	23
5.13 Połączenie internetowe komputera	24
5.14 Zakonczenie konfiguracji ochrony produktu AVG	25
<b>6. Po instalacji</b>	<b>26</b>
6.1 Optymalizacja skanowania	26
6.2 Rejestracja produktu	26
6.3 Dostęp do Interfejsu użytkownika	26
6.4 Skanowanie całego komputera	27
6.5 Test Eicar	27

6.6 Konfiguracja domyślna AVG .....	28
<b>7. Interfejs użytkownika AVG .....</b>	<b>29</b>
7.1 Menu systemowe .....	30
7.1.1 Plik .....	30
7.1.2 Składniki .....	30
7.1.3 Historia .....	30
7.1.4 Narzędzia .....	30
7.1.5 Pomoc .....	30
7.2 Status bezpieczeństwa .....	33
7.3 Linki .....	34
7.4 Przegląd składników .....	35
7.5 Statystyki .....	36
7.6 Ikona na pasku zadań .....	36
<b>8. Składniki AVG .....</b>	<b>38</b>
8.1 Anti-Virus .....	38
8.1.1 Zasady działania składnika Anti-Virus .....	38
8.1.2 Interfejs składnika Anti-Virus .....	38
8.2 Anti-Spyware .....	40
8.2.1 Zasady działania składnika Anti-Spyware .....	40
8.2.2 Interfejs składnika Anti-Spyware .....	40
8.3 Anti-Rootkit .....	42
8.4 Zapora .....	42
8.4.1 Zasady działania Zapory .....	42
8.4.2 Profile Zapory .....	42
8.4.3 Interfejs Zapory .....	42
8.5 Skaner poczty e-mail .....	47
8.5.1 Zasady działania Skanera poczty e-mail .....	47
8.5.2 Interfejs Skanera poczty e-mail .....	47
8.5.3 Zagrożenia wykryte przez Skaner poczty e-mail .....	47
8.6 Licencja .....	51
8.7 LinkScanner .....	52
8.7.1 Zasady działania technologii LinkScanner .....	52
8.7.2 Interfejs LinkScanner .....	52
8.7.3 AVG Search-Shield .....	52
8.7.4 AVG Active Surf-Shield .....	52
8.8 Ochrona Sieci .....	56

8.8.1	Zasady działania składnika Ochrona Sieci .....	56
8.8.2	Interfejs składnika Ochrona Sieci .....	56
8.8.3	Obiekt wykryty przez składnik Ochrona Sieci .....	56
8.9	Ochrona rezydentna .....	63
8.9.1	Zasady działania Ochrony rezydentnej .....	63
8.9.2	Interfejs składnika Ochrona rezydentna .....	63
8.9.3	Zagrożenia wykryte przez Ochronę rezydentna .....	63
8.10	Menedżer aktualizacji .....	68
8.10.1	Zasady działania Menedżera aktualizacji .....	68
8.10.2	Interfejs Menedżera aktualizacji .....	68
<b>9.</b>	<b>Pasek narzędzi AVG Security Toolbar .....</b>	<b>71</b>
9.1	Interfejs paska narzędzi AVG Security Toolbar .....	71
9.2	Opcje Paska narzędzi AVG Security Toolbar .....	73
9.2.1	Karta Ogólne .....	73
9.2.2	Karta Użyteczne przyciski .....	73
9.2.3	Karta Bezpieczeństwo .....	73
9.2.4	Karta Opcje zaawansowane .....	73
<b>10.</b>	<b>Zaawansowane ustawienia AVG .....</b>	<b>78</b>
10.1	Wygląd .....	78
10.2	Dźwięki .....	80
10.3	Ignoruj błędny stan składników .....	82
10.4	Przechowalnia wirusów .....	83
10.5	Wyjątki PNP .....	84
10.6	Ochrona Sieci .....	87
10.6.1	Ochrona WWW .....	87
10.6.2	Komunikatory internetowe .....	87
10.7	LinkScanner .....	91
10.8	Skany .....	92
10.8.1	Skan całego komputera .....	92
10.8.2	Skan rozszerzenia powłoki .....	92
10.8.3	Skan określonych plików lub folderów .....	92
10.8.4	Skan urządzeń wymiennych .....	92
10.9	Zaplanowane zadania .....	99
10.9.1	Skan zaplanowany .....	99
10.9.2	Harmonogram aktualizacji bazy wirusów .....	99
10.10	Skaner poczty e-mail .....	110

10.10.1	Certyfikacja .....	110
10.10.2	Filtrowanie poczty .....	110
10.10.3	Dzienniki i Wyniki .....	110
10.10.4	Serwery .....	110
10.11	Ochrona rezydentna .....	120
10.11.1	Ustawienia zaawansowane .....	120
10.11.2	Wykluczenia katalogów .....	120
10.11.3	Wykluczone pliki .....	120
10.12	Serwer pamięci podręcznej .....	125
10.13	Anti-Rootkit .....	127
10.14	Aktualizacja .....	128
10.14.1	Proxy .....	128
10.14.2	Połączenie telefoniczne .....	128
10.14.3	URL .....	128
10.14.4	Zarządzaj .....	128
10.15	Administracja zdalna .....	135
<b>11.</b>	<b>Ustawienia Zapory .....</b>	<b>137</b>
11.1	Ogólne .....	137
11.2	Bezpieczeństwo .....	138
11.3	Profile kart sieciowych i obszarów .....	139
11.4	Dzienniki .....	140
11.5	Profile .....	142
11.5.1	Informacje o profilu .....	142
11.5.2	Zdefiniowane sieci .....	142
11.5.3	Aplikacje .....	142
11.5.4	Usługi systemowe .....	142
<b>12.</b>	<b>Skanowanie AVG .....</b>	<b>154</b>
12.1	Interfejs skanowania .....	154
12.2	Wstępnie zdefiniowane testy .....	155
12.2.1	Skan całego komputera .....	155
12.2.2	Skan określonych plików lub folderów .....	155
12.3	Skan z poziomu eksploratora systemu Windows .....	163
12.4	Skan z poziomu wiersza poleceń .....	164
12.4.1	Parametry skanowania z wiersza poleceń .....	164
12.5	Planowanie skanowania .....	167
12.5.1	Ustawienia harmonogramu .....	167

12.5.2 Jak skanowac? .....	167
12.5.3 Co skanowac? .....	167
12.6 Przegląd wyników skanowania .....	178
12.7 Szczegóły wyników skanowania .....	179
12.7.1 Karta "Przegląd wyników" .....	179
12.7.2 Karta "Infekcje" .....	179
12.7.3 Karta "Oprogramowanie szpiegujące" .....	179
12.7.4 Karta "Ostrzeżenia" .....	179
12.7.5 Karta "Rootkity" .....	179
12.7.6 Karta "Informacje" .....	179
12.8 Przechowalnia wirusów .....	188
<b>13. Aktualizacje AVG .....</b>	<b>190</b>
13.1 Poziomy aktualizacji .....	190
13.2 Typy aktualizacji .....	190
13.3 Proces aktualizacji .....	191
<b>14. Historia zdarzeń .....</b>	<b>192</b>
<b>15. FAQ i pomoc techniczna .....</b>	<b>194</b>



## 1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację systemu **AVG 9 Anti-Virus plus Firewall**.

**Gratulujemy zakupu systemu AVG 9 Anti-Virus plus Firewall!**

System **AVG 9 Anti-Virus plus Firewall** należy do linii uznanych i nagradzanych produktów AVG, które zapewniają użytkownikom spokój ducha, a ich komputerom — pełne bezpieczeństwo. Podobnie jak pozostałe produkty system **AVG 9 Anti-Virus plus Firewall** zaprojektowano od podstaw pod kątem zapewnienia słynnego już poziomu ochrony w nowy, bardziej przyjazny dla użytkownika sposób.

Nowy produkt **AVG 9 Anti-Virus plus Firewall** łączy ulepszony interfejs z agresywniejszym i szybszym skanowaniem. Dla wygody użytkownika zautomatyzowano najczęściej używane funkcje i dodano nowe, „inteligentne” opcje, które pozwalają precyzyjnie dostosować funkcje ochronne programu do swoich potrzeb. Koniec z poświęcaniem wydajności na rzecz ochrony!

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



## 2. Wymagania instalacyjne AVG

### 2.1. Obsługiwane systemy operacyjne

System **AVG 9 Anti-Virus plus Firewall** służy do ochrony stacji roboczych działających pod następującymi 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)
- Windows 7 (x86 i x64, wszystkie edycje)

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

### 2.2. Minimalne i zalecane wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG 9 Anti-Virus plus Firewall**:

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

Zalecane wymagania sprzętowe dla systemu **AVG 9 Anti-Virus plus Firewall**:

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



### 3. Opcje instalacji systemu AVG

System AVG można zainstalować za pomocą instalatora znajdującego się na oryginalnym dysku CD lub pobranego z witryny firmy AVG (<http://www.avg.com/>).

**Przed rozpoczęciem instalacji systemu AVG zalecamy odwiedzenie naszej witryny (<http://www.avg.com/>) w celu sprawdzenia, czy jest dostępny nowy plik instalacyjny. Dzięki temu możesz mieć pewność, że instalujesz najnowszą dostępną wersję systemu AVG 9 Anti-Virus plus Firewall.**

**Polecamy wypróbowanie nowego programu [AVG Download Manager](#) – narzędzia, które pomoże skonfigurować plik instalacyjny w zadanym języku.**

Podczas samego procesu instalacji konieczne będzie podanie numeru licencji/sprzedazy. Należy więc przygotować go przed rozpoczęciem instalacji. Numer sprzedazy znajduje się na opakowaniu dysku CD. W przypadku zakupienia pakietu AVG przez internet, numer licencji dostarczany jest poprzez e-mail.

## 4. AVG Download Manager

Program **AVG Download Manager** to proste narzędzie, które pomaga w wyborze odpowiedniego pliku instalacyjnego próbnej wersji danego produktu AVG. Na podstawie wprowadzonych przez użytkownika informacji, menedżer wybierze odpowiedni produkt, typ licencji, zestaw składników i język. Na koniec program **AVG Download Manager** pobierze odpowiednie pliki i rozpocznie [proces instalacji](#).

**Ostrzeżenie:** Program *AVG Download Manager* nie jest odpowiedni do pobierania wersji sieciowych oraz SBS i obsługuje tylko następujące systemy operacyjne: Windows 2000 (SP4 + pakiet zbiorczy SRP), Windows XP, Windows Vista i Windows 7.

Program **AVG Download Manager** można pobrać ze strony internetowej firmy AVG dostępnej pod adresem <http://www.avg.com/>). Poniżej znajduje się krótki opis każdego wymaganego kroku w oknie programu **AVG Download Manager**:

### 4.1. Wybór języka



W pierwszym kroku wyświetlanym w programie **AVG Download Manager** należy z rozwijanego menu wybrać język instalacji. Należy pamiętać, że wybór ten dotyczy tylko procesu instalacji; po jej zakończeniu język programu będzie można zmienić bezpośrednio w jego ustawieniach. Aby kontynuować, kliknij przycisk **Dalej**.

## 4.2. Test połączenia

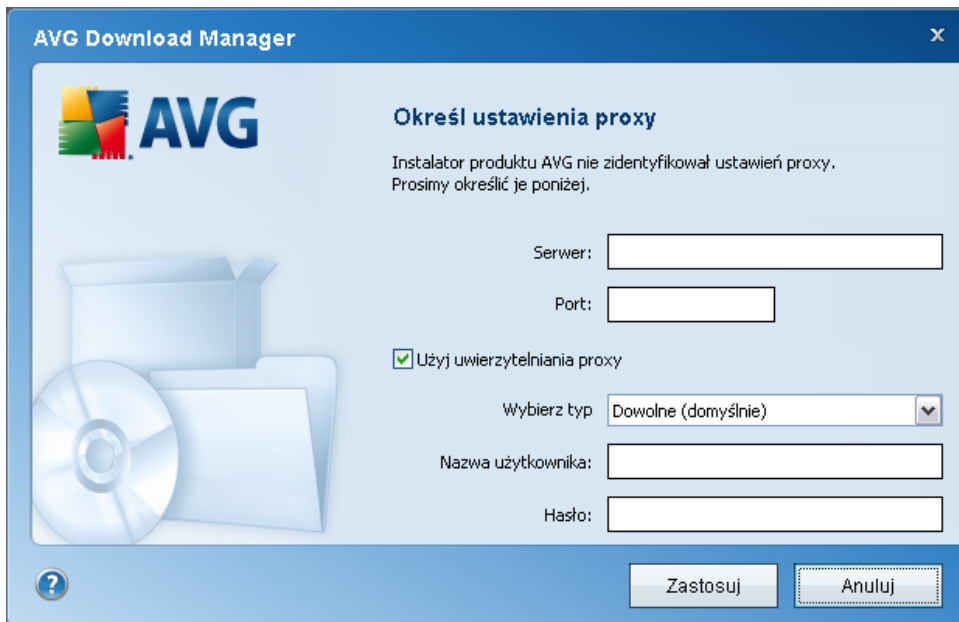
W następnym kroku program **AVG Download Manager** spróbuje nawiązać połączenie internetowe, aby można było znaleźć aktualizacje. Przejście do procesu aktualizacji nie będzie możliwe, dopóki program **AVG Download Manager** nie zakończy testu połączenia.

- Jeśli test wykaze brak łączności, należy upewnić się, że komputer jest faktycznie połączony z internetem. Aby ponownie spróbować, kliknij przycisk **Powtór**



- Jeśli używasz serwera proxy, kliknij przycisk **Ustawienia proxy** i wprowadź [wymagane informacje](#):
- Jeśli test wypadł pomyślnie, kliknij przycisk **Dalej**, aby kontynuować.

### 4.3. Ustawienia proxy

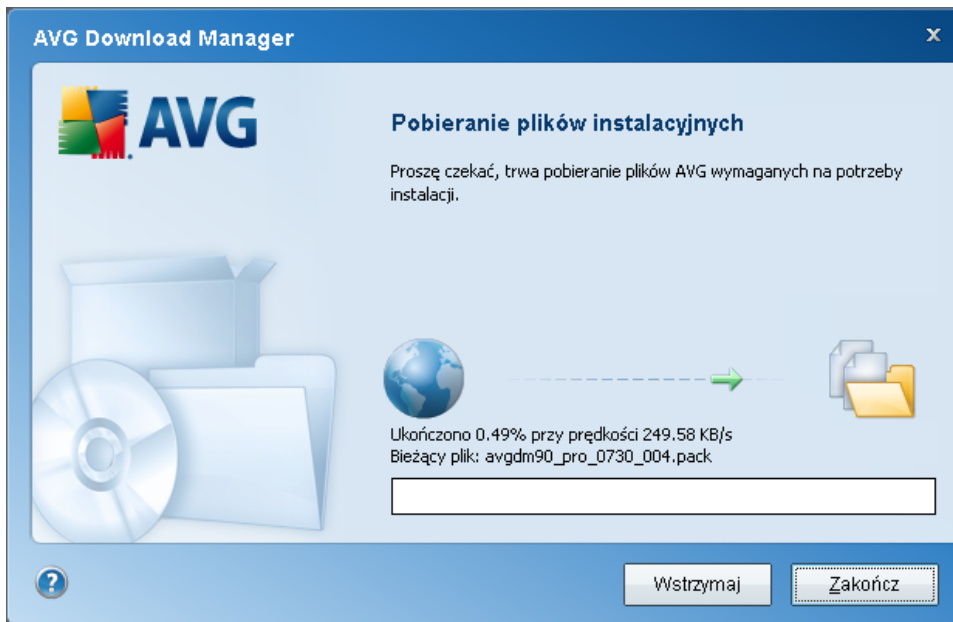


Jeśli program **AVG Download Manager** nie może zidentyfikować ustawień proxy, trzeba określić je ręcznie. Podaj następujące informacje:

- **Serwer** — prawidłowa nazwa lub adres IP serwera proxy.
- **Port** — odpowiedni numer portu.
- **Użyj uwierzytelniania proxy** — zaznacz to pole, jeśli Twój serwer proxy wymaga uwierzytelniania.
- **Wybierz typ uwierzytelniania** — wybierz z listy rozwijanej typ uwierzytelniania. Stanowczo zalecamy, aby zachować wartość domyślną (*serwer sam poda swoje wymagania*). Doświadczeni użytkownicy mogą jednak wybrać opcję "Podstawowe" (*wymagane przez niektóre serwery*) lub "NTLM" (*wymagane przez wszystkie serwery ISA*). Następnie podaj prawidłową **Nazwę użytkownika** i **Hasło** (opcjonalnie).

Po potwierdzeniu ustawień za pomocą przycisku **Zastosuj** program **AVG Download Manager** automatycznie przejdzie do następnego kroku.

#### 4.4. Pobieranie plików instalacyjnych



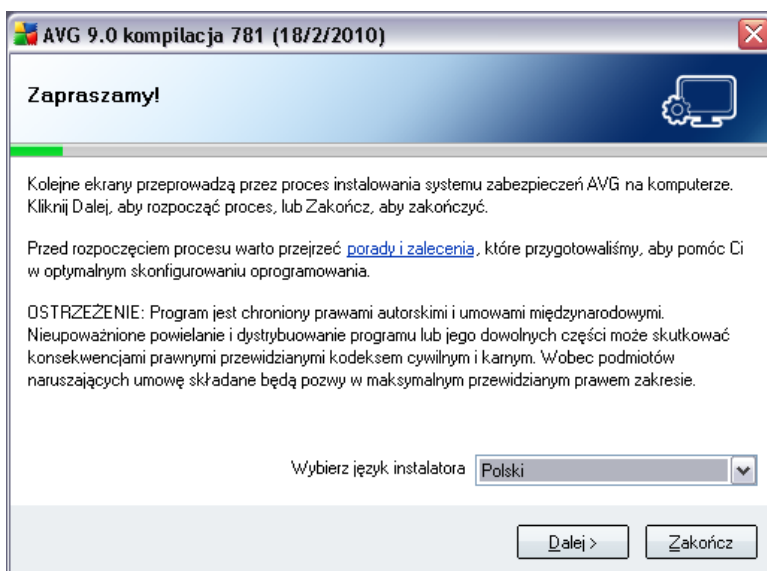
Podano już wszystkie informacje, których program **AVG Download Manager** potrzebuje do pobrania pakietów instalacyjnych i uruchomienia instalacji. Teraz można rozpocząć [instalację systemu AVG](#).

## 5. Proces instalacji systemu AVG

Do zainstalowania systemu **AVG 9 Anti-Virus plus Firewall** na komputerze konieczny jest najnowszy plik instalacyjny. Można znaleźć go na dysku CD będącym częścią dystrybucyjnej edycji programu - istnieje jednak w tym wypadku ryzyko, że będzie on nieaktualny. Dlatego zaleca się pobranie najnowszego pliku instalacyjnego z internetu. Można go pobrać na stronie internetowej firmy AVG (<http://www.avg.com/>) w sekcji [Pomoc techniczna / Pobierz](#). Można również użyć nowego narzędzia [AVG Download Manager](#), które pomaga wybrać odpowiedni pakiet instalacyjny i automatycznie uruchamia proces instalacji.

Instalacja to sekwencja okien dialogowych zawierających krótkie opisy poszczególnych etapów. Poniżej znajdują się wyjaśnienia każdego z nich:

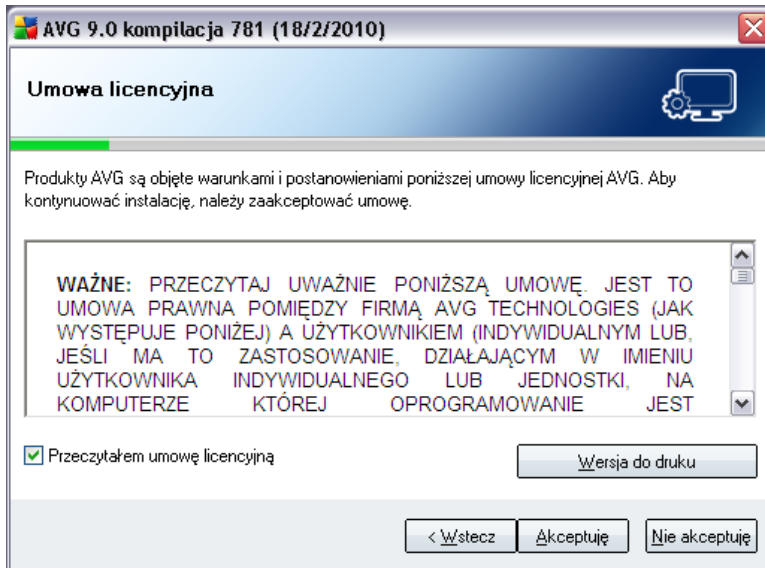
### 5.1. Uruchamianie instalacji



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

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

## 5.2. Umowa licencyjna



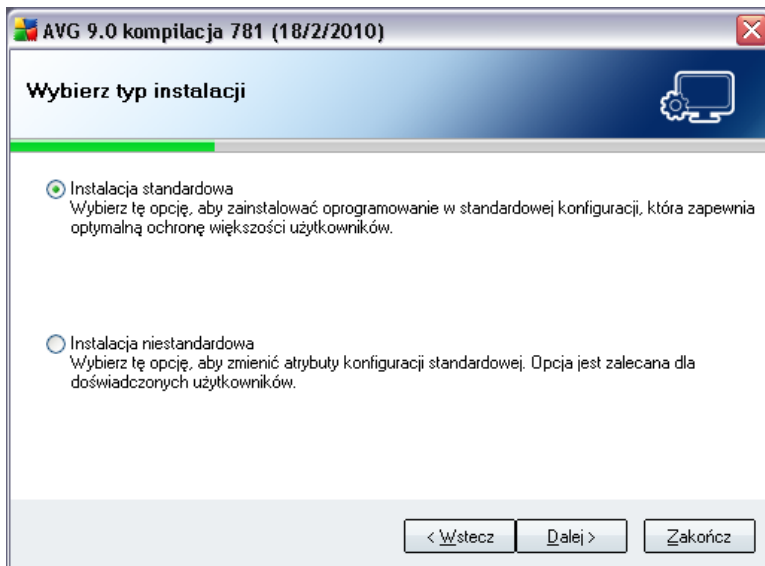
Okno dialogowe **Umowa licencyjna** zawiera pełną treść umowy licencyjnej AVG. Przeczytaj ją uważnie i potwierdź jej akceptację, zaznaczając pole **Przeczytałem warunki umowy licencyjnej** i wciskając przycisk **Dalej**.

Jeśli nie zgadzasz się na postanowienia umowy, kliknij przycisk **Nie akceptuję**; instalacja zostanie natychmiast przerwana.

## 5.3. Sprawdzanie stanu systemu

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

## 5.4. Wybieranie typu instalacji



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

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

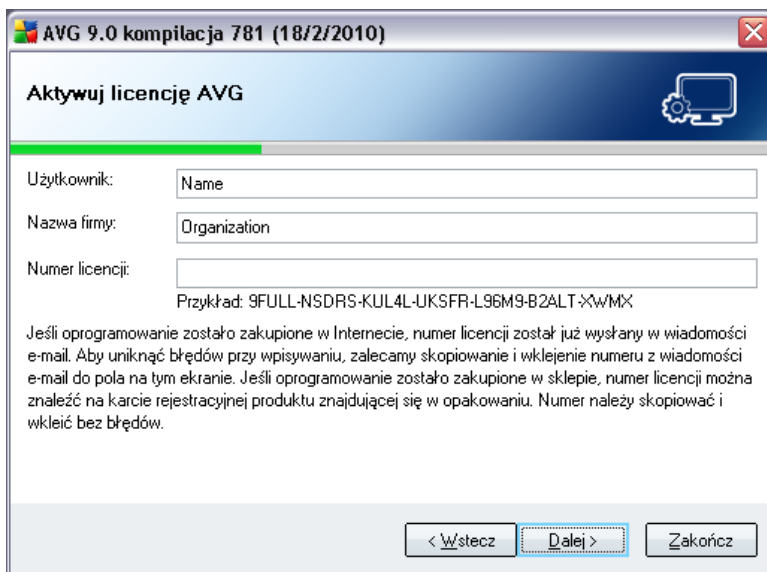
**Instalację niestandardową** powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować systemu AVG z domyślnymi ustawieniami, tj. na przykład po to, aby dostosować go do specyficznych wymagań systemowych.

## 5.5. Uaktywnienie licencji AVG

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

Następnie wprowadź numer licencji (lub numer sprzedaży) w polu tekstowym **Numer licencji**. Numer sprzedaży można znaleźć na opakowaniu dysku CD z

oprogramowaniem **AVG 9 Anti-Virus plus Firewall**. Numer licencji jest wysyłany za pośrednictwem poczty e-mail po dokonaniu zakupu oprogramowania **AVG 9 Anti-Virus plus Firewall** online. Ważne jest dokładne wprowadzenie wspomnianego numeru. Jeśli numer jest dostępny w formie cyfrowej (w wiadomości e-mail), zaleca się skopiowanie go i wklejenie w odpowiednim polu.

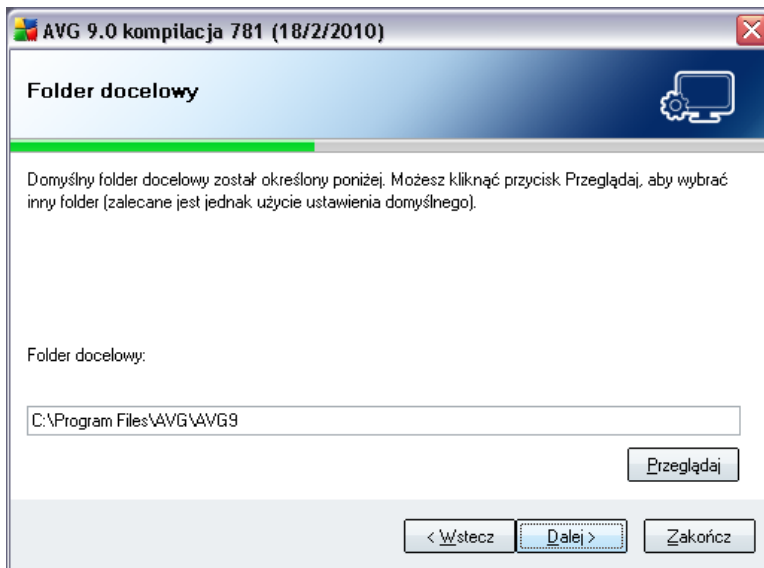


The screenshot shows a window titled "AVG 9.0 kompilacja 781 (18/2/2010)" with a close button in the top right corner. The main heading is "Aktywuj licencję AVG" with a gear icon. Below the heading are three input fields: "Użytkownik:" with "Name" as a placeholder, "Nazwa firmy:" with "Organization" as a placeholder, and "Numer licencji:" which is empty. Below the license field is an example: "Przykład: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XXWMX". A paragraph of text explains that if the software was purchased online, the license number was sent via email and should be copied and pasted. If purchased in a store, the license number is on the product's registration card. At the bottom, there are three buttons: "< Wstecz", "Dalej >" (highlighted with a dashed border), and "Zakończ".

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

Jeśli w poprzednim kroku została wybrana instalacja standardowa, nastąpi przekierowanie bezpośrednio do okna **Pasek narzędzi AVG Security Toolbar**. Jeśli została wybrana instalacja niestandardowa, zostanie wyświetlone okno **Folder docelowy**.

## 5.6. Instalacja niestandardowa – Folder docelowy

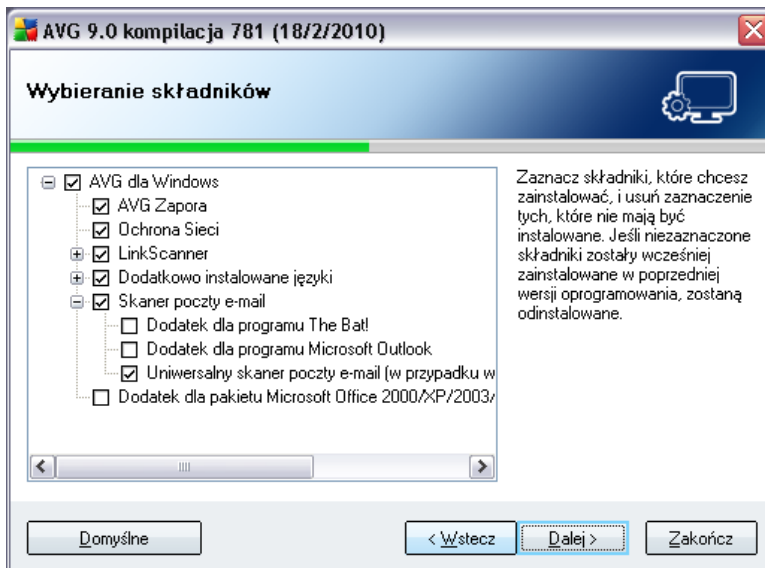


Okno dialogowe **Folder docelowy** umożliwia określenie lokalizacji, w której system **AVG 9 Anti-Virus plus Firewall** ma zostać zainstalowany. Domyślnie pakiet AVG jest instalowany w folderze "Program Files" na dysku C:. Jeśli wybrany folder nie istnieje, zostanie wyświetlone nowe okno dialogowe z pytaniem o zgodę na jego utworzenie.

Aby zmienić tę lokalizację, kliknij przycisk **Przełączaj** i w wyświetlonym oknie wybierz odpowiedni folder.

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

## 5.7. Instalacja niestandardowa – Wybór składników



Okno dialogowe **Wybór składników** zawiera przegląd możliwych do zainstalowania składników systemu **AVG 9 Anti-Virus plus Firewall**. Jeśli ustawienia domyślne nie są dla Ciebie odpowiednie, możesz dodać lub usunąć zadane składniki.

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

### • Wybór języka

Na tej samej liście można także zdefiniować język (lub języki) instalowanego systemu AVG. Należy w tym celu zaznaczyć opcję **Dodatkowo zainstalowane języki** i wybrać je z odpowiedniego menu.

### • Pluginy skanera poczty e-mail

Wybranie pozycji **Skaner poczty e-mail** pozwala wskazać pluginy, które mają zostać zainstalowane w celu zapewnienia ochrony poczty elektronicznej. Domyślnie instalowany jest **Plugin dla programu Microsoft Outlook**. Inną opcją jest **Dodatek dla programu The Bat!**. W przypadku korzystania z innego klienta poczty e-mail (*MS Exchange, Qualcomm Eudora, ...*) należy wybrać **Uniwersalny skaner poczty e-mail**, który chroni wiadomości e-mail niezależnie od używanego programu pocztowego.

Aby kontynuować, kliknij przycisk **Dalej**.

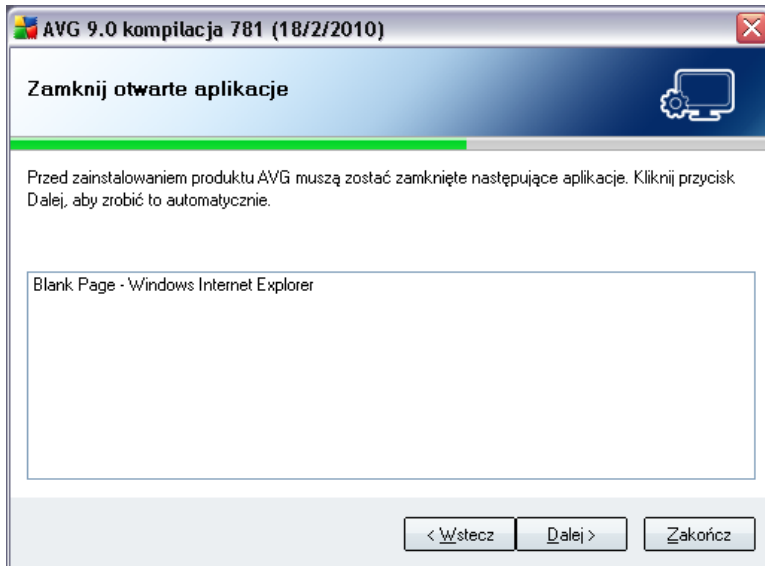
## 5.8. Pasek narzędzi AVG Security Toolbar



W oknie dialogowym **Pasek narzędzi AVG Security Toolbar** należy zdecydować, czy ma zostać zainstalowany **Pasek narzędzi AVG Security Toolbar** (służący do weryfikacji wyników wyszukiwania zwracanych przez obsługiwane wyszukiwarki internetowe). Jeśli domyślne ustawienia nie zostaną zmienione, składnik zostanie automatycznie zainstalowany w przeglądarce internetowej (obecnie obsługiwane przeglądarki to Microsoft Internet Explorer w wersji 6.0 i późniejszych i Mozilla Firefox w wersji 2.0 i późniejszych), aby zapewnić kompleksową ochronę podczas surfowania po internecie.

Można tam również zdecydować, czy Yahoo! ma być wyszukiwarką domyślną. Jeśli tak, zaznacz odpowiednie pole wyboru.

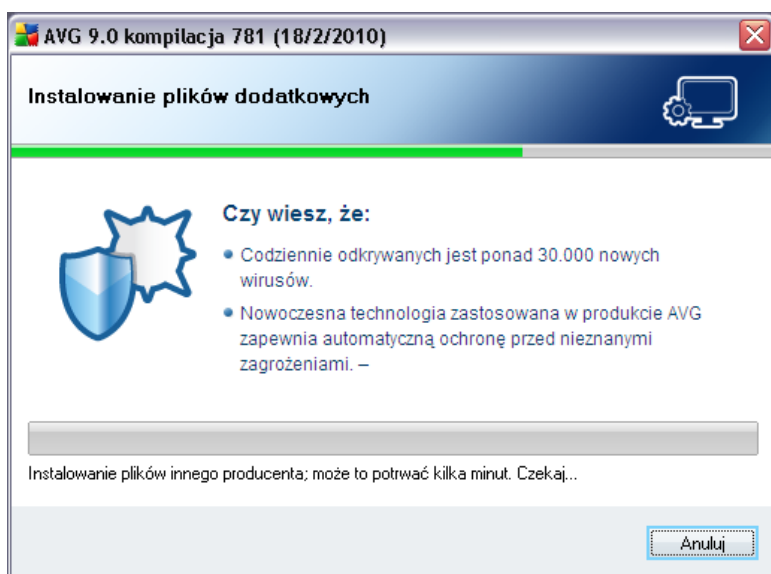
## 5.9. Zamknij otwarte aplikacje



Okno dialogowe **Zamknij wszystkie otwarte aplikacje** zostaje wyświetlone w trakcie procesu instalacji tylko wtedy, gdy na komputerze uruchomione są równocześnie inne programy, które mogłyby zakłócać przebieg instalacji. Następnie zostaje wyświetlona lista programów, które muszą zostać zamknięte, aby możliwe było pomyślne zakończenie procesu instalacji. Kliknij przycisk **Dalej**, aby potwierdzić zamknięcie odpowiednich aplikacji i przejść do następnego kroku.

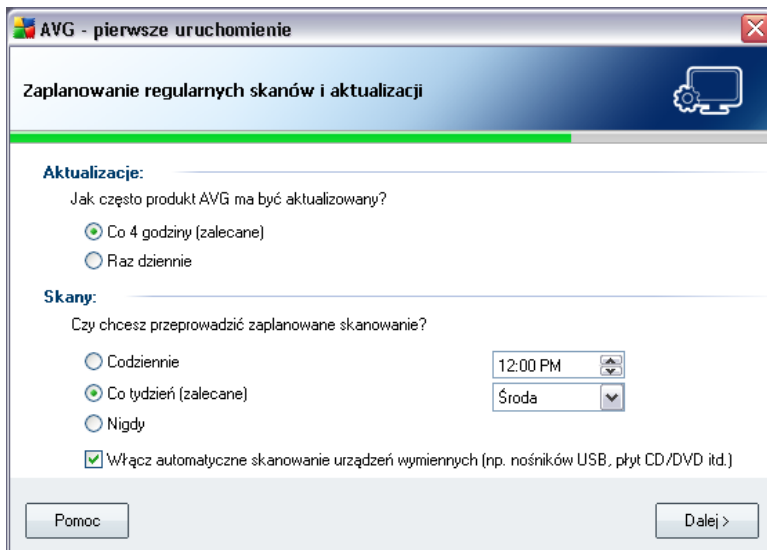
## 5.10. Instalowanie systemu AVG

Okno dialogowe **Instalowanie systemu AVG** zawiera informacje o postępie instalacji i nie wymaga działań ze strony użytkownika:



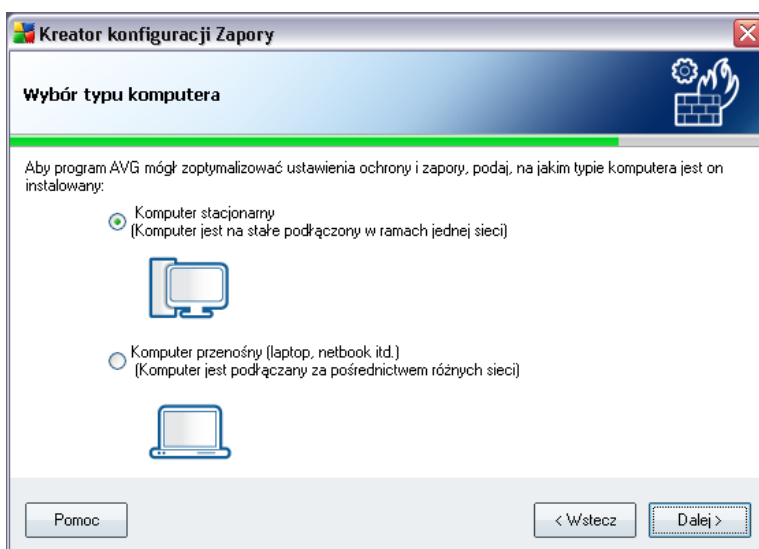
Po zakończeniu instalacji automatycznie nastąpi przekierowanie do następnego okna dialogowego.

### 5.1.1. Zaplanowanie regularnych skanów i aktualizacji



W oknie dialogowym **Planowanie cyklicznych skanów i aktualizacji** określić można częstotliwość sprawdzania dostępności nowych plików aktualizacji i czasu, w którym należy uruchomić [skan zaplanowany](#). Zaleca się zachowanie wartości domyślnych. Aby kontynuować, kliknij przycisk **Dalej**.

### 5.1.2. Wybór typu komputera



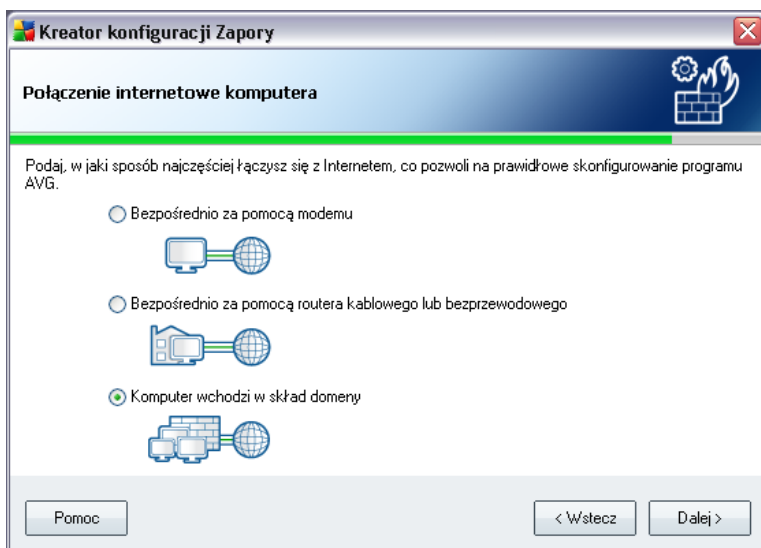
W tym oknie dialogowym **Kreator konfiguracji składnika Zapora** zapyta o rodzaj używanego komputera. Na przykład: notebook łączący się z internetem z wielu różnych lokalizacji (*lotniska, pokoje hotelowe itp.*) wymaga bardziej rygorystycznych reguł zabezpieczeń niż komputer pracujący w domenie (*siec firmowa itp.*). Na podstawie wybranego sposobu użytkowania komputera dobrany zostanie poziom bezpieczeństwa domyślnych reguł **Zapory**.

Dostępne są tu dwie opcje:

- **Komputer stacjonarny**
- **Komputer przenośny**

Wybór należy potwierdzić kliknięciem przycisku **Dalej**, co spowoduje przejście do następnego okna dialogowego.

### 5.13. Połączenie internetowe komputera



W tym oknie, **Kreator konfiguracji Zapory** wyświetla pytanie o sposób podłączenia komputera do internetu. Domyślne reguły **Zapory** zostaną dopasowane do poziomu zabezpieczeń zapewnianych przez wybrany rodzaj połączenia.

Dostępne są tu trzy opcje:

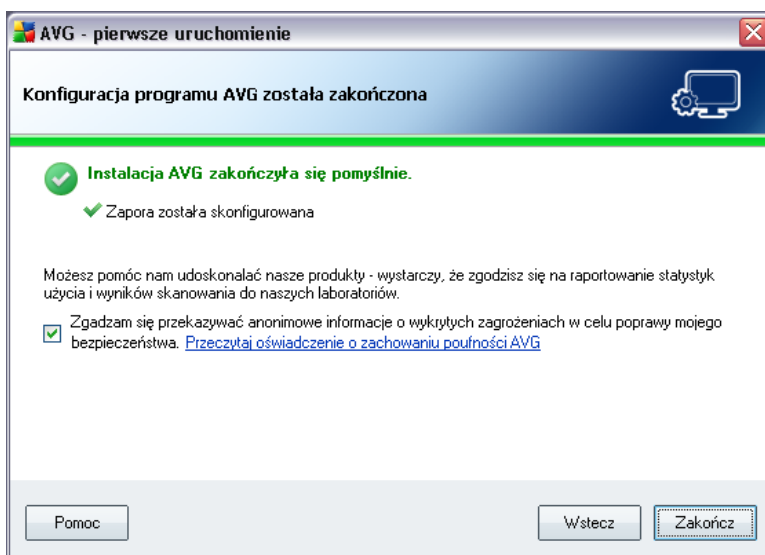
- **Bezpośrednio za pomocą modemu**

- **Bezpośrednio za pomocą routera kablowego lub bezprzewodowego**
- **Komputer wchodzi w skład domeny**

Wskaz, który typ połączenia internetowego jest najbardziej zbliżony do Twojego.

Wybór należy potwierdzić kliknięciem przycisku **Dalej**, co spowoduje przejście do następnego okna dialogowego.

## 5.14. Zakonczenie konfiguracji ochrony produktu AVG



System **AVG 9 Anti-Virus plus Firewall** został skonfigurowany.

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

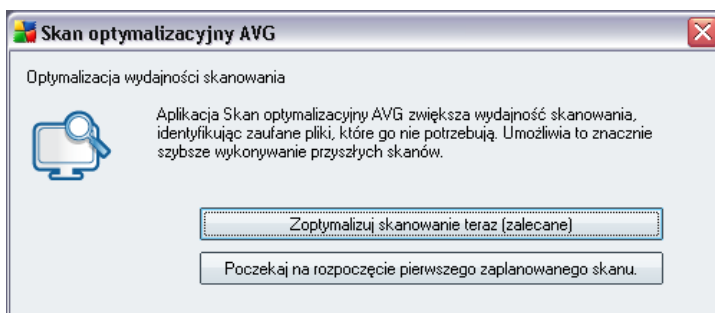
Na koniec należy wcisnąć przycisk **Zakończ**. Rozpoczęcie pracy z systemem AVG może wymagać ponownego uruchomienia komputera.

## 6. Po instalacji

### 6.1. Optymalizacja skanowania

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

Po zakończeniu procesu instalacji zostanie wyświetlone nowe okno dialogowe z opcją optymalizacji skanowania:



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

### 6.2. Rejestracja produktu

Po ukończeniu instalacji systemu **AVG 9 Anti-Virus plus Firewall** należy zarejestrować produkt online na stronie internetowej AVG (<http://www.avg.com/>) w sekcji **Rejestracja** (postępując zgodnie z wyświetlanymi tam instrukcjami). Rejestracja umożliwia pełny dostęp do konta użytkownika AVG, biuletynu aktualizacji AVG i innych usług oferowanych wyłącznie zarejestrowanym klientom.

### 6.3. Dostęp do Interfejsu użytkownika

Dostęp do [interfejsu użytkownika AVG](#) można uzyskać na kilka sposobów:

- klikając dwukrotnie ikonę AVG na pasku zadań,
- klikając dwukrotnie ikonę AVG na pulpicie,

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

## 6.4. Skanowanie całego komputera

Istnieje pewne ryzyko, że wirus dostał się do komputera przed zainstalowaniem systemu **AVG 9 Anti-Virus plus Firewall**. Z tego powodu należy uruchomić test **[Skan całego komputera](#)**, aby upewnić się, że jest on w pełni bezpieczny.

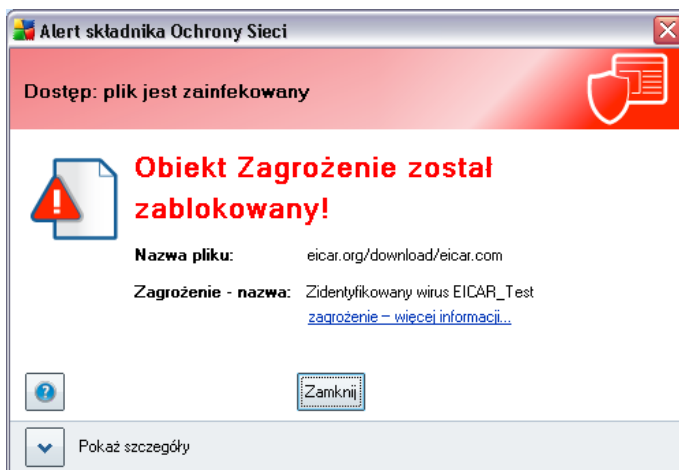
Instrukcje dotyczące uruchamiania testu **[Skan całego komputera](#)** zawiera rozdział **[Skanowanie AVG](#)**.

## 6.5. Test Eicar

Aby potwierdzić, że system **AVG 9 Anti-Virus plus Firewall** został zainstalowany poprawnie, można przeprowadzić test EICAR.

Test EICAR jest standardowa i całkowicie bezpieczna metoda służąca do sprawdzania prawidłowości działania systemu antywirusowego. Można go bezpiecznie rozpowszechnić, ponieważ nie jest prawdziwym wirusem i nie zawiera żadnych fragmentów złośliwego kodu. Większość produktów rozpoznaje go jako wirusa (*choć zwykle zgłasza go pod jednoznaczna nazwa, np. „EICAR-AV-Test”*). Wirusa EICAR można pobrać z witryny stowarzyszenia EICAR, dostępnej pod adresem [www.eicar.com](http://www.eicar.com). Można tam również znaleźć wszystkie niezbędne informacje na temat testu EICAR.

Spróbuj pobrać plik ***eicar.com*** i zapisać go na dysku twardym komputera. Natychmiast po rozpoczęciu pobierania pliku testowego, składnik **[Ochrona Sieci](#)** zareaguje wyświetleniem ostrzeżenia. Pojawienie się komunikatu potwierdza, że oprogramowanie AVG jest prawidłowo zainstalowane na komputerze.





Ze strony internetowej <http://www.eicar.com> można również pobrać skompresowaną wersję "wirusa" EICAR (w formie pliku *eicar\_com.zip*). **Ochrona Sieci** pozwoli pobrać ten plik i zapisać go na dysku, ale już **Ochrona rezydentna** wykryje tego "wirusa" w chwili rozpakowywania go. **Jesli system AVG nie rozpozna pliku testowego EICAR jako wirusa, należy ponownie sprawdzić jego konfigurację!**

## 6.6. Konfiguracja domyślna AVG

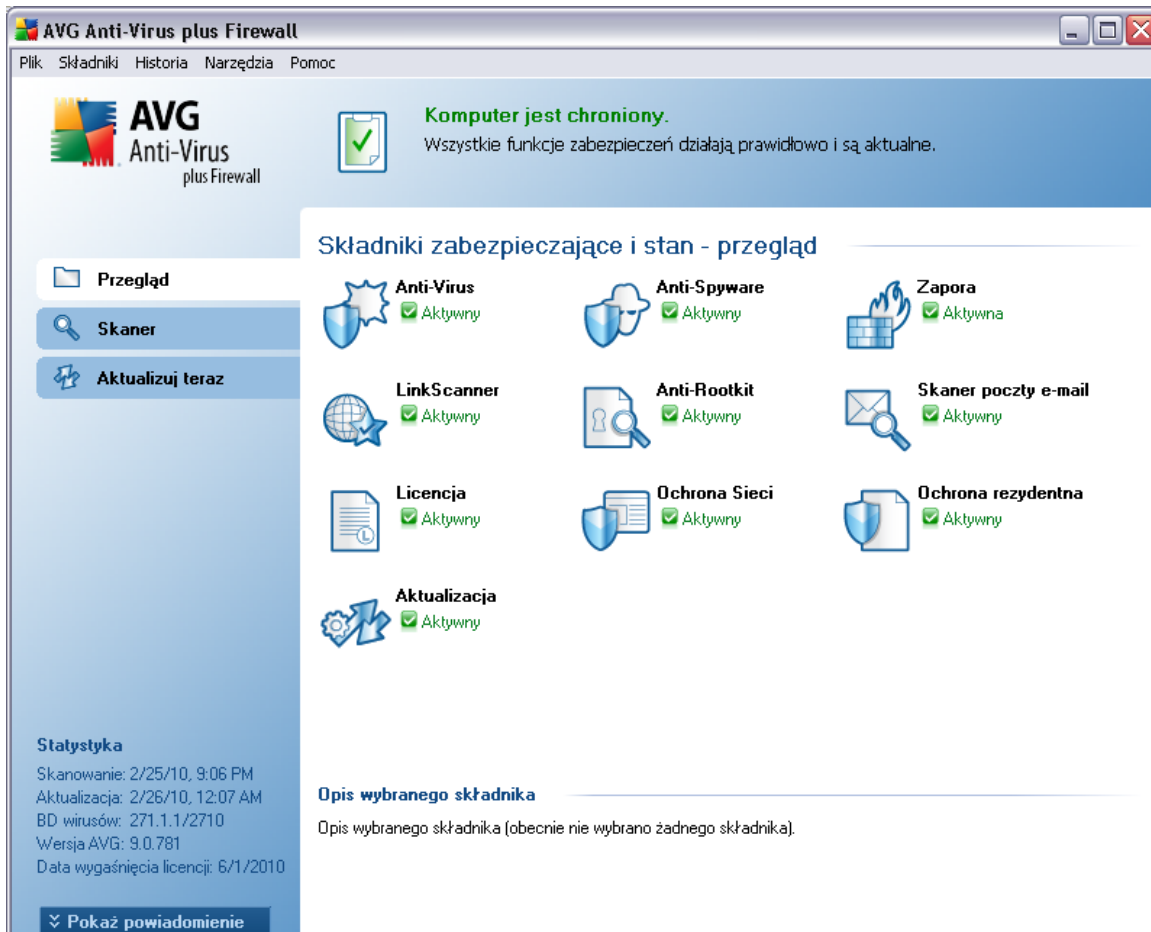
Konfiguracja domyślna (*ustawienia stosowane zaraz po instalacji*) systemu **AVG 9 Anti-Virus plus Firewall** jest wstępnie definiowana przez dostawcę oprogramowania i ma na celu zapewnienie optymalnej wydajności wszystkich składników i funkcji.

***Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach! Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników.***

Mniejsze zmiany ustawień [składników AVG](#) można wprowadzać bezpośrednio z ich interfejsu użytkownika. Jeśli konfiguracja systemu AVG powinna zostać lepiej dopasowana do potrzeb użytkownika, należy przejść do [zaawansowanych ustawień systemu AVG](#), wybierając z menu systemowego pozycję **Narzędzia/Ustawienia zaawansowane** i edytując opcje w otwartym oknie dialogowym [Zaawansowane ustawienia AVG](#).

## 7. Interfejs użytkownika AVG

Otwarcie systemu **AVG 9 Anti-Virus plus Firewall** następuje w jego oknie głównym:



Okno główne jest podzielone na kilka sekcji:

- **Menu główne** (górny wiersz okna) to standardowe narzędzie nawigacyjne umożliwiające dostęp do wszystkich składników, usług i funkcji programu AVG — [szczegóły >>](#)
- **Informacje o stanie bezpieczeństwa** (prawa część górnej sekcji okna) zawiera informacje dotyczące bieżącego stanu programu AVG — [szczegóły >>](#)
- **Szybkie łącza** (lewa kolumna) umożliwiają uzyskanie szybkiego dostępu do najważniejszych i najczęściej używanych funkcji programu AVG — [szczegóły](#)

>>

- **Przegląd składników** (centralna część okna) zawiera przegląd zainstalowanych składników programu AVG — [szczegóły >>](#)
- **Statystyka** (lewa dolna sekcja okna) zawiera najważniejsze dane statystyczne dotyczące działania programu — [szczegóły >>](#)
- **Ikona na pasku zadań** (prawy dolny róg ekranu, na pasku systemowym) sygnalizuje bieżący stan programu AVG — [szczegóły >>](#)

## 7.1. Menu systemowe

**Menu systemowe** to standardowa metoda nawigacji we wszystkich aplikacjach w systemie Windows. Jest zlokalizowane horyzontalnie w górnej części głównego okna systemu **AVG 9 Anti-Virus plus Firewall**. Menu systemowe zapewnia dostęp do poszczególnych składników AVG, funkcji i usług.

Menu systemowe jest podzielone na pięć sekcji:

### 7.1.1. Plik

- **Zakończ** — powoduje zamknięcie **AVG 9 Anti-Virus plus Firewall** interfejsu użytkownika. System AVG działa jednak w tle, a komputer jest nadal chroniony!

### 7.1.2. Składniki

Pozycja **Składniki** w menu głównym zawiera łącza do wszystkich zainstalowanych składników systemu AVG; kliknięcie któregoś z nich powoduje otwarcie domyślnego okna interfejsu odpowiedniego składnika:

- **Przegląd systemu** — pozwala przełączyć widok do domyślnego okna interfejsu użytkownika systemu AVG, zawierającego [przegląd zainstalowanych składników i ich stanu](#).
- **Anti-Virus** — otwiera domyślne okno interfejsu składnika **Anti-Virus**.
- **Anti-Rootkit** — otwiera domyślne okno interfejsu składnika **Anti-Rootkit**.
- **Anti-Spyware** — otwiera domyślne okno interfejsu składnika **Anti-Spyware**.
- **Zapora** — otwiera domyślne okno interfejsu składnika **Zapora**.
- **Link Scanner** — otwiera domyślne okno interfejsu składnika **Link Scanner**.

- ***Skaner poczty e-mail*** — otwiera domyslne okno interfejsu skladnika [\*\*\*Skaner poczty e-mail\*\*\*](#).
- ***Licencja*** — otwiera domyslne okno interfejsu skladnika [\*\*\*Licencja\*\*\*](#).
- ***Ochrona Sieci*** — otwiera domyslne okno interfejsu skladnika [\*\*\*Ochrona Sieci\*\*\*](#).
- ***Ochrona rezydentna*** — otwiera domyslne okno interfejsu skladnika [\*\*\*Ochrona rezydentna\*\*\*](#).
- ***Menedzer aktualizacji*** — otwiera domyslne okno interfejsu [\*\*\*Menedzera aktualizacji\*\*\*](#).

### 7.1.3. Historia

- [\*\*\*Wyniki skanowania\*\*\*](#) — przelacza do interfejsu skanera AVG, konkretnie do okna dialogowego [\*\*\*Przegląd wyników skanowania\*\*\*](#)
- [\*\*\*Zagrożenia wykryte przez Ochrone rezydentna\*\*\*](#) — powoduje otwarcie okna dialogowego zawierajacego przeglad zagrozen wykrytych przez skladnik [\*\*\*Ochrona rezydentna\*\*\*](#)
- [\*\*\*Zagrożenia wykryte przez Skaner poczty e-mail\*\*\*](#) — otwiera okno dialogowe zawierajacego przeglad zalaczników e-mail uznanych za niebezpieczne przez skladnik [\*\*\*Skaner poczty e-mail\*\*\*](#).
- [\*\*\*Zagrożenia wykryte przez Ochrone Sieci\*\*\*](#) — otwiera okno dialogowe zawierajace przeglad zagrozen wykrytych przez skladnik [\*\*\*Ochrone Sieci\*\*\*](#)
- [\*\*\*Przechowalnia wirusów\*\*\*](#) — powoduje otwarcie interfejsu [\*\*\*Przechowalni wirusów\*\*\*](#), do której program AVG przenosi wszystkie niemozliwe do wyleczenia infekcje. W czasie tej kwarantanny zainfekowane pliki sa izolowane i nie zagrazaja bezpieczenstwu komputera, a jednoczesnie istnieje mozliwosc ich naprawy w przyszlosci.
- [\*\*\*Dziennik historii zdarzen\*\*\*](#) — powoduje otwarcie interfejsu dziennika historii z przegladem wszystkich zarejestrowanych akcji **AVG 9 Anti-Virus plus Firewall** .
- [\*\*\*Zapora\*\*\*](#) — powoduje otwarcie karty [\*\*\*Dzienniki\*\*\*](#) (dostepnej również w Konfiguracji Zapory), która zawiera szczególowy przeglad wszystkich dzialan tego skladnika

#### 7.1.4. Narzędzia

- **Skanuj komputer** — przelacza do [Interfejsu skanera AVG](#)i uruchamia skanowanie całego komputera
- **Skanuj wybrany folder** — przelacza do [Interfejsu skanera AVG](#)i umożliwia zdefiniowanie (w ramach struktury katalogów i dysków) plików oraz folderów, które mają być przeskanowane
- **Skanuj plik**  umożliwia uruchomienie na zadanie testu pojedynczego pliku wybranego z drzewa katalogów.
- **Aktualizuj**  automatycznie uruchamia proces aktualizacji systemu **AVG 9 Anti-Virus plus Firewall**
- **Aktualizuj z katalogu** — uruchamia proces aktualizacji korzystając z pliku zlokalizowanego w określonym folderze na dysku lokalnym. Jednak ta opcja jest zalecana do użytku jedynie w sytuacjach awaryjnych, np. gdy nie ma połączenia z internetem (*komputer został zainfekowany i odłączony od internetu, komputer jest podłączony do sieci bez dostępu do internetu itp.*). W nowo otwartym oknie należy wskazać folder, w którym został wcześniej umieszczony plik aktualizacyjny i uruchomić proces.
- **Ustawienia zaawansowane**  otwiera okno dialogowe **Ustawienia zaawansowane systemu AVG**, w którym można edytować konfigurację systemu **AVG 9 Anti-Virus plus Firewall**. Na ogół zaleca się zachowanie domyślnych ustawień zdefiniowanych przez producenta oprogramowania AVG.
- **Ustawienia Zapory** — otwiera okno zaawansowanej konfiguracji składnika **Zapora AVG**.

#### 7.1.5. Pomoc

- **Spis treści** — otwiera pliki pomocy systemu AVG.
- **Uzyskaj pomoc online** — otwiera witrynę firmy AVG (<http://www.avg.com/>) na stronie centrum pomocy technicznej dla klientów.
- **Strona Mój AVG** — otwiera witrynę systemu AVG (<http://www.avg.com/>).
- **Informacje o wirusach i zagrożeniach** — powoduje otwarcie **Encyklopedii Wirusów** online, w której znaleźć można szczegółowe informacje na temat znanych wirusów.
- **Aktywuj ponownie** — otwiera okno **Aktywacja programu AVG** zawierające

dane wprowadzone na etapie [personalizacja programu AVG](#) (podczas [procesu instalacji](#)). W oknie tym można wprowadzić numer licencji w celu zastąpienia numeru sprzedaży (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*).

- [Zarejestruj teraz](#) — łączy się ze stroną rejestracji w witrynie systemu AVG (<http://www.avg.com/>). Należy tam podać swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.

**Uwaga:** W przypadku korzystania z próbnej wersji systemu **AVG 9 Anti-Virus plus Firewall**, ostatnie dwie wyświetlone pozycje to **Kup teraz i Aktywuj**. Umożliwiają one uaktualnienie programu do jego pełnej wersji. W przypadku systemu **AVG 9 Anti-Virus plus Firewall** zainstalowanego z numerem sprzedaży, te pozycje to **Zarejestruj i Aktywuj**. Więcej informacji można znaleźć sekcji [Licencja](#) niniejszej dokumentacji.

- **AVG – informacje** — otwiera okno dialogowe **Informacje**. Okno to składa się z pięciu kart zawierających informacje na temat nazwy programu, wersji silnika antywirusowego i jego bazy danych, systemu, umowy licencyjnej oraz danych kontaktowych firmy **AVG Technologies CZ**.

## 7.2. Status bezpieczeństwa

Sekcja **Informacje o stanie bezpieczeństwa** znajduje się w górnej części Interfejsu użytkownika AVG. Znajdziesz tam informacje o bieżącym stanie bezpieczeństwa systemu **AVG 9 Anti-Virus plus Firewall**. W obszarze tym mogą być wyświetlane następujące ikony:



Ikona zielona oznacza, że system AVG jest w pełni funkcjonalny. Komputer jest całkowicie chroniony, bazy danych są aktualne, a wszystkie zainstalowane składniki działają prawidłowo.



Ikona pomarańczowa oznacza, że co najmniej jeden składnik jest nieprawidłowo skonfigurowany; należy sprawdzić jego właściwości i ustawienia. W systemie AVG nie wystąpił jednak żaden problem krytyczny, a użytkownik prawdopodobnie wyłączył tylko z jakiegoś powodu jeden lub więcej składników. System AVG nadal chroni komputer, należy jednak sprawdzić ustawienia składnika, który zgłasza problem. Jego nazwa jest wyświetlana w sekcji **Informacje o stanie bezpieczeństwa**.

Ikona ta jest także wyświetlana, gdy z jakiegos powodu [stan błędu składników ma być ignorowany](#) (opcja "Ignoruj stan składnika" jest dostępna po kliknięciu prawym przyciskiem ikony odpowiedniego składnika w głównej sekcji okna AVG). Użycie tej opcji może być wskazane w określonych sytuacjach, ale stanowczo zaleca się jak najszybsze ponowne wyłączenie opcji **Ignoruj stan składnika**.



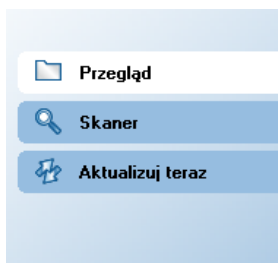
Ikona czerwona oznacza, że stan systemu AVG jest krytyczny! Jeden lub więcej składników nie działa, a system AVG nie może chronić komputera. Należy natychmiast usunąć zgłoszony problem. Jeśli nie jest to możliwe, należy skontaktować się z zespołem [Pomocy Technicznej AVG](#).

Stanowczo zaleca się reagowanie na zmiany **Statusu Bezpieczeństwa** i natychmiastowe rozwiązywanie ewentualnych problemów. Brak reakcji narazi komputer na poważne zagrożenia!

**Uwaga:** Dostęp do informacji o stanie systemu AVG zapewnia przez cały czas również [ikona na pasku zadań](#).

### 7.3. Linki

**Szybkie linki** (z lewej strony [interfejsu użytkownika AVG](#)) pozwalają natychmiast uzyskać dostęp do najważniejszych i najczęściej używanych funkcji systemu AVG:



- **Przegląd** — pozwala przełączać między bieżącym interfejsem AVG a interfejsem domyślnym, zawierającym przegląd wszystkich zainstalowanych składników - zobacz rozdział [Przegląd składników >>](#)
- **Skaner** — otwiera interfejs skanowania AVG, w którym można uruchamiać test, planować skany i edytować ich parametry (zobacz rozdział [Skanowanie AVG >>](#))
- **Aktualizuj teraz** — otwiera odpowiedni interfejs i uruchamia proces aktualizacji systemu AVG (zobacz rozdział [Aktualizacje AVG >>](#))

Linki te są dostępne przez cały czas. Kliknięcie jednego z nich w celu uruchomienia określonego procesu powoduje wyświetlenie innego okna dialogowego, ale sama sekcja linków nie ulegnie zmianie. Uruchomiony proces został dodatkowo przedstawiony w formie graficznej.

## 7.4. Przegląd składników

Sekcja **Przegląd składników** znajduje się w środkowej części [interfejsu użytkownika AVG](#). Obszar ten podzielony jest na dwie części:

- Przegląd wszystkich zainstalowanych składników (panel z odpowiednimi ikonami oraz informacjami o tym, czy dany składnik jest aktywny, czy nie)
- Opis wybranego składnika.

Sekcja **Przegląd składników** systemu **AVG 9 Anti-Virus plus Firewall** zawiera informacje o następujących składnikach:

- **Anti-Virus** — zapewnia ochronę przed wirusami, które mogą zainfekować komputer — [szczegóły >>](#)
- **Anti-Spyware** — skanuje uruchamiane aplikacje w tle — [szczegóły >>](#)
- **Zapora** — kontroluje wymianę danych z innymi komputerami w internecie lub sieci lokalnej — [szczegóły >>](#)
- **LinkScanner** — sprawdza wyniki wyszukiwania wyświetlane przez serwisy internetowe — [szczegóły >>](#)
- **Anti-Rootkit** — wykrywa programy i technologie próbujące ukryć w systemie szkodliwe oprogramowanie — [szczegóły >>](#)
- **Skaner poczty e-mail** — sprawdza wszystkie przychodzące i wychodzące wiadomości e-mail w poszukiwaniu wirusów — [szczegóły >>](#)
- **Licencja** — wyświetla numer, typ i datę wygasnięcia licencji — [szczegóły >>](#)
- **Ochrona Sieci** — skanuje wszystkie dane pobierane przez przeglądarkę internetową — [szczegóły >>](#)
- **Ochrona rezydentna** — działa w tle; skanuje pliki przy ich kopiowaniu, otwieraniu i zapisywaniu — [szczegóły >>](#)
- **Menedżer aktualizacji** — kontroluje wszystkie aktualizacje systemu AVG —

[szczegóły >>](#)

Pojedyncze kliknięcie ikony dowolnego składnika powoduje podświetlenie go w sekcji przeglądu. Jednocześnie u dołu interfejsu użytkownika pojawia się opis funkcji wybranego składnika. Dwukrotne kliknięcie ikony powoduje otwarcie interfejsu konkretnego składnika (z jego opcjami i statystykami).

Kliknięcie prawym przyciskiem ikony składnika powoduje otwarcie menu kontekstowego. Można w nim nie tylko otworzyć graficzny interfejs składnika, ale także wybrać opcję **ignorowania stanu składnika**. Opcje te należy wybrać, jeśli [stan błędu składnika](#) jest znany, ale z dowolnego powodu system AVG ma być nadal używany, a użytkownik nie ma być ostrzegany za pomocą [ikony na pasku zadań](#).


## 7.5. Statystyki


Obszar **Statystyki** znajduje się w lewym dolnym rogu [Interfejsu użytkownika AVG](#). Sekcja ta zawiera szereg informacji o działaniu programu:

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

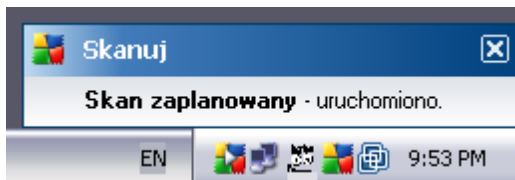
## 7.6. Ikona na pasku zadań

**Ikona na pasku zadań** (na pasku zadań systemu Windows) wskazuje obecny stan systemu **AVG 9 Anti-Virus plus Firewall**. Ikona ta jest zawsze widoczna, niezależnie od tego, czy Interfejs użytkownika AVG jest otwarty, czy też nie.

Jeśli  **ikona na pasku zadań** jest kolorowa, wszystkie składniki systemu AVG są aktywne i w pełni funkcjonalne. Może ona być kolorowa także wtedy, gdy system AVG zasygnalizował błąd, ale użytkownik akceptuje go i celowo [ignoruje stan składników](#).

Ikona z wykrzyknikiem  wskazuje problem (*nieaktywny składnik, stan błędu itp.*). W takim przypadku należy dwukrotnie kliknąć **ikone AVG**, aby otworzyć Interfejs użytkownika i sprawdzić stan składników.

Ikona na pasku zadań informuje również o bieżących aktywnościach systemu AVG i możliwych zmianach stanu programów (*np. automatyczne uruchomienie zaplanowanego skanowania lub aktualizacji, przełączanie profilu Zapory, zmianie stanu składnika, wystąpienie stanu błędu, ...*) dzięki wyskakującym okienkom wyświetlanym nad ikoną AVG:



Dwukrotne kliknięcie **ikony na pasku zadań** pozwala także szybko, w dowolnym momencie uzyskać dostęp do Interfejsu użytkownika systemu AVG. Kliknięcie **ikony na pasku zadań** prawym przyciskiem myszy otwiera menu kontekstowe zawierające następujące opcje:

- **Otwórz Interfejs użytkownika AVG** — otwiera [Interfejs użytkownika](#).
- **Aktualizuj** — uruchamia natychmiastową [aktualizację](#)

## 8. Składniki AVG

### 8.1. Anti-Virus

#### 8.1.1. Zasady działania składnika Anti-Virus

Silnik skanujący programu antywirusowego skanuje wszystkie pliki i wykonywane na nich operacje (otwieranie, zamykanie itd.) w poszukiwaniu znanych wirusów. Każdy wykryty wirus jest blokowany (aby nie mógł wykonywać żadnych szkodliwych działań), a następnie usuwany lub izolowany. Większość programów antywirusowych korzysta także z analizy heurystycznej — pliki są skanowane w poszukiwaniu charakterystycznych cech wirusów - tak zwanych sygnatur. Oznacza to, że skaner antywirusowy może wykryć nowe, nieznane dotąd wirusy, jeśli posiadają one pewne popularne właściwości.

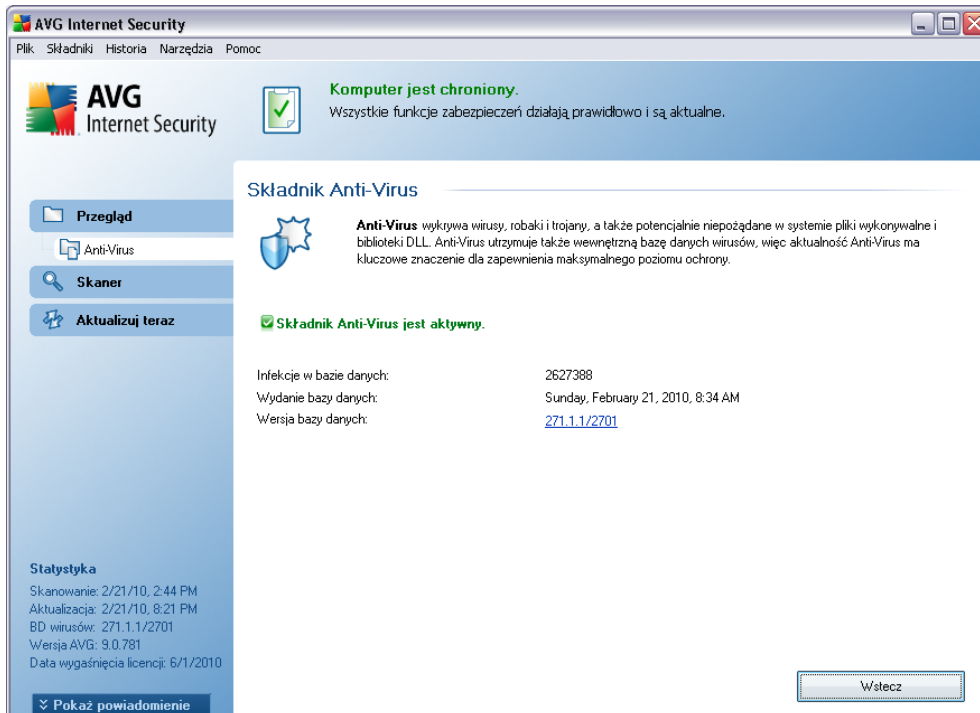
***Ważną zaletą ochrony antywirusowej jest fakt, że nie pozwala ona na uruchomienie żadnych znanych wirusów na komputerze!***

Korzystanie z tylko jednej technologii nie zapewnia stuprocentowej skuteczności wykrywania wirusów, dlatego składnik **Anti-Virus** wykorzystuje jednocześnie kilka metod:

- Skanowanie — wyszukiwanie ciągów znaków typowych dla danego wirusa.
- Analiza heurystyczna — dynamiczna emulacja instrukcji skanowanego obiektu w środowisku maszyny wirtualnej.
- Wykrywanie generyczne — wykrywanie instrukcji typowych dla danego wirusa lub grupy wirusów.

Program AVG jest również w stanie analizować i wykrywać wykonywalne aplikacje i biblioteki DLL, które mogą być potencjalnie niepożądane w Twoim systemie. Takie zagrożenia (różne rodzaje oprogramowania szpiegującego, reklamowego itp.) nazywane są również Potencjalnie Niechcianymi Programami. Ponadto program AVG skanuje rejestr systemu w poszukiwaniu podejrzanych wpisów, a także monitoruje tymczasowe pliki internetowe i śledzące pliki cookie. Umożliwia to traktowanie wszystkich potencjalnie szkodliwych obiektów w ten sam sposób jak infekcji.

## 8.1.2. Interfejs składowika Anti-Virus



Interfejs składowika **Anti-Virus** zawiera krótki opis jego funkcji, informacje o bieżącym stanie (Składowik *Anti-Virus* jest aktywny.), a także krótki przegląd statystyk:

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

Interfejs tego składowika zawiera tylko jeden przycisk (**Wstecz**) — kliknięcie go powoduje powrót do domyślnego [interfejsu użytkownika systemu AVG](#) (przeglądu składowików).

**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składowiki pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu



AVG, należy wybrać z menu głównego **Narzędzia / Ustawienia zaawansowane** i skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

## 8.2. Anti-Spyware

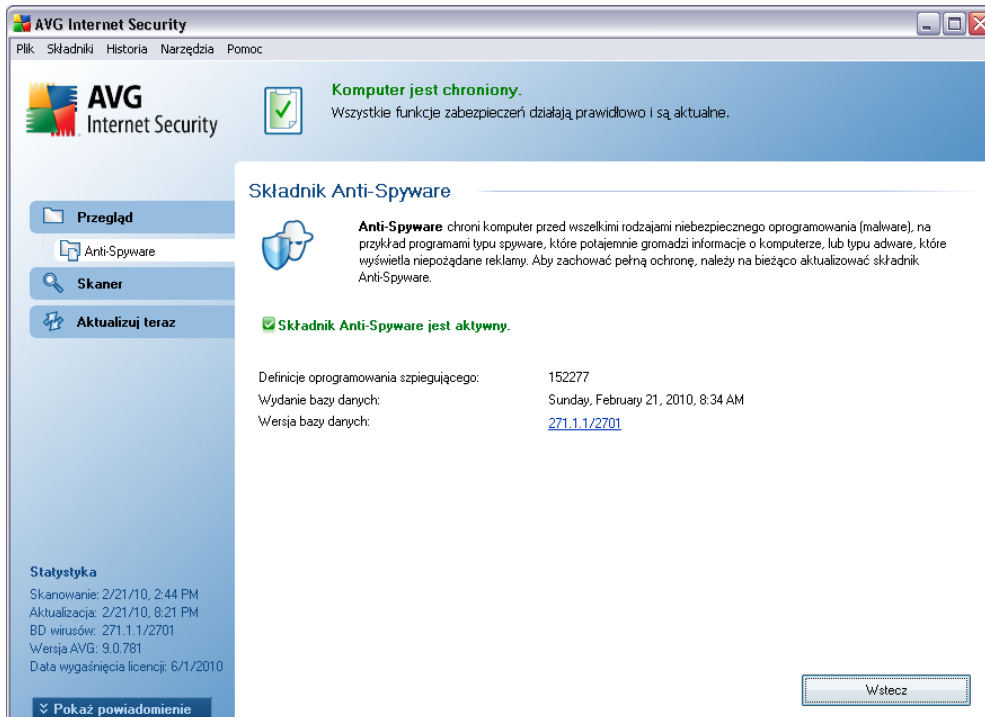
### 8.2.1. Zasady działania składnika Anti-Spyware

Oprogramowanie szpiegujące (spyware) jest zazwyczaj definiowane jako pewien rodzaj szkodliwego oprogramowania, które gromadzi informacje z komputera użytkownika bez jego wiedzy i pozwolenia. Niektóre aplikacje szpiegujące mogą być instalowane celowo i często zawierają reklamy, wyskakujące okna i inne nieprzyjemne elementy.

Obecnie źródłem większości infekcji są potencjalnie niebezpieczne witryny internetowe. Powszechne są również inne metody rozprzestrzeniania, na przykład poprzez e-mail lub w efekcie działalności robaków i wirusów. Najskuteczniejszą ochroną jest stosowanie stale pracującego w tle składnika **Anti-Spyware**, który działa jak ochrona rezydentna i skanuje aplikacje podczas ich uruchamiania.

Istnieje jednak ryzyko, że szkodliwe oprogramowanie znalazło się na komputerze przed zainstalowaniem systemu **AVG 9 Anti-Virus plus Firewall** lub że użytkownik zaniedbał jego aktualizację, nie korzystając z aktualnych [baz wirusów i nowych wersji programu](#). Z tego powodu AVG umożliwia pełne przeskanowanie komputera pod kątem obecności oprogramowania szpiegującego (za pomocą interfejsu skanera). Wykrywa on również szkodliwe oprogramowanie, które jest uspijone lub nie stwarza zagrożenia, czyli takie, które zostało pobrane, ale nie aktywowane.

## 8.2.2. Interfejs składowca Anti-Spyware



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

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

Interfejs tego składowca zawiera tylko jeden przycisk (**Wstecz**) — kliknięcie go powoduje powrót do domyślnego [interfejsu użytkownika systemu AVG](#) (przeglądu składowców).

**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składowce pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego **Narzędzia / Ustawienia zaawansowane** i

skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

### 8.3. Anti-Rootkit

Program typu rootkit to aplikacja zaprojektowana w celu przejęcia całkowitej kontroli nad systemem komputerowym bez zgody jego właścicieli czy upowaznionych administratorów. Bezpośredni dostęp do sprzętu jest rzadko wymagany, ponieważ programy typu rootkit w pełni zdalnie kontrolują system operacyjny komputera. Zwykle ukrywają one swoją obecność myląc lub unikając standardowych mechanizmów bezpieczeństwa systemu operacyjnego. Wiele z nich jest jednocześnie koniami trojańskimi, które dodatkowo starają się przekonać użytkowników, że ich systemy są bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorującymi) oraz plików lub danych przed samym systemem operacyjnym.

### 8.4. Zapora

Zapora internetowa to system, który wymusza stosowanie zasad kontroli dostępu między dwoma lub większą liczbą sieci, blokując lub umożliwiając przepływ danych. Zapora składa się z zestawu reguł, które sterują komunikacją na każdym indywidualnym porcie sieciowym, chroniąc w ten sposób sieć lokalną przed atakami, których źródło znajduje się na zewnątrz (zazwyczaj w internecie). Komunikacja jest oceniana (w oparciu o zdefiniowane reguły), a następnie akceptowana lub blokowana. Jeśli zapora wykryje próbę ataku, blokuje ją i nie pozwala intruzowi przejąć kontroli nad komputerem.

Konfiguracja Zapory pozwala blokować lub dopuszczać komunikację wewnętrzną lub zewnętrzną (zarówno wychodzącą, jak i przychodzącą) na konkretnych portach i dla zdefiniowanych programów. Zapora może np. akceptować tylko ruch WWW, z którego korzysta program Microsoft Internet Explorer. Próba transmisji danych WWW przez jakkolwiek inną przeglądarkę będzie w takim przypadku blokowana.

Zapora chroni również Twoje dane osobowe - nikt nie uzyska ich z Twojego komputera bez wyraźnej zgody. Decyduje też o tym, jak wymieniane są dane z innymi komputerami w sieci lokalnej lub internecie. Zapora w środowisku komercyjnym chroni również pojedyncze komputery przed atakami przeprowadzanymi z wnętrza tej samej sieci.

**Sugestia:** *Generalnie nie zaleca się używania więcej niż jednej zapory internetowej na tym samym komputerze. Zainstalowanie dodatkowych zapór nie zwiększy bezpieczeństwa komputera. Zwiększy się natomiast prawdopodobieństwo, że wystąpią konflikty między tymi dwiema aplikacjami. Dlatego też zalecamy używanie tylko jednej zapory i wyłączenie wszystkich innych. Pozwala to wyeliminować ryzyko konfliktów i wszelkich problemów z tym związanych.*

### 8.4.1. Zasady działania Zapory

W systemie AVG **Zapora** kontroluje cały ruch na każdym porcie sieciowym komputera. Na podstawie zdefiniowanych reguł **Zapora** ocenia uruchomione aplikacje (chcąc nawiązać połączenie z siecią lokalną lub internetem) oraz programy usiłujące z zewnątrz połączyć się z Twoim komputerem. **Zapora** dopuszcza lub blokuje komunikacje tych aplikacji na określonych portach sieciowych. Domyślnie, jeśli aplikacja jest nieznana (tj. nie posiada zdefiniowanych reguł **Zapory**), wyświetlone będzie pytanie, czy jej komunikacja ma zostać zaakceptowana.

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

#### Zapora może wykonać następujące czynności:

- Automatycznie zablokować lub zezwolić na komunikację znanych [aplikacji](#), albo poprosić użytkownika o potwierdzenie
- Korzystać z kompletnych [profilów](#) zawierających wstępnie zdefiniowane reguły (zgodnie z Twoimi potrzebami)
- [Automatycznie przełączać profile](#) przy łączeniu się z różnymi sieciami lub przy używaniu różnych kart sieciowych

### 8.4.2. Profile Zapory

Zapora umożliwia definiowanie określonych reguł bezpieczeństwa w oparciu o środowisko i tryb pracy komputera. **\*\*\*** Każda z opcji wymaga innego poziomu zabezpieczeń, a ich dostosowywanie odbywa się za pomocą odpowiednich profili. Krótko mówiąc, [profil Zapory](#) to określona konfiguracja tego składnika. Dostępna jest pewna liczba wstępnie zdefiniowanych profili. **\*\*\***

#### Dostępne profile

- **Odblokuj wszystko** profil systemowy składnika [Zapora](#) wstępnie skonfigurowany przez producenta; jest zawsze dostępny. Gdy profil ten jest aktywny, cała komunikacja sieciowa jest akceptowana, bez stosowania jakichkolwiek reguł zabezpieczeń - tak, jakby składnik [Zapora](#) był wyłączony (tj. *wszystkie programy mogą wymieniać dane, ale pakiety wciąż obsługiwane są przez sterownik filtra AVG - aby tego uniknąć, całkowicie wyłącz Zaporę*). Tego profilu systemowego nie można powielić ani usunąć, a jego ustawienia nie da się modyfikować.

- **Blokuj wszystko** to profil systemowy składnika **Zapora** wstępnie skonfigurowany przez producenta; jest zawsze dostępny. Gdy zostanie on aktywowany, wszystkie próby komunikacji z siecią będą blokowane. Komputer nie będzie ani dostępny z sieci zewnętrznej, ani nie będzie mógł się z nią połączyć. Tego profilu systemowego nie można powielić ani usunąć, a jego ustawień nie da się modyfikować.
- **Profile niestandardowe:**
  - **Podłączony bezpośrednio do internetu** — odpowiedni dla typowych komputerów stacjonarnych połączonych bezpośrednio z internetem lub dla notebooków łączących się z internetem poza bezpieczną siecią firmową. Opcje te należy wybrać, jeśli łączysz się z siecią w domu małej sieci firmowej (bez centralnej administracji). Opcje te należy wybrać również podczas podróżowania z notebookiem i łączenia się z sieciami nieznanymi i potencjalnie niebezpiecznymi miejscami (*kawiarnie internetowe, pokoje hotelowe itp.*). Zostaną w tym wypadku utworzone bardziej restrykcyjne reguły, ponieważ zakłada się, że komputer taki nie ma zapewnionej żadnej dodatkowej ochrony, dlatego też wymaga maksymalnej troski o bezpieczeństwo.
  - **Komputer w domenie** — odpowiedni dla komputerów pracujących w sieci lokalnej, np. w szkołach lub sieci firmowej. Zakłada się, że wspomniana sieć chroniona jest przy użyciu pewnych dodatkowych środków, więc poziom bezpieczeństwa może być niższy niż dla pojedynczego komputera.
  - **Sieć w domu lub małym biurze** — odpowiedni dla komputerów w mniejszej sieci, np. w domu lub w małej firmie (zazwyczaj tylko kilka komputerów połączonych ze sobą, bez „centralnego” administratora).

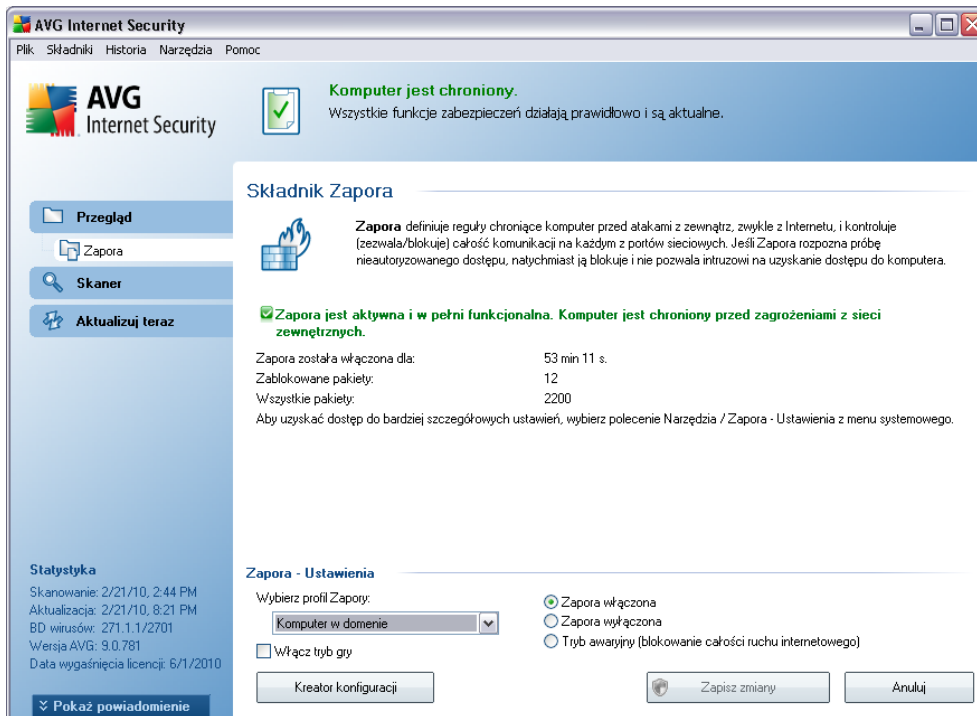
## Przelaczanie profili

Funkcja przeliczania profili umożliwi składnikowi **Zapora** automatyczne przeliczanie się na zdefiniowany wcześniej profil w przypadku użycia określonej karty sieciowej lub połączenia z określonym typem sieci. Jeśli do obszaru sieciowego nie został jeszcze przypisany żaden profil, przy najbliższym połączeniu z tym obszarem **Zapora** wyświetli okno dialogowe z prośbą o przypisanie profilu.

Profile można tworzyć dla dowolnych interfejsów sieciowych lub obszarów. Ich dalsze ustawienia dostępne są w oknie **Profile kart sieciowych i obszarów**, w którym można również w razie potrzeby wyłączyć te funkcje (*w takim przypadku dla każdego rodzaju połączenia będzie używany profil domyślny*).

Zazwyczaj funkcja ta będzie przydatna dla użytkowników laptopów, korzystających z różnych typów połączeń. W przypadku komputera stacjonarnego korzystającego tylko z jednego typu połączenia (tj. *kablowego połączenia z internetem*) funkcja przelaczania profili prawdopodobnie nigdy nie będzie używana.

### 8.4.3. Interfejs Zapory



Interfejs składnika **Zapora** udostępnia niektóre podstawowe informacje na temat funkcji oraz krótkie omówienie statystyk **Zapory**:

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

#### Podstawowa konfiguracja składnika

- **Wybierz profil Zapory** — z menu rozwijanego wybierz jeden ze

zdefiniowanych profili — dwa profile są dostępne przez cały czas (*domyślne profile o nazwach **Odblokuj wszystko** oraz **Blokuj wszystko***). Inne profile zostały dodane ręcznie w wyniku edycji ustawień w oknie [Profile](#) w [Ustawieniach Zapory](#).

- **Włącz tryb gry** — Zaznaczenie tego pola daje pewność, że podczas działania aplikacji pełnoekranowych (gier, prezentacji programu PowerPoint itp.) [Zapora](#) nie będzie wyświetlała okien dialogowych z pytaniami, czy komunikacja dla nieznanego programu ma zostać odblokowana. Jeśli w tym czasie nowy program spróbuje połączyć się z siecią, [Zapora](#) automatycznie odblokuje lub zablokuje tę próbę (zgodnie z ustawieniami bieżącego profilu).
- **Stan Zapory:**
  - **Zapora włączona** — należy zaznaczyć te opcje, aby zezwalać na komunikację wszystkim aplikacjom, którym w zbiorze reguł zdefiniowanych dla wybranego profilu [Zapory](#) przypisano akcje Odblokuj.
  - **Zapora wyłączona** — ta opcja całkowicie wyłącza [Zapora](#). Ruch sieciowy nie będzie blokowany ani monitorowany!
  - **Tryb awaryjny (blokowanie całości ruchu internetowego)** — należy zaznaczyć te opcje, aby blokować cały ruch na wszystkich portach. [Zapora](#) wciąż działa, lecz komunikacja z siecią jest zablokowana.

**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana ustawień Zapory, należy wybrać z menu głównego pozycję **Narzędzia / Ustawienia Zapory** i edytować konfigurację w nowo otwartym oknie dialogowym [Ustawienia Zapory](#).

### Przyciski kontrolne

- **Kreator konfiguracji** — przycisk ten pozwala przejść do okna *Wybór typu komputera (używanego podczas instalacji)*, w którym można skonfigurować działanie [Zapory](#).
- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — kliknięcie tego przycisku powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG \(przeglądu składników\)](#).

## 8.5. Skaner poczty e-mail

Poczta e-mail to od dawna częste źródło wirusów i koni trojańskich. Wyludzenia danych i spam powodują, że stała się ona jeszcze większym zagrożeniem. Darmowe konta pocztowe są szczególnie narażone na otrzymywanie szkodliwych wiadomości e-mail, *gdyż rzadko korzystają z technologii antyspamowych*, a domowi użytkownicy najczęściej używają właśnie takich kont. Dodatkowo odwiedzają oni nieznane witryny i wpisują w formularzach dane osobowe (*takie jak adres e-mail*), co powoduje, że w jeszcze większym stopniu narażają się na ataki za pośrednictwem poczty e-mail. Firmy używają na ogół komercyjnych kont pocztowych, które w celu ograniczenia ryzyka korzystają z filtrów antyspamowych i innych środków bezpieczeństwa.

### 8.5.1. Zasady działania Skanera poczty e-mail

Składnik **Skaner poczty e-mail** automatycznie skanuje pocztę przychodzącą i wychodzącą. Można z niego korzystać przy programach pocztowych, dla których nie powstały pluginy AVG (*np. Outlook Express, Mozilla, Incredimail itd.*).

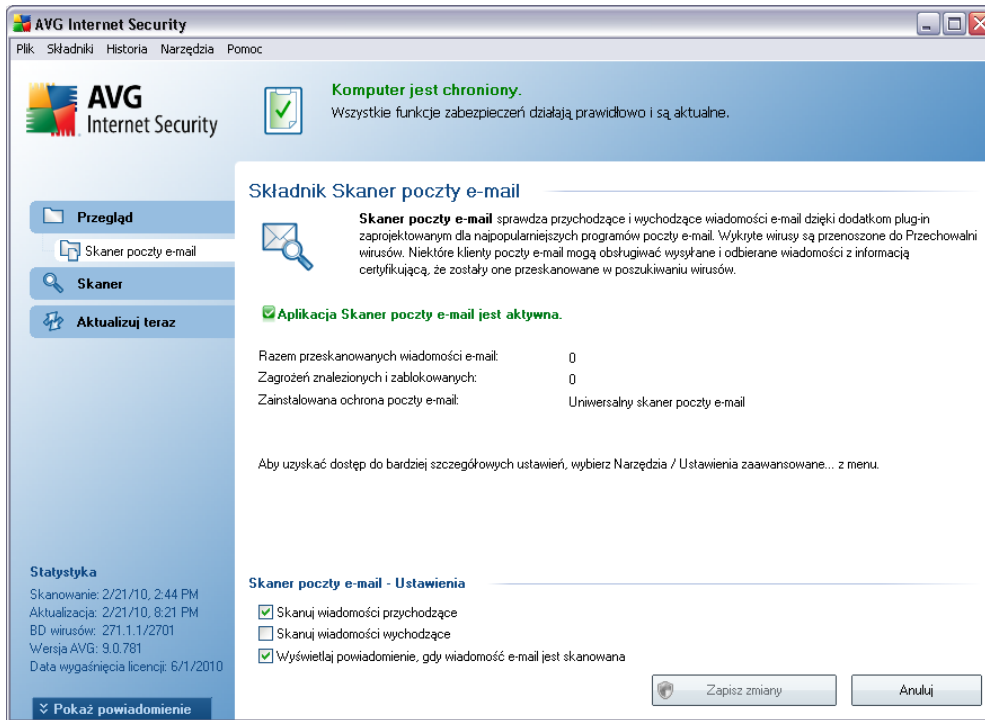
Podczas [instalacji](#) systemu AVG tworzone są automatyczne serwery kontrolujące pocztę e-mail: jeden do sprawdzania wiadomości przychodzących, drugi do wychodzących. Przy pomocy tych serwerów wiadomości e-mail są automatycznie sprawdzane na portach 110 i 25 (*standardowe porty dla wysyłania/odbierania poczty e-mail*).

**Skaner poczty e-mail** pośredniczy między programem pocztowym a zewnętrznymi serwerami pocztowymi.

- **Poczta przychodząca:** Podczas otrzymywania wiadomości z serwera, **Skaner poczty e-mail** sprawdza ją w poszukiwaniu wirusów, usuwa zainfekowane załączniki i dołącza certyfikat. Wykryte wirusy są natychmiast poddawane kwarantannie w [Przechowalni wirusów](#). Wiadomość jest później przekazywana do programu pocztowego.
- **Poczta wychodząca:** Wiadomość jest wysyłana z programu pocztowego do składnika Skaner poczty e-mail, gdzie jest sprawdzana wraz z załącznikami w poszukiwaniu wirusów. Następnie wiadomość jest wysyłana do serwera SMTP (*skanowanie wychodzących wiadomości e-mail jest domyślnie wyłączone i można je skonfigurować ręcznie*).

**Uwaga:** Skaner poczty e-mail nie jest przeznaczony dla platform serwerowych!

## 8.5.2. Interfejs Skanera poczty e-mail



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

- **Razem przeskanowanych wiadomości e-mail** — liczba wiadomości e-mail przeskanowanych od czasu ostatniego uruchomienia skłladnika **Skaner poczty e-mail** (w razie potrzeby ta wartosc moze zostac zresetowana, np. dla celów statystycznych — *Resetuj wartosc*)
- **Zagrożeń znalezionych i zablokowanych** — liczba zainfekowanych wiadomości wykrytych od czasu ostatniego uruchomienia **Skanera poczty e-mail**.
- **Zainstalowany plugin poczty e-mail** — informacje o pluginie odpowiednim dla Twojego domyślnego klienta poczty

### Podstawowa konfiguracja skłladnika

W dolnej czesci okna znajduje sie sekcja **Skaner poczty e-mail - Ustawienia** , w

której można skonfigurować podstawowe funkcje składnika:

- **Skanuj wiadomości przychodzące** — pozycje te należy zaznaczyć, aby wszystkie wiadomości e-mail przychodzące na dane konto pocztowe były skanowane w poszukiwaniu wirusów. Domyślnie ta opcja jest włączona i nie zaleca się zmian w tych ustawieniach!
- **Skanuj wiadomości wychodzące** — zaznaczenie tej opcji pozwala określić, czy powinny być skanowane wszystkie wiadomości e-mail wysyłane z konta pocztowego. Opcja ta jest domyślnie wyłączona.
- **Wyswietlaj ikony powiadomienia, gdy wiadomość e-mail jest skanowana** — pozycje należy zaznaczyć, jeśli nad ikoną AVG na pasku zadań ma być wyświetlane odpowiednie okno powiadomienia w chwili, gdy poczta jest skanowana przez składnik [Skaner poczty e-mail](#). Domyślnie ta opcja jest włączona i nie zaleca się zmian w tych ustawieniach!

Dostęp do zaawansowanej konfiguracji **Skamera poczty e-mail** można uzyskać z poziomu menu **Narzędzia / Ustawienia zaawansowane**. Wszelkie zmiany w konfiguracji powinny być wprowadzane wyłącznie przez doświadczonych użytkowników!

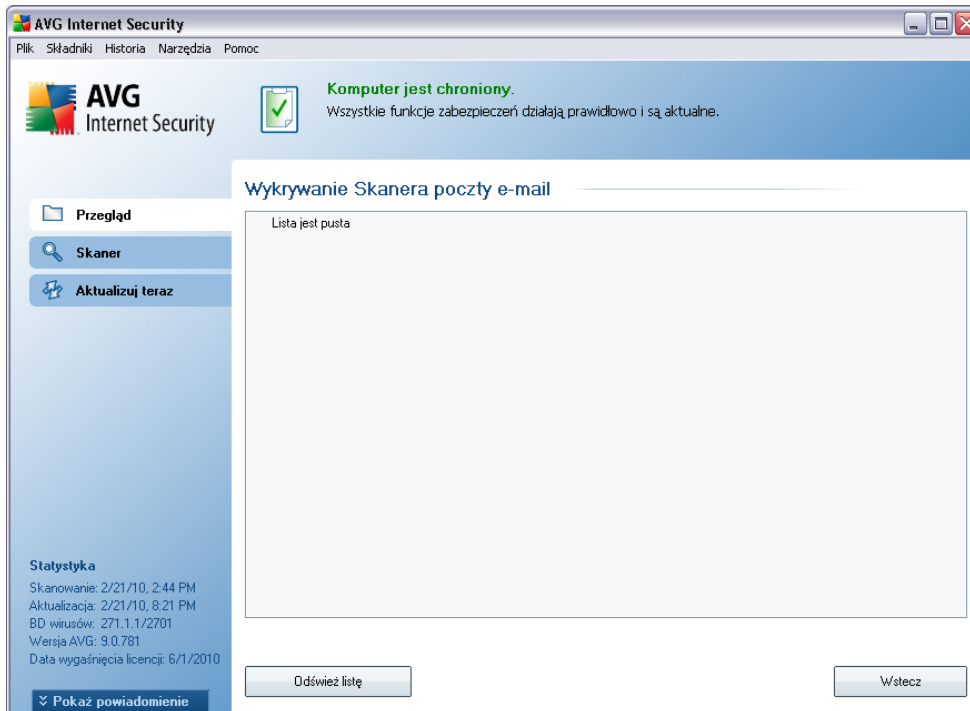
**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego **Narzędzia / Ustawienia zaawansowane** i skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

## Przyciski kontrolne

W interfejsie **Skamera poczty e-mail** dostępne są następujące przyciski kontrolne:

- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — kliknięcie tego przycisku powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

### 8.5.3. Zagrozenia wykryte przez Skaner poczty e-mail



W oknie **Zagrozenia wykryte przez Skaner poczty e-mail** (dostepnym po wybraniu odpowiedniej opcji z menu *Historia*) wyswietlana jest lista wszystkich obiektów wykrytych przez składnik **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.
- **Czas wykrycia** — data i godzina wykrycia podejrzanego obiektu.
- **Typ obiektu** — typ wykrytego obiektu.

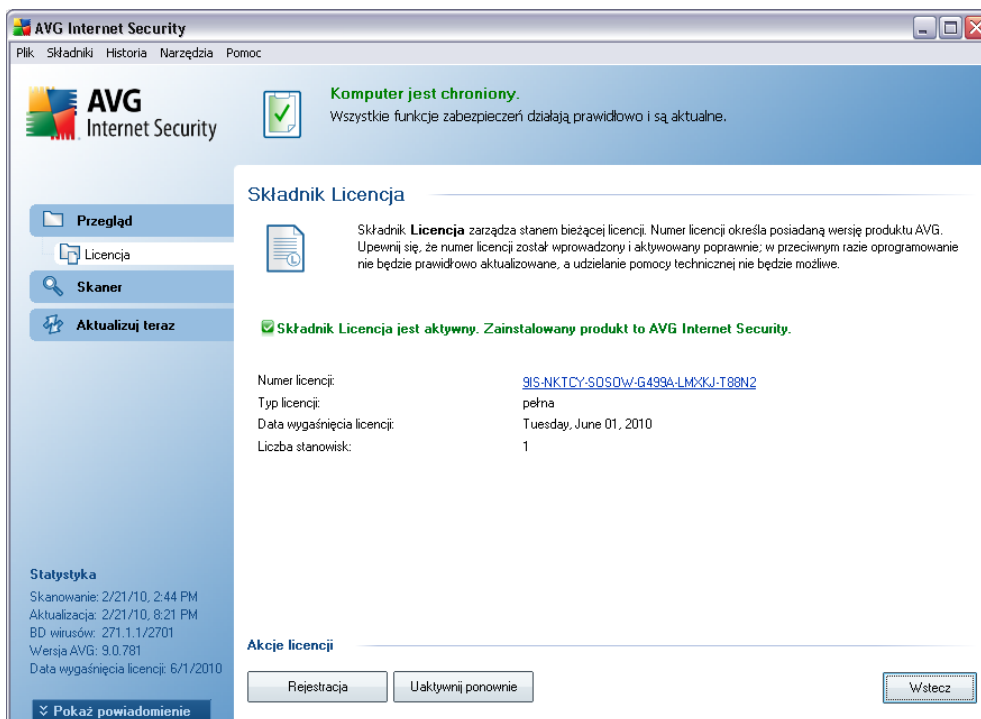
U dolu okna znajduja sie informacje na temat laczonej liczby wykrytych infekcji. Ponadto, mozna wyeksportowac cala liste obiektów do pliku, (**Eksportuj liste do pliku**) lub usunac wszystkie jej pozycje (**Opróżnij liste**).

## Przyciski kontrolne

W interfejsie składnika **Skaner poczty e-mail** dostępne są następujące przyciski sterujące:

- **Odśwież listę** – aktualizuje listę wykrytych zagrożeń.
- **Wstecz** – przełącza z powrotem do domyślnego [Interfejsu użytkownika systemu AVG](#) (przeglądu składników).

## 8.6. Licencja



Okno dialogowe składnika **Licencja** zawiera krótki opis jego funkcji, informacje o jego bieżącym stanie (Składnik Licencja *jest aktywny.*), a także następujące informacje:

- **Numer licencji** – dokładny numer licencji. Jeżeli kiedykolwiek będziesz proszony o podanie swojego numeru licencji, użyj go w tej samej formie. Dlatego też zdecydowanie zalecamy korzystanie z metody kopiuj-wklej w przypadku jakiegokolwiek manipulacji numerem licencji.

- **Typ licencji** — określa typ zainstalowanego produktu.
- **Data wygasnięcia licencji** — data określająca okres ważności licencji. Aby korzystać z systemu **AVG 9 Anti-Virus plus Firewall** po tej dacie, należy odnowić licencje. [Licencje można odnowić online](http://www.avg.com/) za pośrednictwem witryny firmy AVG (<http://www.avg.com/>).
- **Liczba stanowisk** — liczba stacji roboczych, na których można zainstalować system **AVG 9 Anti-Virus plus Firewall**.

### Przyciski kontrolne

- **Zarejestruj** — łączy się ze stroną rejestracji w witrynie internetowej systemu AVG (<http://www.avg.com/>). Należy tam podać swoje dane rejestracyjne — jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.
- **Uaktywnij ponownie** — otwiera okno dialogowe **Aktywacja programu AVG** zawierające dane wprowadzone na etapie **Personalizacji programu AVG** podczas **Instalacji**. W oknie tym można wprowadzić numer licencji w celu zastąpienia numeru sprzedaży (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*).

**Uwaga:** W przypadku korzystania z próbnej wersji systemu **AVG 9 Anti-Virus plus Firewall**, **dostępne przyciski to Kup teraz i Aktywuj**. Umożliwiają one uaktualnienie programu do jego pełnej wersji. W przypadku systemu **AVG 9 Anti-Virus plus Firewall** zainstalowanego z numerem sprzedaży, te przyciski to **Zarejestruj i Aktywuj**.

- **Wstecz** — kliknięcie tego przycisku powoduje powrót do domyślnego [Interfejsu użytkownika systemu AVG](#) (przeglądu składników).

## 8.7. LinkScanner

### 8.7.1. Zasady działania technologii LinkScanner

Składnik **LinkScanner**® zapewnia darmową ochronę przed witrynami internetowymi, które zdolne są do instalowania na komputerze szkodliwego oprogramowania za pośrednictwem przeglądarki internetowej lub jej pluginów. Technologia składnika **LinkScanner** składa się z dwóch funkcji: [AVG Search-Shield](#) i [AVG Active Surf-Shield](#)

:

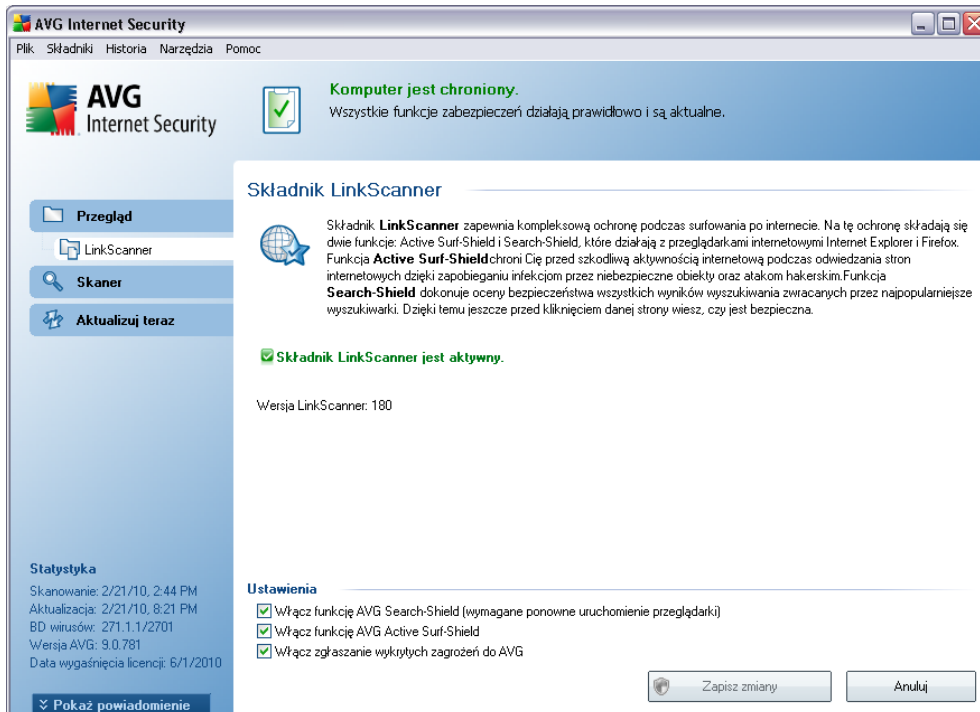
- **Składnik** *ΑςΓ Σεαρχη Σηιελδ* zawiera listę witryn sieci Web (*adresów URL*), które uznane zostały za niebezpieczne. Wszystkie wyniki wyszukiwania serwisów Google, Yahoo!, Bing, Baidu, Yandex i Altavista są sprawdzane na podstawie tej listy, a następnie obok każdego z nich wyświetlana jest odpowiednia ikona klasyfikacji bezpieczeństwa. (w przypadku wyników wyszukiwania serwisu Yahoo! wyświetlane są tylko ikony „niebezpieczna witryna”). Jeśli bezpośrednio w przeglądarce wprowadzony zostanie jakikolwiek adres, kliknięty zostanie link na stronie WWW lub np. w wiadomości e-mail, AVG automatycznie go przeskanuje i — w razie potrzeby — adres zostanie zablokowany.
- **Składnik AVG Active Surf-Shield** skanuje zawartość odwiedzanych witryn internetowych bez względu na ich adres. Nawet jeśli jakaś witryna nie zostanie wykryta przez składnik **AVG Search Shield** (np. gdy utworzono nową szkodliwą witrynę sieci Web lub witryna wcześniej uznana za nieszkodliwą zawiera aktualnie niebezpieczny kod), przy próbie jej odwiedzenia zostanie ona przeskanowana (a w razie podejrzenia zablokowana) przez składnik **AVG Active Surf-Shield**.

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

### 8.7.2. Interfejs LinkScanner

Składnik **LinkScanner** składa się z dwóch funkcji, które można włączyć lub wyłączyć w jego interfejsie:

Interfejs składnika **LinkScanner** zawiera krótki opis jego funkcji oraz informacje na temat jego bieżącego stanu (*Składnik LinkScanner jest aktywny*). Co więcej, można tam znaleźć informacje o numerze wersji najnowszej bazy danych składnika **LinkScanner** (*Wersja składnika LinkScanner*).




W dolnej części okna dialogowego możliwa jest edycja następujących opcji:


- **Włącz składnik AVG Search-Shield** (opcja domyślnie włączona) — skanuje wszystkie łącza pojawiające się w wynikach wyszukiwania serwisów Google, Yahoo!, Bing, Baidu, Yandex i Altavista, a następnie obok każdego z nich wyświetla odpowiednią klasyfikację bezpieczeństwa.
- **Włącz funkcję AVG Active Surf-Shield** — (domyślnie włączona): aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (w czasie rzeczywistym). Znane złośliwe witryny i ich niebezpieczna zawartość blokowane są już w momencie otwarcia ich przez użytkownika za pomocą przeglądarki (lub jakiegokolwiek innej aplikacji korzystającej z protokołu HTTP).
- **Włącz zgłaszanie wykrytych zagrożeń do firmy AVG** — należy zaznaczyć to pole, aby włączyć raportowanie exploitów oraz niebezpiecznych witryn znalezionych przy użyciu funkcji **Safe Surf** lub **Safe Search**. Informacje te są przekazywane do naszej bazy danych.


### 8.7.3. AVG Search-Shield


Podczas surfowania po internecie z włączonym składnikiem **AVG Search-Shield** wszystkie wyniki zwracane przez najbardziej popularne wyszukiwarki internetowe, np. Yahoo!, Google, Bing, Altavista, Yandex itd. są oceniane pod kątem obecności niebezpiecznego lub podejrzanego kodu. Sprawdzając te łącza i oznaczając niebezpieczne, składnik **AVG Link Scanner** ostrzega przed przejściem na niebezpieczną lub podejrzaną stronę. Dzięki temu można mieć pewność, że odwiedza się tylko bezpieczne witryny internetowe.


Obok ocenianego aktualnie wyniku wyszukiwania wyświetlany jest symbol informujący o trwającym sprawdzaniu łącza. Po zakończeniu skanowania wyświetlana jest ikona informująca o jego wynikach:

 Strona, do której prowadzi łącze, jest bezpieczna (w wyszukiwarce Yahoo! ta ikona nie jest wyświetlana na [pasku narzędzi AVG Security Toolbar!](#)).

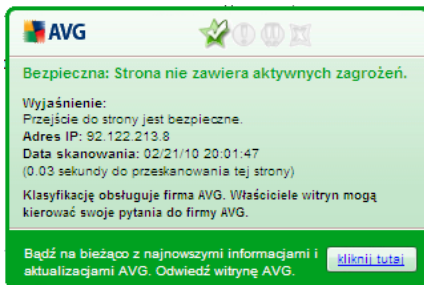
 Strona, do której prowadzi łącze, nie zawiera zagrożeń, ale jest podejrzana (wątpliwości budzi jej pochodzenie lub przeznaczenie, więc nie zaleca się dokonywania na niej zakupów itp.).

 Strona, do której prowadzi łącze, jest bezpieczna, ale zawiera łącza do potencjalnie niebezpiecznych stron lub podejrzanego kodu (który jednak nie stanowi bezpośredniego zagrożenia).

 Strona, do której prowadzi łącze, zawiera aktywne zagrożenia! Dla bezpieczeństwa użytkownika dostęp do tej strony zostanie zablokowany.

 Strona, do której prowadzi łącze, nie jest dostępna i nie udało się jej przeskanować.

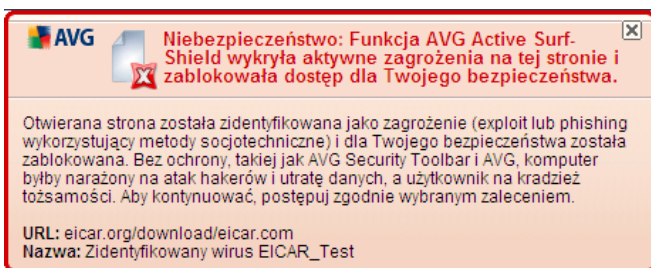
Umieszczenie kursora na wybranej ikonie wyników sprawdzania powoduje wyświetlenie szczegółowych informacji o danym łączu. Informacje te obejmują dodatkowe szczegóły dotyczące zagrożenia (jeśli są dostępne), adres IP serwera docelowego, oraz czas skanowania strony przez produkt AVG:



#### 8.7.4. AVG Active Surf-Shield

Ta zaawansowana funkcja ochrony blokuje szkodliwa zawartość dowolnej otwieranej witryny internetowej, zapobiegając pobraniu jej na dysk twardy. Gdy funkcja ta jest włączona, kliknięcie linku lub wpisanie adresu URL prowadzącego do niebezpiecznej witryny powoduje automatycznie zablokowanie jej otwarcia, dzięki czemu komputer nie zostanie nieswiadomie zainfekowany. Należy pamiętać, że nawet samo wyświetlenie niebezpiecznej witryny internetowej może zainfekować komputer. Dlatego też, gdy zostanie wywołana strona zawierająca kod wykorzystujący luki zabezpieczeń lub inne poważne zagrożenia, składnik [AVG Link Scanner](#) nie pozwoli na jej wyświetlenia w przeglądarce.

Jeśli kiedykolwiek trafisz na szkodliwą stronę internetową, [składnik Link Scanner](#) wyświetli w przeglądarce ostrzeżenie podobne do tego:



***Odwiedzanie takiej witryny jest bardzo ryzykowne i należy tego unikać!***

### 8.8. Ochrona Sieci

#### 8.8.1. Zasady działania składnika Ochrona Sieci

**Ochrona Sieci** to rodzaj programu rezydentnego, zapewniającego ochronę w czasie rzeczywistym. Skanuje on zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików) jeszcze zanim zostaną wyświetlone w przeglądarce

lub pobrane na dysk twardy.

**Ochrona Sieci** wykrywa strony zawierające niebezpieczny kod javascript i blokuje ich ładowanie. Ponadto, identyfikuje szkodliwe oprogramowanie zawarte na stronach WWW i w razie podejrzenia zatrzymuje pobieranie, aby nie dopuścić do infekcji komputera.

**Uwaga:** *Ochrona Sieci nie jest przeznaczona dla platform serwerowych!*

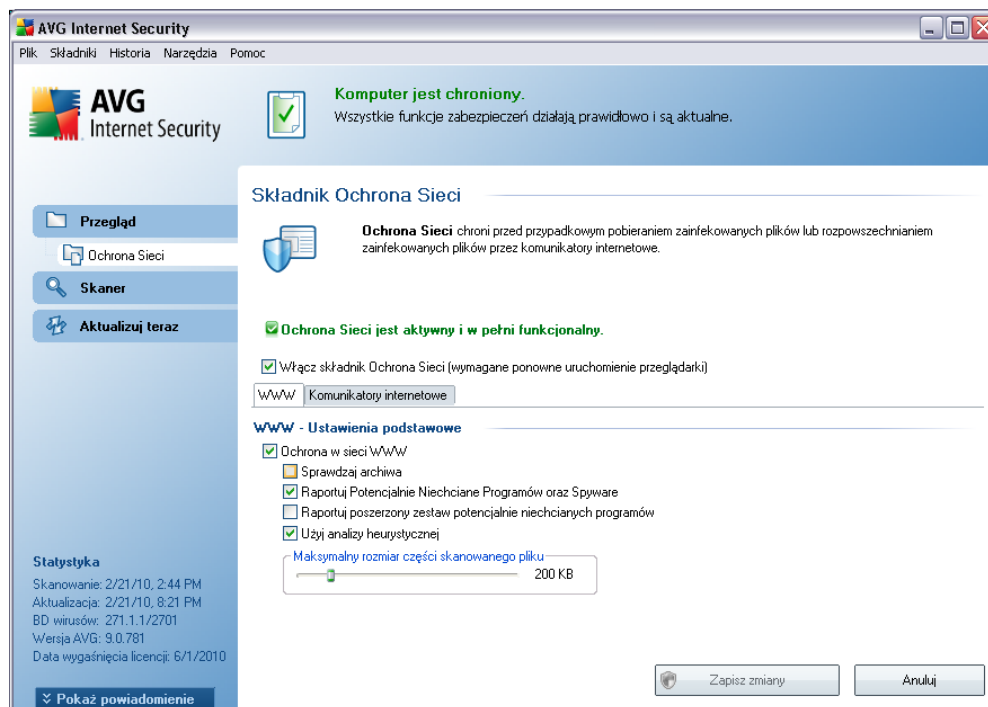
### 8.8.2. Interfejs składnika Ochrona Sieci

Interfejs składnika **Ochrona Sieci** opisuje działanie tego rodzaju ochrony. Znajdują się tam informacje na temat jej bieżącego stanu (*Składnik Ochrona Sieci jest aktywny i w pełni funkcjonalny.*). W dolnej części okna widoczne są podstawowe opcje Ochrony sieci WWW.

#### Podstawowa konfiguracja składnika

Najistotniejszą opcją umożliwia natychmiastowe włączenie lub wyłączenie składnika **Ochrona Sieci** (można to zrobić, zaznaczając lub usuwając zaznaczenie pola **Włącz Ochronę Sieci**). Opcja ta jest domyślnie włączona, a składnik **Ochrona Sieci** aktywny. Jednak jeśli nie istnieją ważne powody do zmiany tego ustawienia, zaleca się pozostawienie składnika aktywnego. Jeśli to pole jest zaznaczone, a składnik **Ochrona Sieci** jest włączony, na dwóch kolejnych kartach znajdują się dalsze opcje konfiguracji:

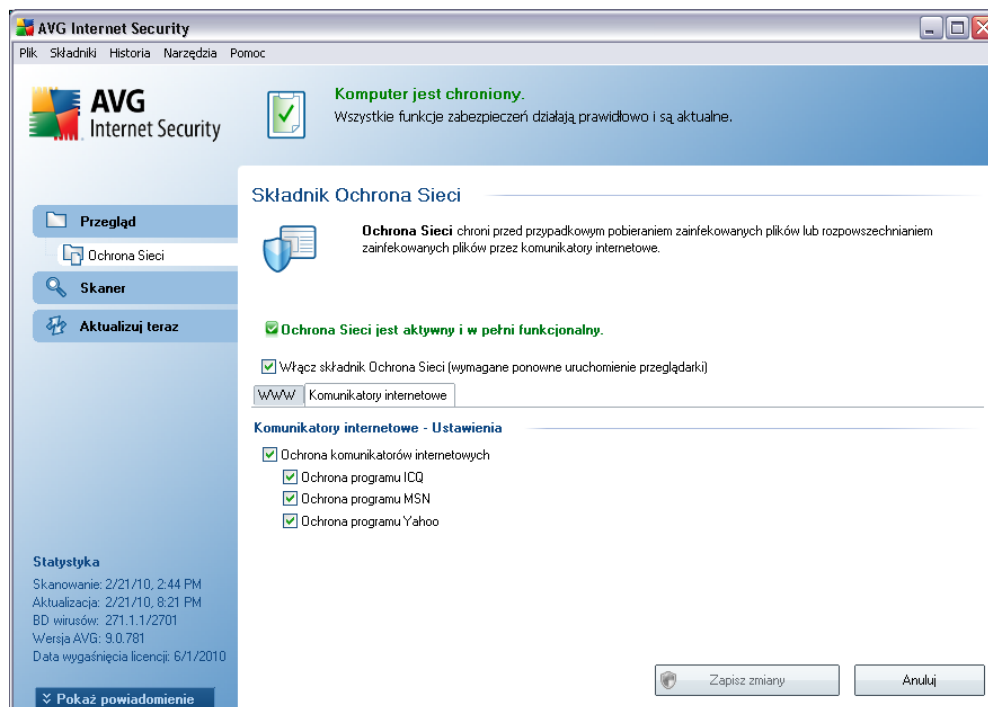
- **WWW** — karta odpowiadająca za skanowanie zawartości witryny internetowych. Interfejs pozwala modyfikować następujące ustawienia:



- **Ochrona sieci WWW** — potwierdza, że składnik **Ochrona Sieci** ma skanować zawartość stron internetowych. Jeśli ta opcja jest aktywna (domyślnie), można włączyć lub wyłączyć następujące funkcje:
  - **Skanuj wewnątrz archiwów** — skanowanie ma obejmować także archiwa dostępne na odwiedzanych stronach WWW.
  - **Raportuj zagrożenia potencjalnie niechcianymi programami i oprogramowaniem szpiegującym** (opcja domyślnie włączona) — zaznaczenie tego pola powoduje włączenie silnika **Anti-Spyware** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączenia tej opcji — znacząco zwiększa ona poziom ochrony komputera
  - **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości oprogramowania szpiegującego, czyli programów, które są zupełnie

bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- **Użyj heurystyki** — skanowanie zawartości wyświetlanych stron ma wykorzystywać analizę heurystyczną, czyli dynamiczną symulację i ocenę instrukcji skanowanego obiektu w wirtualnym środowisku. Dlatego też metoda ta pozwala wykryć nawet taki szkodliwy kod, który nie został jeszcze opisany w bazie danych wirusów (*patrz rozdział [Zasady działania składowika Anti-Virus](#)*).
- **Maksymalny rozmiar skanowanych plików** — jeśli wyświetlana strona zawiera pliki, można skanować ich zawartość jeszcze przed pobraniem na twardy dysk. Ponieważ jednak skanowanie obszernych plików zajmuje dłuższy czas, otwieranie stron WWW może zostać znacznie spowolnione. Za pomocą tego suwaka można określić maksymalny rozmiar plików, które mają być skanowane przez składowik **Ochrona Sieci**. Nawet jeśli pobierany plik jest większy od wybranego limitu i nie zostanie przeskanowany przez **Ochronę Sieci**, nie zmniejsza to Twojego bezpieczeństwa: jeśli plik jest zainfekowany, składowik **Ochrona rezydentna** natychmiast to wykryje.
- **Komunikatory internetowe** — karta umożliwiająca edycję ustawień monitorowania komunikatorów internetowych (*np. ICQ, MSN Messenger, Yahoo itp.*).



- Ochrona komunikatorów internetowych — zaznacz to pole, jeśli chcesz, aby Ochrona Sieci zapewniała bezpieczeństwo komunikacji online. O ile opcja ta jest zaznaczona, można dodatkowo określić, które komunikatory internetowe mają być kontrolowane — aktualnie program **AVG 9 Anti-Virus plus Firewall** obsługuje aplikacje ICQ, MSN oraz Yahoo.

**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego **Narzędzia / Ustawienia zaawansowane** i skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

### Przyciski kontrolne

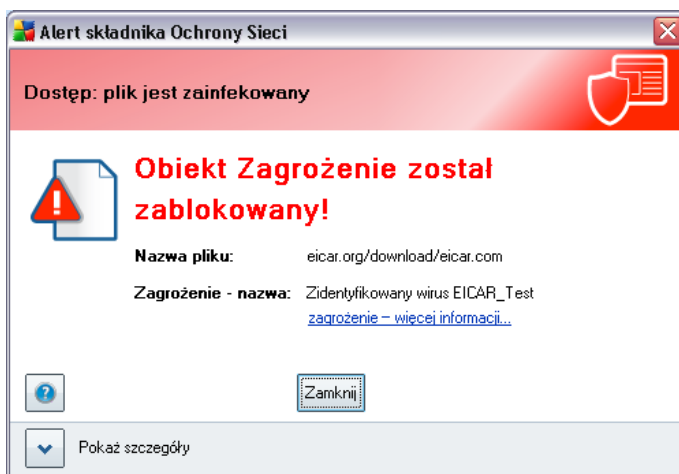
W interfejsie składnika **Ochrona rezydentna** dostępne są następujące przyciski kontrolne:

- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.

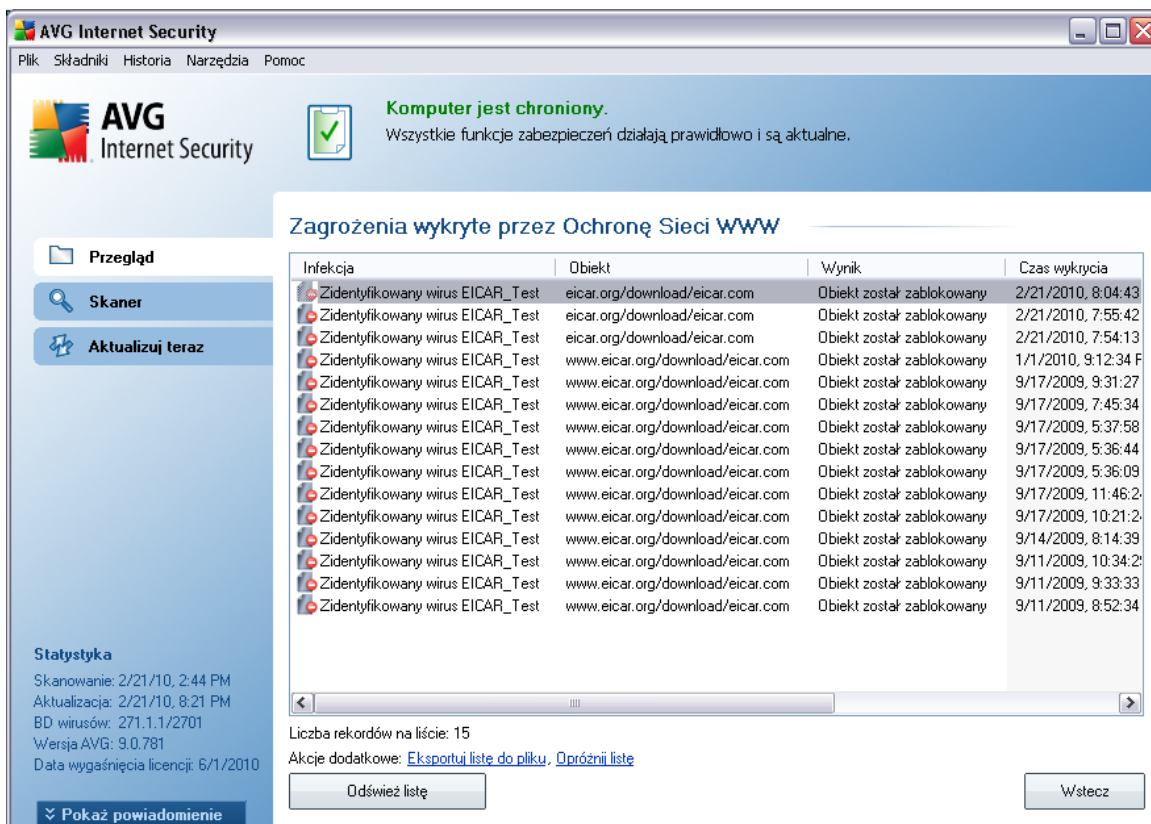
- **Anuluj** — powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

### 8.8.3. Obiekt wykryty przez składnik Ochrona Sieci

**Ochrona Sieci** skanuje zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików) jeszcze zanim zostaną wyświetlone w przeglądarce lub pobrane na dysk twardy. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego okna:



Podejrzana strona nie zostanie otwarta, a wykryty obiekt zostanie zapisany na liście **zagrożeń wykrytych przez Ochronę Sieci** (ten przegląd wykrytych zagrożeń jest dostępny z menu systemowego po wybraniu opcji [Historia / Zagrożenia wykryte przez Ochronę Sieci](#)).



AVG Internet Security

Plik Składniki Historia Narzędzia Pomoc

**AVG Internet Security**

**Komputer jest chroniony.**  
Wszystkie funkcje zabezpieczeń działają prawidłowo i są aktualne.

Zagrożenia wykryte przez Ochronę Sieci WWW

Infekcja	Obiekt	Wynik	Czas wykrycia
Zidentyfikowany wirus EICAR_Test	eicar.org/download/eicar.com	Obiekt został zablokowany	2/21/2010, 8:04:43
Zidentyfikowany wirus EICAR_Test	eicar.org/download/eicar.com	Obiekt został zablokowany	2/21/2010, 7:55:42
Zidentyfikowany wirus EICAR_Test	eicar.org/download/eicar.com	Obiekt został zablokowany	2/21/2010, 7:54:13
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	1/1/2010, 9:12:34 F
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 9:31:27
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 7:45:34
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 5:37:58
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 5:36:44
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 5:36:09
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 11:46:2
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/17/2009, 10:21:2
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/14/2009, 8:14:39
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/11/2009, 10:34:2
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/11/2009, 9:33:33
Zidentyfikowany wirus EICAR_Test	www.eicar.org/download/eicar.com	Obiekt został zablokowany	9/11/2009, 8:52:34

Statystyka  
Skanowanie: 2/21/10, 2:44 PM  
Aktualizacja: 2/21/10, 8:21 PM  
BD wirusów: 271.1.1/2701  
Wersja AVG: 9.0.781  
Data wygaśnięcia licencji: 6/1/2010

Liczba rekordów na liście: 15  
Akcje dodatkowe: [Eksportuj listę do pliku](#), [Opróżnij listę](#)

Odśwież listę Wstecz

Podawane są tam następujące informacje:

- **Infekcja** — opis (ewentualnie nazwa) wykrytego zagrożenia.
- **Obiekt** — źródło obiektu (strona WWW)
- **Wynik** — działanie podjęte w związku z wykryciem.
- **Czas wykrycia** — data i godzina wykrycia i zablokowania zagrożenia
- **Typ obiektu** — typ wykrytego obiektu.
- **Proces** — akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co umożliwiło jego wykrycie).

U dołu okna znajdują się informacje na temat łącznej liczby wykrytych infekcji. Ponadto, można wyeksportować całą listę obiektów do pliku, (**Eksportuj listę do pliku**) lub usunąć wszystkie jej pozycje (**Opróżnij listę**). Przycisk **Odśwież listę** pozwala

zaktualizowac liste obiektów wykrytych przez składnik **Ochrona Sieci**. Przycisk **Wstecz** przelacza z powrotem do domyślnego okna [Interfejsu użytkownika systemu AVG](#) (przeglądu składników).

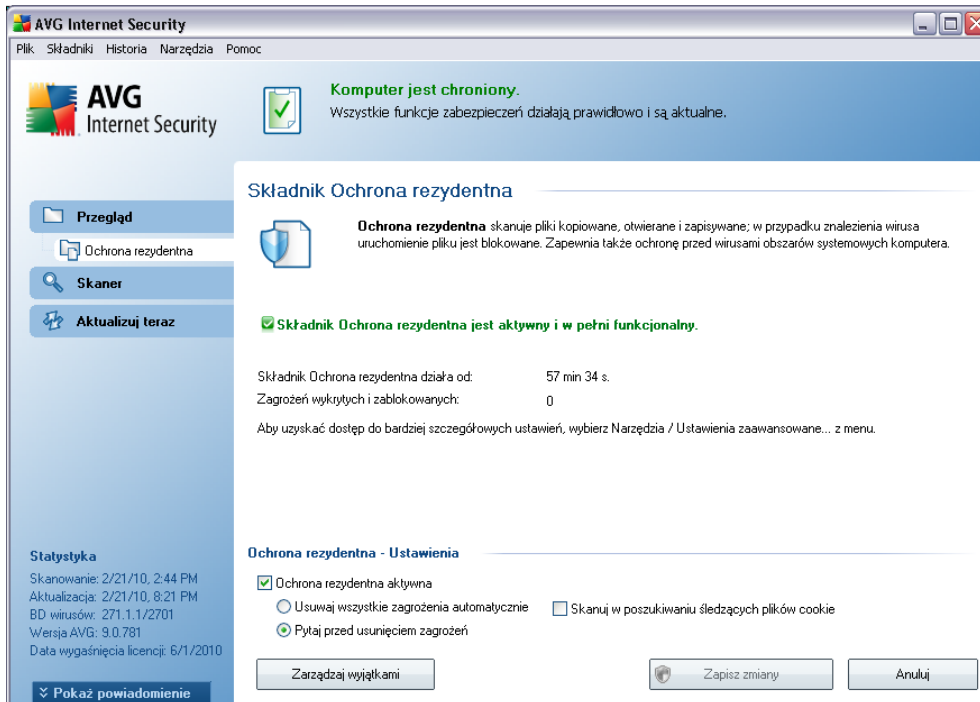
## 8.9. Ochrona rezydentna

### 8.9.1. Zasady działania Ochrony rezydentnej

Składnik **Ochrona rezydentna** zapewnia stała ochronę komputera. Składnik ten skanuje każdy otwierany, zapisywany lub kopiowany plik, oraz chroni obszary systemowe komputera. Po wykryciu wirusa w przetwarzanym pliku, **Ochrona rezydentna** zatrzymuje aktualnie wykonywane operacje i uniemożliwia uaktywnienie się wirusa. Użytkownik zwykle nie zauważa działania tego składnika, ponieważ funkcjonuje ona „w tle” i wyświetla powiadomienia tylko w przypadku, gdy wykryje zagrożenie. Domyślna reakcja **Ochrony rezydentnej** jest zablokowanie dostępu do niebezpiecznego pliku. Składnik **Ochrona rezydentna** jest ładowany do pamięci komputera podczas uruchamiania systemu.

**Ostrzeżenie: Ochrona rezydentna ładowana jest do pamięci komputera podczas uruchamiania systemu i musi pozostać włączona przez cały czas!**

## 8.9.2. Interfejs składowika Ochrona rezydentna



Oprócz przeglądu najważniejszych statystyk oraz informacji na temat stanu składowika (*składnik Ochrona rezydentna jest aktywny i w pełni funkcjonalny*), interfejs **Ochrony rezydentnej** oferuje także kilka elementarnych opcji konfiguracyjnych. Wyszwytlane sa następujące statystyki:

- **Ochrona Rezydenta działa od** — określa czas, jaki upłynął od ostatniego uruchomienia składowika.
- **Zagrożenia wykryte i zablokowane** — liczba wykrytych infekcji, do których uruchomienia/otwarcia nie dopuszczono (*w razie potrzeby ta wartość może zostać zresetowana, np. do celów statystycznych — Resetuj wartość*)

### Podstawowa konfiguracja składowika

W dolnej części okna dialogowego znajduje się sekcja o nazwie **Ochrona rezydentna — Ustawienia**, w której można edytować niektóre jej podstawowe funkcje (*szczegółowa konfiguracja, podobnie jak w wypadku innych składowików, dostępna jest za pośrednictwem menu Narzędzia/Ustawienia zaawansowane*).

Pole **Ochrona rezydentna aktywna** umożliwia łatwe włączanie/wyłączanie Ochrony rezydentnej. Domyślnie funkcja ta jest włączona. Gdy Ochrona rezydentna jest włączona, można określić w jaki sposób ma reagować na wykryte infekcje:

- o automatycznie (**Usuwać wszystkie zagrożenia automatycznie**)
- o lub tylko za zgodą użytkownika (**Pytaj przed usunięciem zagrożen**).

Wybór ten nie ma wpływu na poziom bezpieczeństwa — umożliwia on jedynie podjęcie każdorazowej decyzji o usunięciu lub pozostawieniu wykrytych infekcji.

W obu przypadkach można określić, czy pliki mają być **skanowane w poszukiwaniu sledzacych plików cookie**. W konkretnych wypadkach można włączyć te opcje, aby osiągnąć najwyższy poziom ochrony, ale domyślnie jest ona wyłączona. (pliki cookie to dane tekstowe wysyłane przez serwer do przeglądarki, która przy następnych odwiedzinach na danej stronie udostępni je serwerowi w celach identyfikacyjnych. Pliki cookie są używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencji dotyczących wyglądu witryny lub zawartości koszyka w sklepach internetowych).

**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego **Narzędzia / Ustawienia zaawansowane** i skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

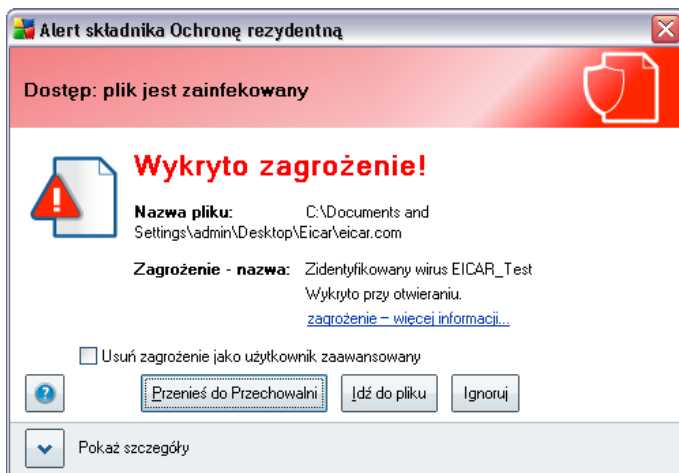
### Przyciski kontrolne

W interfejsie składnika **Ochrona rezydentna** dostępne są następujące przyciski kontrolne:

- **Zarządzaj wyjątkami** otwiera okno dialogowe [Ochrona rezydentna — Wykluczone foldery](#), w którym można zdefiniować foldery pomijane przy skanowaniu przez składnik [Ochrona rezydentna](#).
- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — kliknięcie tego przycisku powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

### 8.9.3. Zagrożenia wykryte przez Ochronę rezydentną

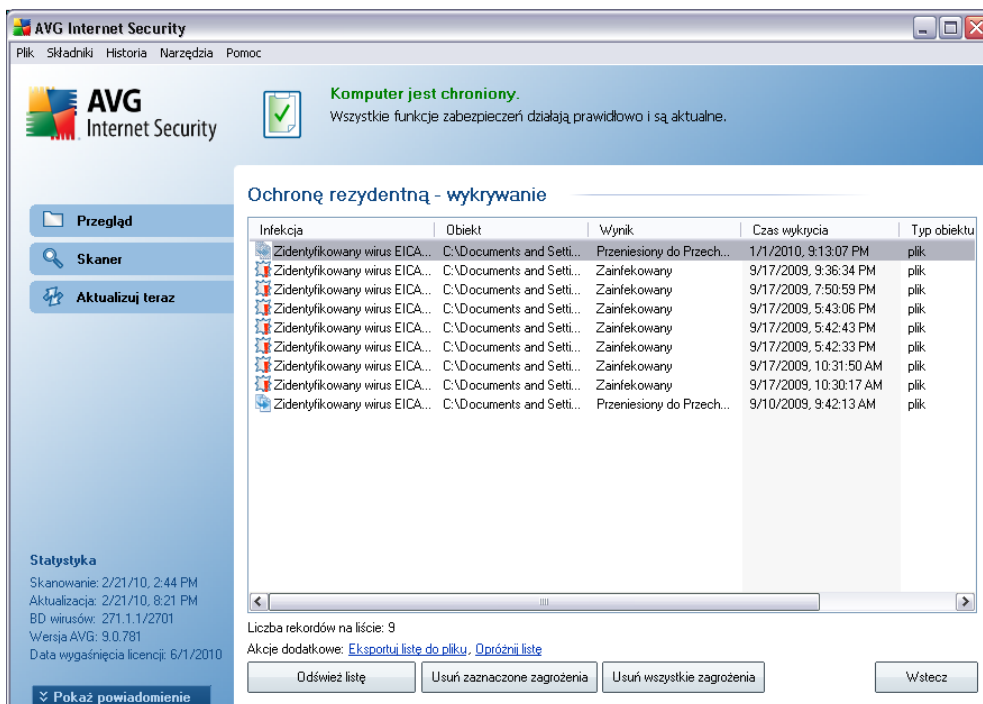
**Ochrona rezydentna** to składnik służący do skanowania plików w trakcie ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego ostrzeżenia:



Okno to zawiera informacje dotyczące wykrytej infekcji i pozwala wybrać czynność, która ma zostać wykonana:

- **Wylecz** — jeśli możliwe jest wyleczenie pliku, system AVG zrobi to automatycznie (opcja zalecana).
- **Przenies do Przechowalni** — wirus zostanie przeniesiony do [Przechowalni wirusów AVG](#)
- **Przejdź do pliku** — pozwala przejść do lokalizacji podejrzanego obiektu (w *nowym oknie Eksploratora Windows*)
- **Ignoruj** — tej opcji NIE należy używać bez uzasadnionego powodu!

Przegląd wszystkich zagrożeń wykrytych przez składnik **Ochrona rezydentna** można znaleźć w oknie dialogowym **Zagrożenia wykryte przez Ochronę rezydentną** dostępnym poprzez menu [Historia / Zagrożenia wykryte przez Ochronę rezydentną](#):



Okno **Zagrożenia wykryte przez Ochronę rezydentną** zawiera przegląd obiektów wykrytych i uznanych przez ten składnik **\*\*\*** za niebezpieczne (które następnie wyleczono lub przeniesiono do **Przechowalni wirusów**). Podawane są tam następujące informacje:

- **Infekcja** — opis (ewentualnie nazwa) wykrytego zagrożenia.
- **Obiekt** — lokalizacja obiektu.
- **Wynik** — działanie podjęte w związku z wykryciem.
- **Czas wykrycia** — data i godzina wykrycia obiektu.
- **Typ obiektu** — typ wykrytego obiektu.
- **Proces** — akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co umożliwiło jego wykrycie).

U dołu okna znajdują się informacje na temat łącznej liczby wykrytych infekcji. Ponadto, można wyeksportować całą listę obiektów do pliku, (**Eksportuj listę do pliku**) lub usunąć wszystkie jej pozycje (**Opróżnij listę**). Przycisk **Odśwież listę** pozwala zaktualizować listę obiektów wykrytych przez **Ochronę rezydentną**. Przycisk **Wstecz**

przelacza z powrotem do domyslnego okna [Interfejsu uzytkownika systemu AVG](#) (przegladu skladnikow).

## 8.10. Menedzer aktualizacji

### 8.10.1. Zasady dzialania Menedzera aktualizacji

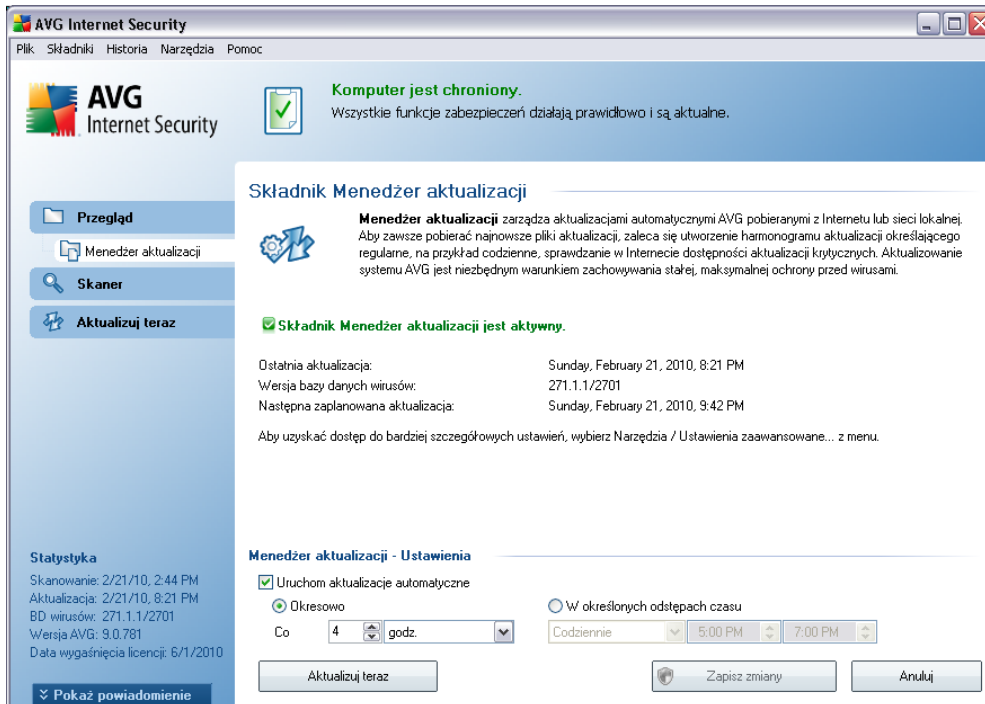
Zadne oprogramowanie zabezpieczajace nie moze zapewnic realnej ochrony przed ruznymi typami zagrozen bez regularnych aktualizacji! Tworcy wirusow nieustannie szukaja nowych luk w programach i systemach operacyjnych, ktore mogliby wykorzystac. Nowe wirusy, szkodliwe oprogramowanie i metody atakow pojawiaja sie kazdego dnia. Z tego powodu dostawcy oprogramowania na biezaco wydaja aktualizacje i poprawki zabezpieczen, ktore 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 wirusow nalezy pobierac codziennie. Mniej istotne aktualizacje programu mozna pobierac co tydzien.

***Uwaga:*** *Wiecej informacji na temat typow i poziomow aktualizacji zawiera rozdzial [Aktualizacje AVG](#).*

## 8.10.2. Interfejs Menedzera aktualizacji



Interfejs składnika **Menedżer aktualizacji** zawiera informacje o jego funkcjach i bieżącym stanie (Składnik *Menedżer aktualizacji jest aktywny.*), a także istotne statystyki:

- **Ostatnia aktualizacja** — data i godzina ostatniej aktualizacji bazy danych.
- **Wersja bazy danych wirusów** — numer ostatniej wersji bazy danych wirusów; numer ten jest zwiększany przy każdej aktualizacji bazy danych.
- **Następna zaplanowana aktualizacja** — godzina i data kolejnej zaplanowanej aktualizacji.

### Podstawowa konfiguracja składnika

W dolnej części okna dialogowego znajduje się sekcja **ustawień Menedzera aktualizacji**, w której można wprowadzać zmiany regul uruchamiania procesu aktualizacji. Można określić tam, czy pliki aktualizacyjne mają być pobierane automatycznie (**Uruchom aktualizacje automatyczne**), czy tylko na zadanie. Opcja **Uruchom aktualizacje automatyczne** jest włączona i zaleca się pozostawienie jej w

tym stanie. Regularne pobieranie najnowszych aktualizacji ma kluczowe znaczenie dla prawidłowego funkcjonowania każdego oprogramowania zabezpieczającego!

Ponadto, można określić, kiedy aktualizacje mają być uruchamiane:

- o **Okresowo** — należy zdefiniować interwał aktualizacji.
- o **O określonej godzinie** — należy zdefiniować dokładną datę i godzinę.

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

**Uwaga:** Dostawca oprogramowania AVG skonfigurował wstępnie wszystkie składniki pod kątem optymalnej wydajności. Konfiguracje systemu AVG należy zmieniać tylko w uzasadnionych przypadkach. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Jeśli konieczna jest zmiana konfiguracji systemu AVG, należy wybrać z menu głównego **Narzędzia / Ustawienia zaawansowane** i skorzystać z interfejsu [Zaawansowane ustawienia AVG](#).

### Przyciski kontrolne

W interfejsie składnika **Menedżer aktualizacji** dostępne są następujące przyciski kontrolne:

- **Aktualizuj teraz** — kliknięcie przycisku uruchamia [natychmiastową aktualizację](#) na zadanie.
- **Zapisz zmiany** — kliknięcie tego przycisku pozwala zapisać i zastosować zmiany wprowadzone w bieżącym oknie.
- **Anuluj** — kliknięcie tego przycisku powoduje powrót do domyślnego okna [Interfejsu użytkownika AVG](#) (przeglądu składników).

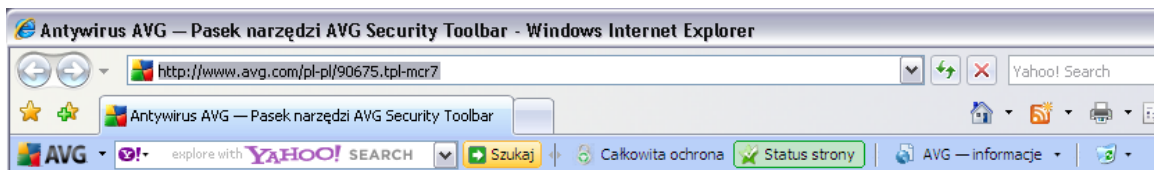
## 9. Pasek narzędzi AVG Security Toolbar

**Pasek narzędzi AVG Security Toolbar** to nowy plugin współpracujący ze składnikiem **AVG Link Scanner**. Zadaniem paska jest sprawdzanie wyników zwracanych przez obsługiwane wyszukiwarki internetowe (*Yahoo!*, *Google*, *Bing*, *Altavista*, *Baidu*). **Pasek narzędzi AVG Security Toolbar** pozwala na kontrolowanie funkcji składnika **AVG Link Scanner** i dostosowywanie jego zachowania.

Jesli w czasie instalacji systemu **AVG 9 Anti-Virus plus Firewall** zostanie wybrana instalacja paska narzędzi, automatycznie nastąpi jego dodanie do przeglądarki internetowej. Uwaga: W przypadku korzystania z alternatywnej przeglądarki internetowej (*np. Avant Browser*) mogą wystąpić nieoczekiwane zachowania.

### 9.1. Interfejs paska narzędzi AVG Security Toolbar

Pasek narzędzi **AVG Security Toolbar** jest zgodny z przeglądarkami **MS Internet Explorer** (wersja 6.0 lub nowsza) i **Mozilla Firefox** (wersja 2.0 lub nowsza). Po podjęciu decyzji o zainstalowaniu paska narzędzi **AVG Security Toolbar** (w czasie procesu instalacji systemu AVG pojawiło się pytanie o zainstalowanie tego składnika), pasek umieszczony jest pod paskiem adresu w oknie przeglądarki:



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

**AVG Security Toolbar** składa się z następujących elementów:

- **Logo AVG** — pozwala uzyskać dostęp do głównych elementów paska. Kliknięcie go spowoduje przejście do witryny systemu AVG (<http://www.avg.com/>). Kliknięcie strzałki obok ikony AVG powoduje otwarcie menu z następującymi opcjami:
  - **Informacje o pasku narzędzi** — link do strony głównej **AVG Security Toolbar**, zawierającej szczegółowe informacje o działaniu paska.
  - **Uruchom AVG 9 Anti-Virus plus Firewall** — powoduje otwarcie interfejsu użytkownika systemu **AVG 9 Anti-Virus plus Firewall**
  - **Opcje** — powoduje otwarcie okna dialogowego, w którym można modyfikować ustawienia paska narzędzi **AVG Security Toolbar** — patrz

rozdział [Opcje paska narzędzi AVG Security Toolbar](#)

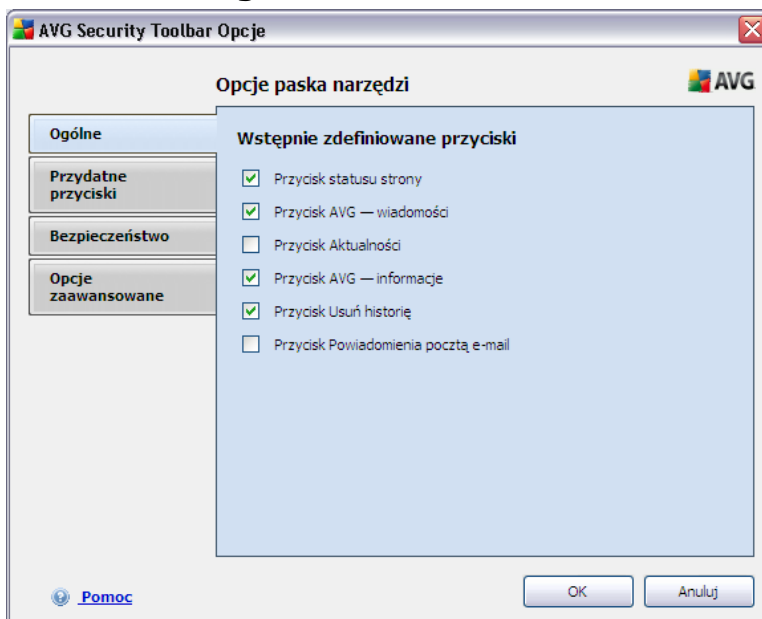
- **Usun historie** — daje dostęp do poleceń: *Usun cała historie, Usun historie wyszukiwania, Usun historie przeglądania, Usun historie pobierania* i *Usun pliki cookie* w Pasku narzędzi AVG Security Toolbar.
- **Aktualizacja** — pozwala sprawdzić dostępność nowych aktualizacji **dotyczących Paska narzędzi AVG**
- **Pomoc** — pomaga znaleźć odpowiednie pliki pomocy, wysłać opinie na temat produktu lub wyświetlić szczegóły dotyczące bieżącej wersji paska narzędzi
- **Pole wyszukiwania** — w polu wyszukiwania należy wprowadzić słowo lub frazę. Następnie należy kliknąć przycisk **Wyszukaj**, aby rozpocząć wyszukiwanie przy użyciu określonej wyszukiwarki (*wyszukiwarke, która ma być używana, można określić w [zaawansowanych opcjach paska narzędzi AVG Security Toolbar](#); dostępne opcje to: Yahoo!, Wikipedia, Baidu, WebHledani i Yandex*) niezależnie od wyświetlanej w danej chwili strony. Wspomniane pole zawiera także historie poprzednich wyszukiwań. Wszystkie wyniki wyszukiwania są sprawdzane za pomocą funkcji [AVG Search-Shield](#).
- **Całkowita ochrona** — ten przycisk wyświetlany jest jako **Całkowita ochrona / Ograniczona ochrona / Brak ochrony** w zależności od wybranej **AVG 9 Anti-Virus plus Firewall** konfiguracji.
- **Stan strony** — ten przycisk wyświetla ocenę ładowanej w danej chwili strony internetowej bezpośrednio na pasku narzędzi. Podstawą oceny są kryteria składnika [AVG Search-Shield](#) (*możliwe oceny strony to: bezpieczna / podejrzana / niebezpieczna / zawiera zagrożenia / nie mogła zostać przeskanowana*). Kliknij przycisk, aby otworzyć panel zawierający szczegółowe informacje dotyczące określonej strony internetowej.
- **Informacje o programie AVG** — zawiera łącza do ważnych informacji dotyczących bezpieczeństwa, znajdujących się w witrynie AVG (<http://www.avg.com/>).
  - **Informacje o pasku narzędzi** — link do strony głównej **AVG Security Toolbar, zawierającej szczegółowe informacje o działaniu paska**.
  - **Zagrożenia — informacje** — otwiera stronę internetową firmy AVG zawierającą informacje na temat najnowszych wirusów i zagrożeń internetowych.

- **Nowosci AVG** — otwiera strone internetowa zawierajaca najnowsze informacje prasowe dotyczace systemu AVG.
- **Obecny poziom zagrozenia** — otwiera strone internetowa laboratorium wirusow, ktora zawiera graficzna reprezentacje obecnego poziomu zagrozen w sieci.
- **Encyklopedia wirusow** — otwiera strone encyklopedii wirusow, w ktorej mozna wyszukac okreslone wirusy na podstawie ich nazw i uzyskac szczegolowe informacje na ich temat.

## 9.2. Opcje Paska narzedzi AVG Security Toolbar

Opcje konfiguracji wszystkich parametrów **Paska narzedzi AVG Security Toolbar** dostepne sa bezposrednio z poziomu panelu **AVG Security Toolbar**. Interfejs edycji dostepny jest po wybraniu opcji **AVG / Opcje** z menu paska. Jego otwarcie nastepuje w nowym oknie dialogowym (**Opcje paska narzedzi**), ktore jest podzielone na cztery sekcje:

### 9.2.1. Karta Ogólne

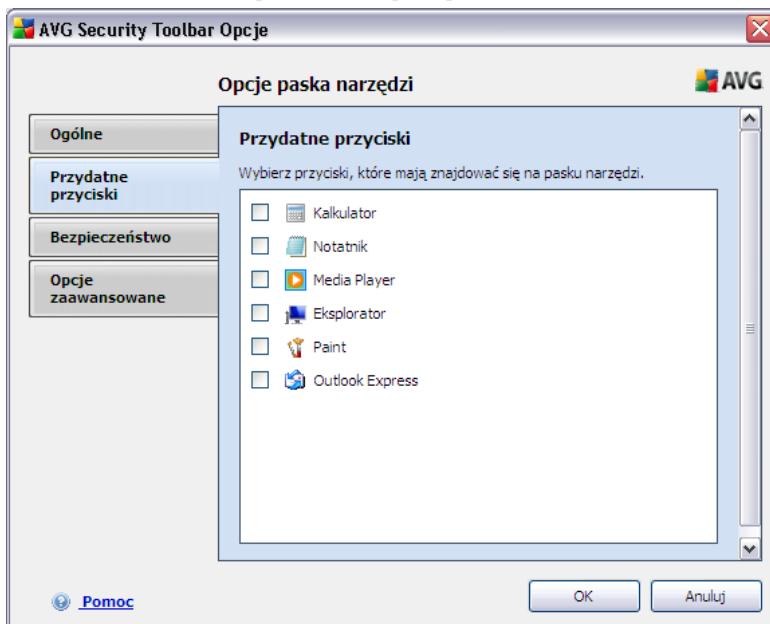


Na tej karcie mozliwe jest okreslenie, ktore przyciski kontrolne paska narzedzi maja byc wyswietlane / ukryte na panelu **Paska narzedzi AVG Security Toolbar**. Należy zaznaczyć opcje wszystkich przycisków, które maja byc wyswietlane. Poniżej znajduje

się opis funkcji wszystkich przycisków paska narzędzi:

- **Nowosci AVG** — przycisk otwiera stronę internetową zawierającą najnowsze informacje prasowe dotyczące systemu AVG.
- **Wiadomosci** — przycisk udostępnia ustrukturalizowany przegląd bieżących wiadomości z codziennej prasy.
- **System AVG — informacje** — przycisk powoduje wyświetlanie na pasku narzędzi AVG informacji dotyczących bieżących zagrożeń i poziomu zagrożenia internetowego, umożliwia otwarcie encyklopedii wirusów i udostępnia dodatkowe wiadomości dotyczące produktów AVG.
- **Przycisk Usun historie** — przycisk ten pozwala usunąć całą historię, lub usunąć historię wyszukiwania, przeglądania i pobierania lub tylko usunąć ciasteczka bezpośrednio z panelu Paska narzędzi AVG Security Toolbar.

### 9.2.2. Karta Uzyteczne przyciski








Karta **Uzyteczne przyciski** umożliwia wybór aplikacji z listy i wyświetlanie ich ikon w interfejsie paska narzędzi. Ikona służy wówczas jako szybkie łącze umożliwiające natychmiastowe uruchomienie odpowiedniej aplikacji.

### 9.2.3. Karta Bezpieczeństwo



Karta **Bezpieczeństwo** jest podzielona na dwie sekcje (**Bezpieczeństwo przeglądarki** i **Oceny**), w których można zaznaczyć określone pola, aby skonfigurować następujące funkcje:

- **Bezpieczeństwo przeglądarki** — te pozycje należy zaznaczyć, aby aktywować lub wyłączyć **funkcje AVG Search-Shield** i/lub **funkcje AVG Surf-Shield**
- **Oceny** — należy wybrać symbole graficzne, które mają być używane przy klasyfikacji wyników wyszukiwania przez funkcję **AVG Search-Shield**:
  -  strona jest bezpieczna
  -  strona jest podejrzana
  -  strona zawiera linki do niebezpiecznych stron
  -  strona zawiera aktywne zagrożenia
  -  strona nie jest dostępna i nie można jej przeskanować

Należy zaznaczyć odpowiednią opcję, aby potwierdzić, że informacje o określonym poziomie zagrożenia mają być wyświetlane. Nie można jednak wyłączyć wyświetlania czerwonego symbolu przypisanego stronom zawierającym realne zagrożenie. **Jesli nie istnieje ważny powód, żeby modyfikować domyślną konfigurację zdefiniowaną przez twórców programu, stanowczo zaleca się jej zachowanie.**

#### 9.2.4. Karta Opcje zaawansowane



Na karcie **Opcje zaawansowane** należy najpierw określić, która wyszukiwarka ma być używana jako domyślna. Dostępne opcje to: *Yahoo!*, *Baidu*, *WebHledani* i *Yandex*. Po zmianieniu domyślnej wyszukiwarki należy ponownie uruchomić przeglądarkę internetową, aby zmiany zostały zachowane.

Następnie można aktywować lub wyłączyć szczegółowe ustawienia paska narzędzi **AVG Security Toolbar**:

- **Ustaw i zachowaj Yahoo! jako wyszukiwarkę na pasku adresu** — (domyślnie włączone) — jeśli ta opcja jest zaznaczona, możliwe jest wprowadzanie słowa kluczowego wyszukiwania bezpośrednio w pasku adresu przeglądarki internetowej, dzięki czemu wyszukiwarka Yahoo! zostanie automatycznie użyta do wyszukania odpowiednich stron internetowych.
- **Zezwalaj systemowi AVG na sugestie dotyczące błędów nawigacji**

**przeglądarki (404/DNS)** (opcja domyślnie włączona) — jeśli podczas przeglądania sieci zostanie wybrana strona nieistniejąca lub niedostępna (błąd 404), automatycznie zostanie zaproponowany przegląd alternatywnych stron o podobnej tematyce.

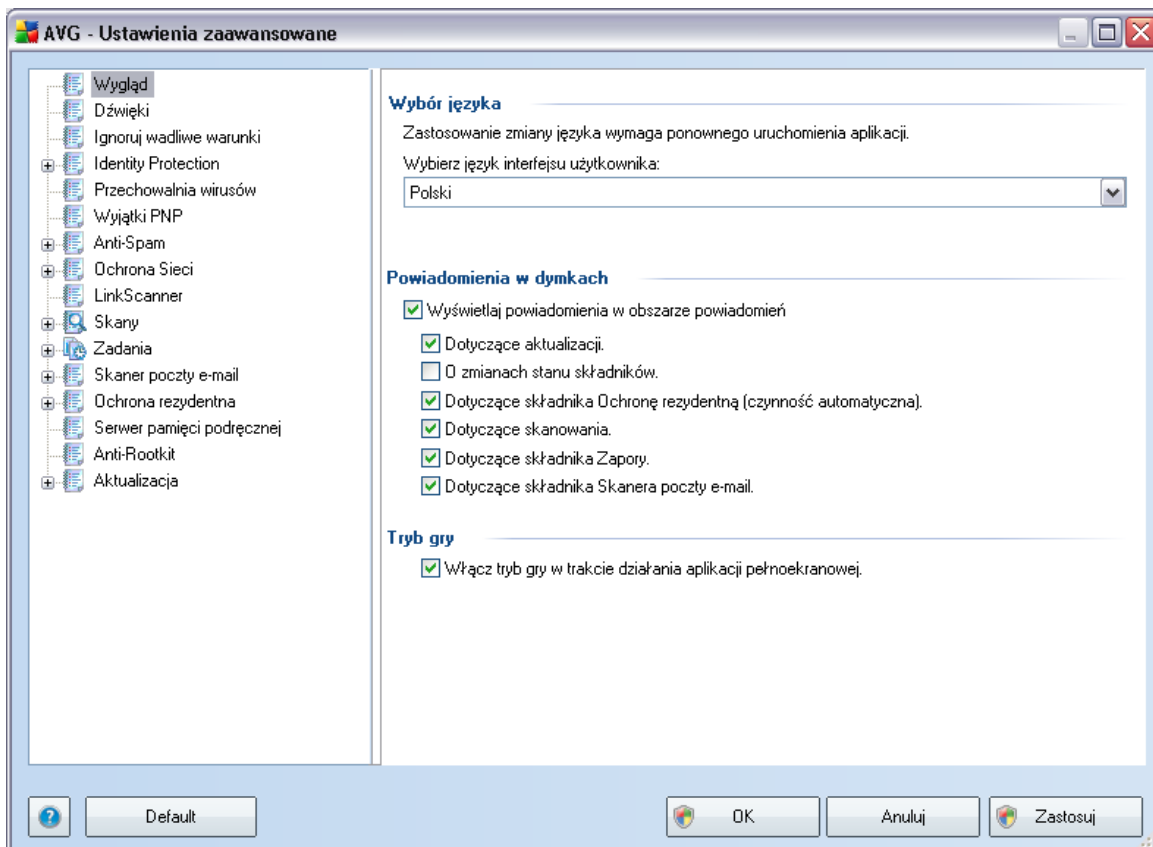
- **Ustaw i zachowaj Yahoo! jako domyślną wyszukiwarkę** — (domyślnie wylaczone) — Yahoo! jest domyślną wyszukiwarką internetową Paska narzędzi AVG Security Toolbar, a aktywowanie tej opcji powoduje, że staje się również domyślną wyszukiwarką przeglądarki internetowej.
- **Ponownie wyświetlaj Pasek narzędzi AVG Security Toolbar, jeśli został ukryty (po tygodniu)** — (domyślnie włączone) — ta opcja jest domyślnie aktywna i w przypadku przypadkowego ukrycia **Paska narzędzi AVG Security Toolbar** zostanie on ponownie wyświetlony po upływie tygodnia.

## 10. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG 9 Anti-Virus plus Firewall** zostają otwarte w nowym oknie o nazwie **Zaawansowane ustawienia systemu AVG**. Okno to podzielone jest na dwa obszary: lewy zawiera drzewo nawigacyjne, a prawy – opcje konfiguracji programu. Wybranie składnika, którego (*lub części którego*) konfiguracja ma zostać zmieniona, powoduje przejście do odpowiedniego okna z prawej strony.

### 10.1. Wygląd

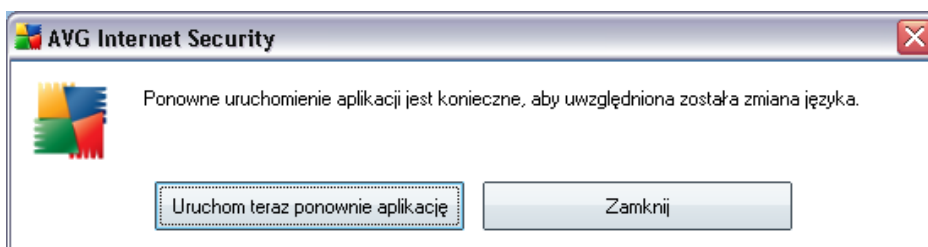
Pierwszy element w drzewie nawigacyjnym, **Wygląd**, odnosi się do ogólnych ustawień [interfejsu użytkownika AVG](#) oraz kilku podstawowych opcji sterujących zachowaniem aplikacji:



### Wybór języka

W sekcji **Wybór języka** można wybrać zadany język z listy rozwijanej; język ten będzie używany w całym [interfejsie użytkownika AVG](#). Menu rozwijane zawiera tylko języki wybrane podczas [instalacji](#) (zobacz rozdział [Instalacja niestandardowa — Wybieranie składników](#)). Przelaczenie aplikacji na inny język wymaga ponownego uruchomienia interfejsu użytkownika. W tym celu należy wykonać następujące kroki:

- Wybierz zadany język aplikacji i potwierdź wybór, klikając przycisk **Zastosuj** (widoczny w prawym dolnym rogu).
- Wcisnij przycisk **OK**, aby potwierdzić.
- W nowym oknie dialogowym pojawi się informacja, że zmiana języka interfejsu systemu AVG wymaga ponownego uruchomienia programu:



## Powiadomienia w dymkach

W tym obszarze można wyłączyć wyświetlane w dymkach powiadomienia dotyczące stanu aplikacji. Domyślnie wszystkie powiadomienia są wyświetlane i nie zaleca się zmiany tych ustawień. Zwykle informują one o zmianach stanu składników AVG i w żadnym wypadku nie wolno ich ignorować!

Jeśli jednak z jakiegos powodu powiadomienia te nie mają być wcale wyświetlane lub mają dotyczyć tylko określonych składników AVG, można zdefiniować własne preferencje, zaznaczając lub usuwając zaznaczenie odpowiednich opcji:

- **Wyświetlaj powiadomienia w obszarze powiadomien** — pole jest domyślnie zaznaczone (*opcja włączona*), a powiadomienia są wyświetlane. Usunięcie zaznaczenia opcji powoduje całkowite wyłączenie wyświetlania powiadomien w dymkach. Po włączeniu tej opcji można bardziej szczegółowo określić, jakie powiadomienia mają być wyświetlane:
  - **Wyświetlaj w obszarze powiadomien komunikaty dotyczące aktualizacji** — należy określić, czy mają być wyświetlane informacje dotyczące rozpoczęcia, postępu i zakończenia aktualizacji systemu AVG;

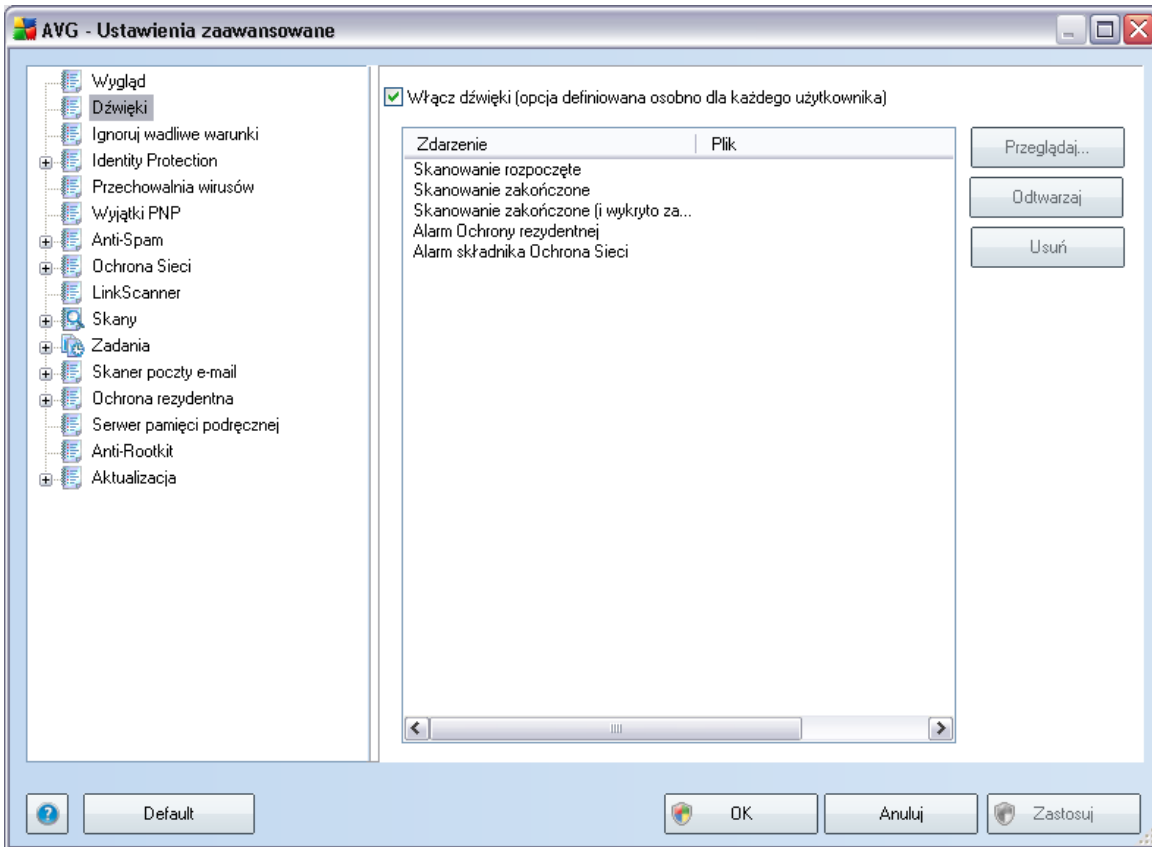
- **Wyswietlaj powiadomienia o zmianach stanu skladników** — należy określić, czy mają być wyświetlane informacje dotyczące aktywności lub nieaktywności składników bądź możliwych problemów ich dotyczących. W przypadku zgłaszania stanu błędu składnika, opcja ta określa funkcję informacyjną [ikony na pasku zadań](#) (zmiany koloru), która wskazuje na problemy z dowolnym składnikiem systemu AVG;
- **Wyswietlaj w obszarze powiadomien komunikaty dotyczące [Ochrony rezydentnej](#)** — należy określić, czy informacje dotyczące zapisywania, kopiowania i otwierania procesów mają być wyświetlane czy ukrywane (*ta konfiguracja jest dostępna tylko, jeśli opcja [automatycznego leczenia](#) Ochrony rezydentnej jest włączona*);
- **Wyswietlaj w obszarze powiadomien komunikaty dotyczące [skanowania](#)** — należy określić, czy mają być wyświetlane informacje dotyczące automatycznego rozpoczęcia, postępu i zakończenia zaplanowanego skanowania;
- **Wyswietlaj w obszarze powiadomien komunikaty dotyczące [Zapory](#)** — należy określić, czy mają być wyświetlane informacje dotyczące stanu i procesów Zapory, np. ostrzeżenia o włączeniu/wyłączeniu składnika, możliwym blokowaniu ruchu sieciowego itp.;
- **Wyswietlaj w obszarze powiadomien komunikaty dotyczące [składnika Skaner poczty e-mail](#)** — należy określić, czy mają być wyświetlane informacje dotyczące skanowania wszystkich przychodzących i wychodzących wiadomości e-mail.

## Tryb gry

Ta funkcja jest przeznaczona dla aplikacji pełnoekranowych, w działaniu których mogłyby przeszkadzać (np. minimalizować lub zakłócać wyświetlanie grafiki) powiadomienia systemu AVG (wyświetlane np. w chwili uruchomienia zaplanowanego skanowania). Aby tego uniknąć, należy pozostawić pole wyboru **Włącz tryb gry w trakcie działania aplikacji pełnoekranowej** zaznaczone (ustawienie domyślne).

## 10.2. Dźwięki

W oknie dialogowym **Dźwięki** można określić, czy system AVG ma informować o określonych czynnościach za pomocą dźwięków. Jeśli tak, należy zaznaczyć pole wyboru **Włącz efekty dźwiękowe** (domyślnie wyłączone), aby włączyć listę czynności systemu AVG:

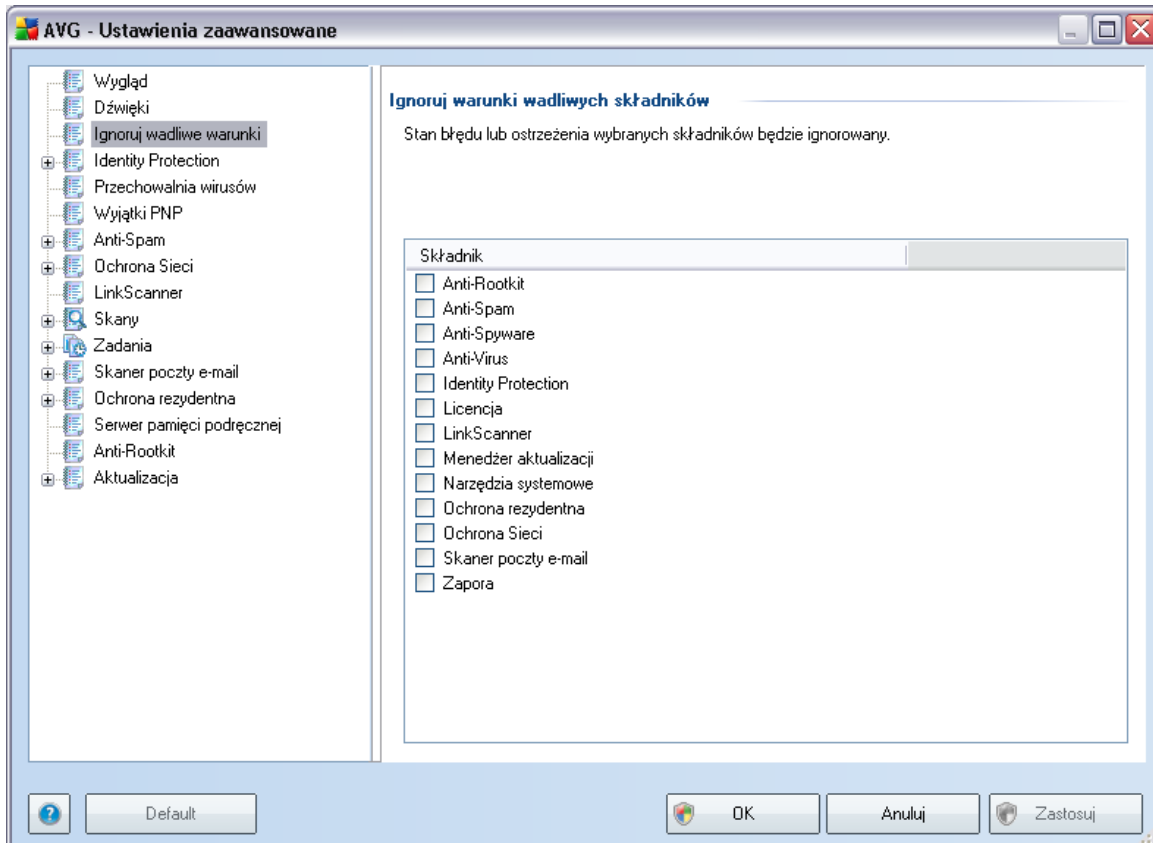


Następnie należy wybrać odpowiednie zdarzenie z listy i wskazać plik dźwiękowy, który ma zostać do niego przypisany (**Przełączaj**). Aby odtworzyć wybrany dźwięk, należy zaznaczyć go na liście i nacisnąć przycisk **Odtwarzaj**. Aby usunąć dźwięk przypisany do określonego zdarzenia, należy użyć przycisku **Usuń**.

**Uwaga:** Obsługiwane są tylko pliki \*.wav!

### 10.3. Ignoruj bledny stan skladników

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



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

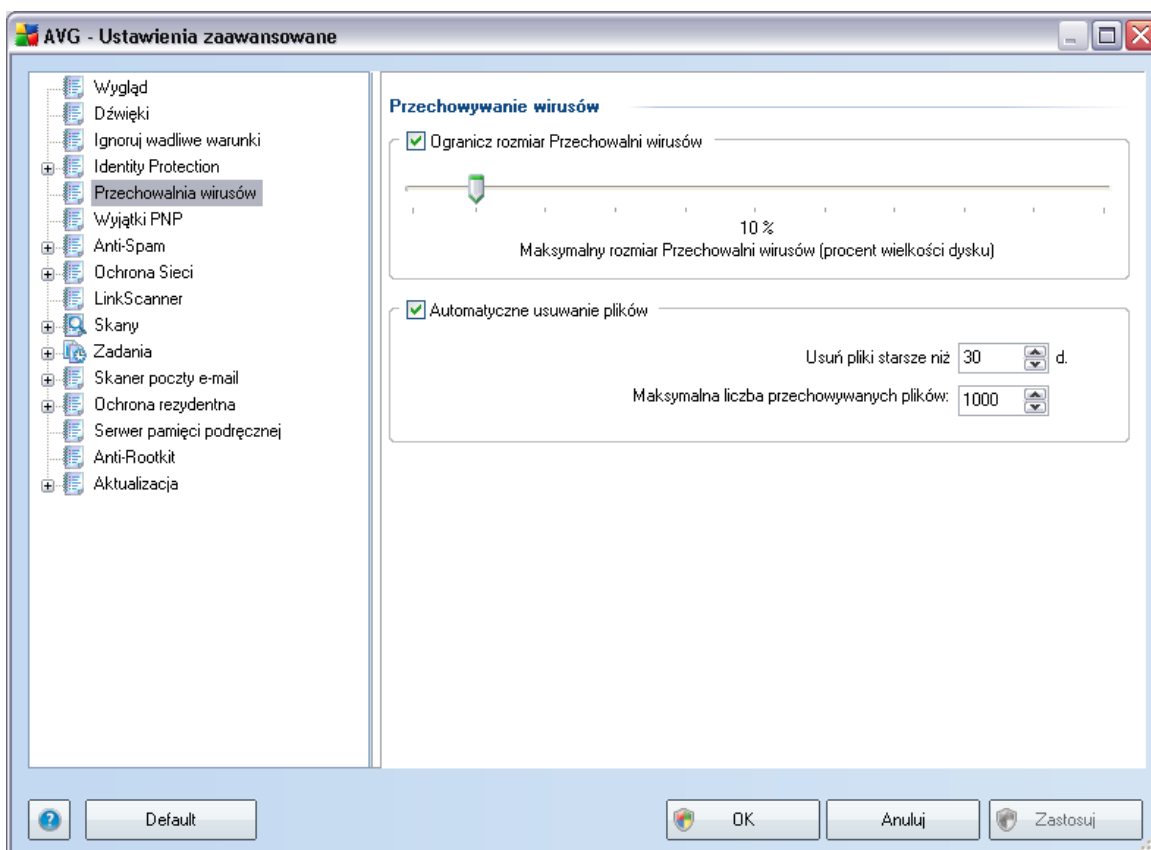
- **ikona na pasku zadan** — gdy wszystkie skladniki systemu AVG dzialaja prawidlowo, wyswietlana ikona jest czterokolorowa; w przypadku bledu wyswietlany jest zolty wykrzyknik,
- tekstowy opis problemu jest widoczny w sekcji **Informacje o stanie bezpieczenstwa** okna glownego AVG

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 wyliczenie skladnika bylo celowe, a ryzyko z tym zwiazane jest znane. Ponadto, gdy ikona jest szara, nie moze juz informowac o ewentualnych realnych bledach.

W takim przypadku nalezy w powyzzszym 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 bezpośrednio w sekcji [przeglądu składników okna głównego AVG](#).

## 10.4. Przechowalnia wirusów



W oknie **Przechowalnia wirusów** mozna zdefiniowac kilka parametrów dotyczących administrowania obiektami znajdującymi się w **Przechowalni**:

- **Ogranicz rozmiar Przechowalni wirusów** — za pomoca suwaka nalezy



okreslic maksymalny rozmiar **Przechowalni wirusów**. Rozmiar jest okreslany w stosunku do rozmiaru dysku lokalnego.

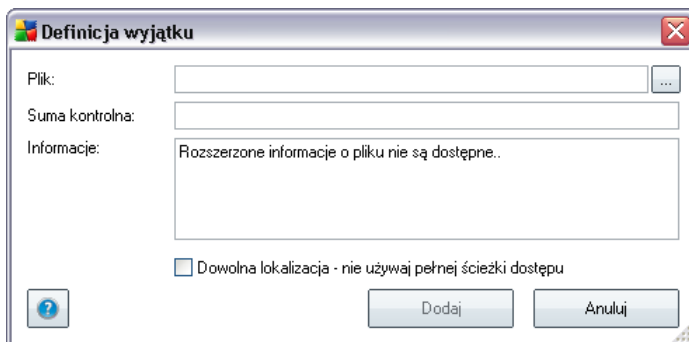
- **Automatyczne usuwanie plików** — w tym obszarze mozna zdefiniowac maksymalny okres przetrzymywania obiektów w **Przechowalni wirusów** (**Usun pliki starsze niz ... dni**) oraz maksymalna liczbe plików, które moga znajdowac sie w **Przechowalni** (**Maksymalna liczba przechowywanych plików**).

## 10.5. Wyjatki PNP

System **AVG 9 Anti-Virus plus Firewall** potrafi analizowac i wykrywac pliki wykonywalne i biblioteki DLL, których obecność w systemie operacyjnym może być niepożądana. W niektórych przypadkach użytkownik może chcieć zachować na komputerze określone potencjalnie niechciane programy (*jeśli zostały zainstalowane celowo*). Niektóre aplikacje, zwłaszcza bezpłatne, zawierają oprogramowanie reklamowe. Może ono zostać wykryte i zgłoszone przez system AVG jako **potencjalnie niechciany program**. Jeśli chcesz zachować taki program na komputerze, możesz zdefiniować go jako wyjątek potencjalnie niechcianych programów:

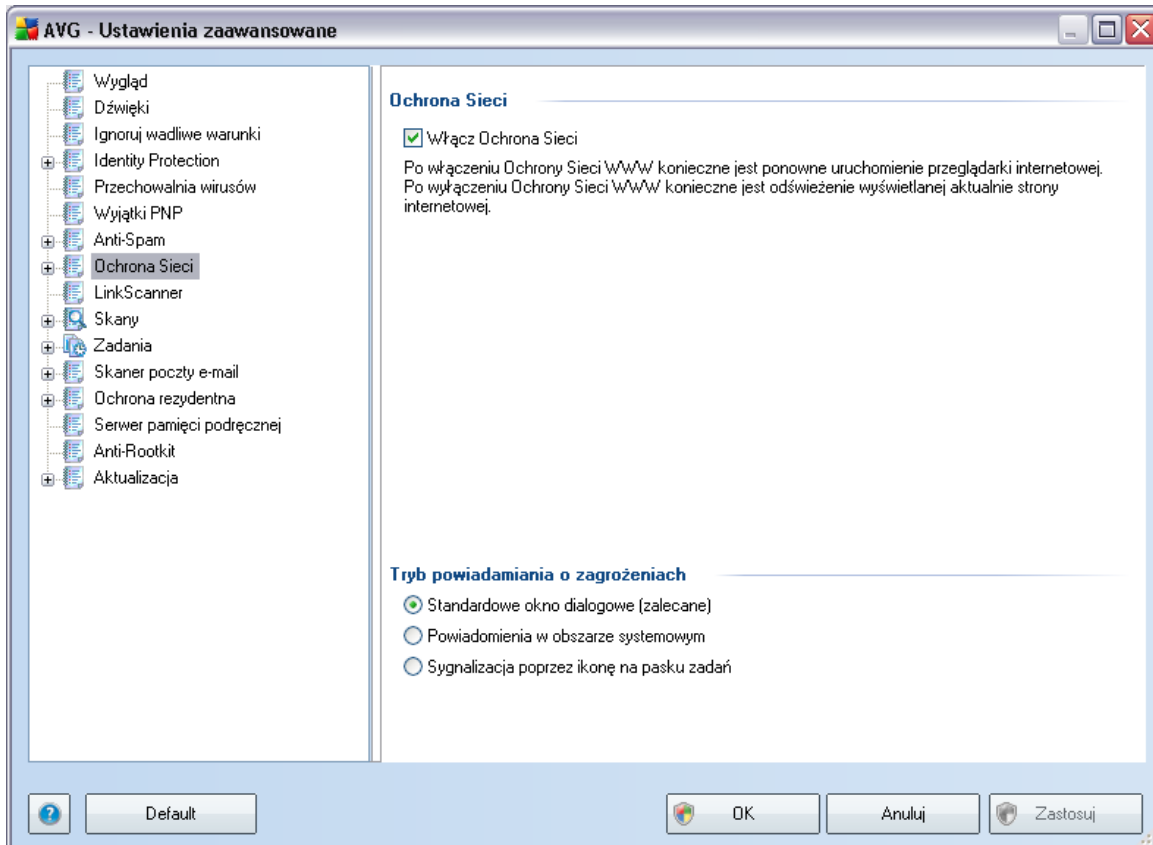


- **Edytuj** — otwiera okno edycji (*identyczne jak okno definiowania nowego wyjątku, patrz nizej*), w którym można zmienić parametry istniejącego wyjątku.
- **Usun** — usuwa wybrany element z listy wyjątków.
- **Dodaj wyjątek** — otwiera okno edycji, w którym można zdefiniować parametry nowego wyjątku:



- **Plik** — należy podać pełną ścieżkę do pliku, który ma być oznaczony jako wyjątek.
- **Suma kontrolna** — wyświetla unikatową „sygnaturę” wybranego pliku. Suma ta jest generowana automatycznie ciągiem znaków, który pozwala programowi AVG jednoznacznie odróżnić wybrany plik od innych. Jest ona generowana i wyświetlana po pomysłnym dodaniu pliku.
- **Informacje o pliku** — wyświetla wszelkie dodatkowe dostępne informacje na temat pliku (*licencja/wersja itp.*).
- **Dowolna lokalizacja — nie używaj pełnej ścieżki dostępu** — jeśli plik ma być zdefiniowany jako wyjątek jedynie dla konkretnej lokalizacji, wówczas należy pozostawić to pole niezaznaczone.

## 10.6. Ochrona Sieci



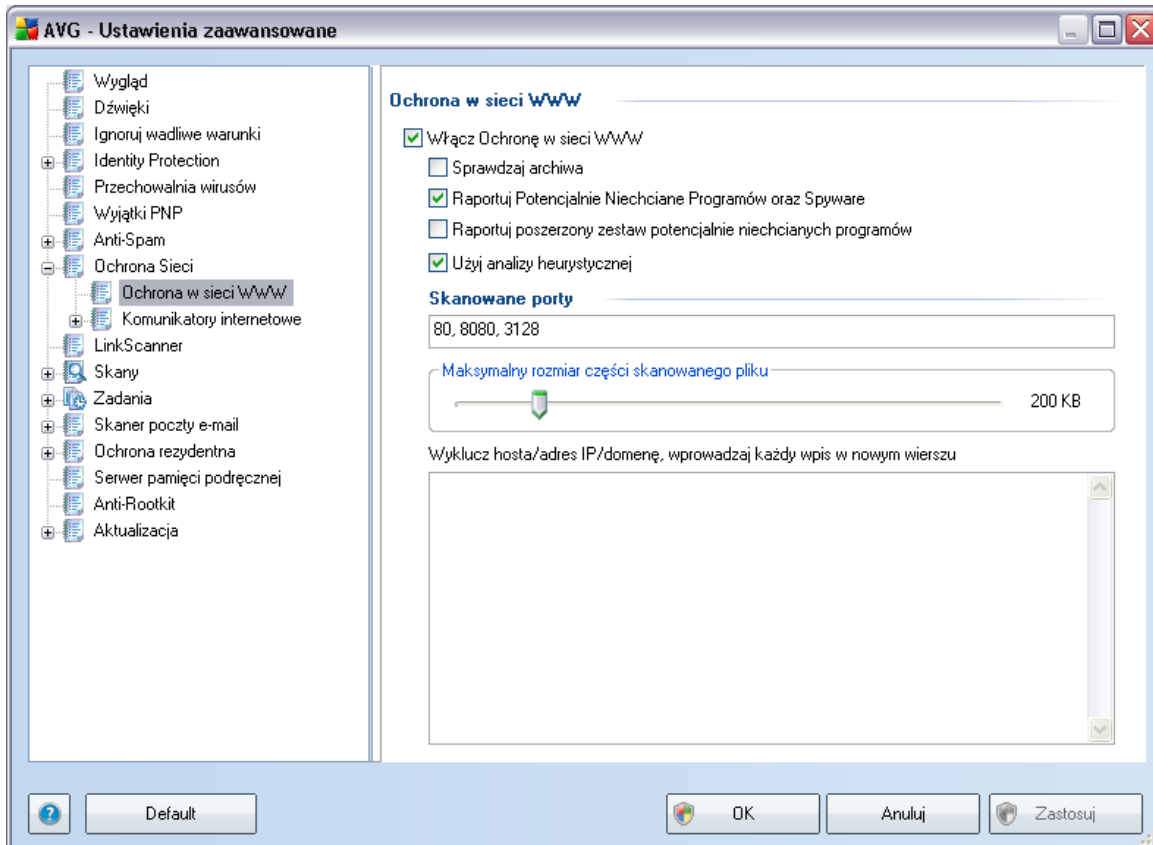
W oknie dialogowym **Ochrona sieci WWW** można włączyć lub wyłączyć cały składnik **Ochrona Sieci** za pomocą opcji **Włącz Ochronę Sieci** (domyślnie opcja jest włączona). Szczegółowe ustawienia tego składnika dostępne są w kolejnych oknach dialogowych dostępnych z poziomu drzewa nawigacyjnego:

- [Ochrona WWW](#)
- [Komunikatory internetowe](#)

### Tryb powiadamiania o zagrożeniach

W dolnej części okna można wybrać sposób informowania o wykrytych zagrożeniach: za pomocą zwykłych okien dialogowych, powiadomien w dymkach lub ikony na pasku zadań.

### 10.6.1. Ochrona WWW



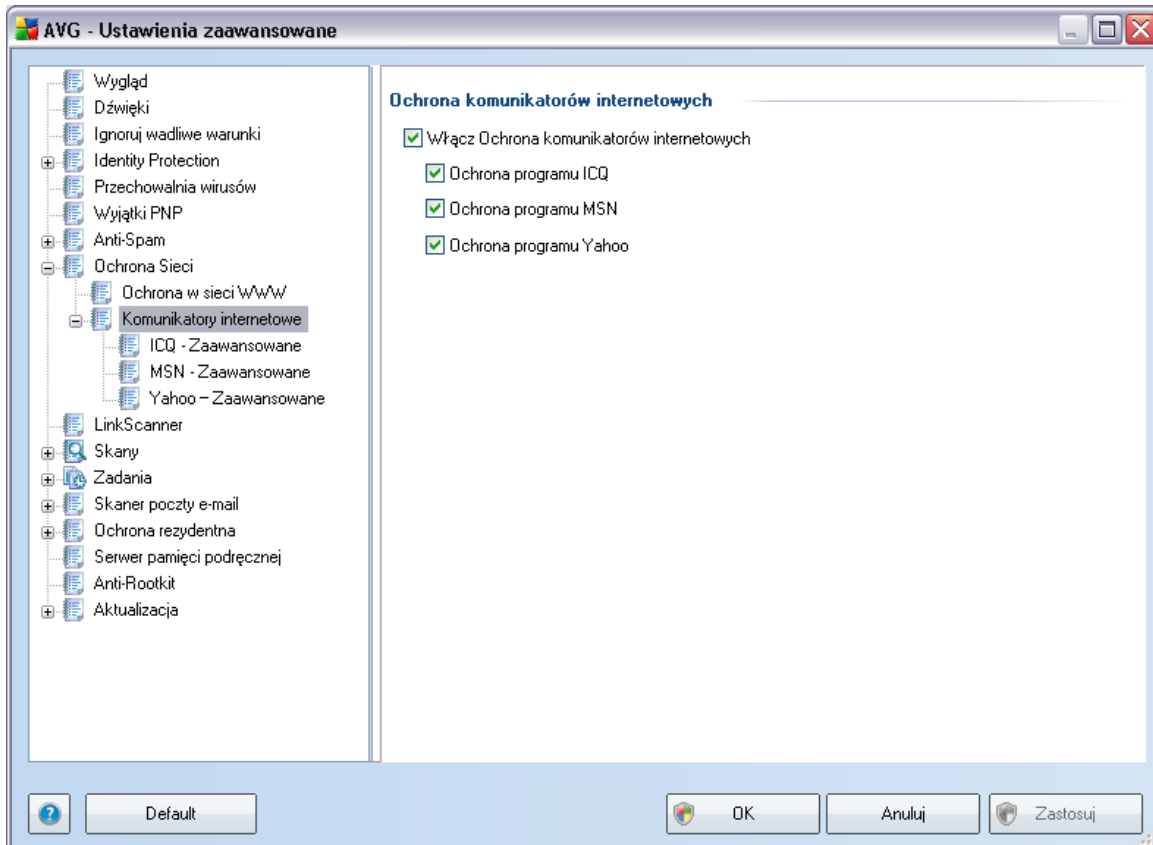
W oknie dialogowym **Ochrona w sieci WWW** można edytować konfigurację dotyczącą skanowania zawartości witryn internetowych. Interfejs pozwala modyfikować następujące ustawienia:

- **Włącz Ochronę sieci WWW** — potwierdza, że składnik **Ochrona Sieci** ma skanować zawartość stron WWW. Jeśli ta opcja jest aktywna (*domyślnie*), można włączyć lub wyłączyć następujące funkcje:
  - **Skanuj wewnątrz archiwów** — skanowanie ma obejmować także archiwa zawarte na wyświetlanych stronach WWW.
  - **Raportuj zagrożenia potencjalnie niechcianymi programami i oprogramowaniem szpiegującym** (*opcja domyślnie włączona*) — zaznaczenie tego pola powoduje włączenie silnika **Anti-Spyware** i przeprowadzenie skanowania w poszukiwaniu oprogramowania

szpiegującego (a nie tylko wirusów). [Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie.](#) Nie zaleca się wyłączenia tej opcji — znacząco zwiększa ona poziom ochrony komputera.

- **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości [oprogramowania szpiegującego](#), czyli programów, które są zupełnie bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.
- **Użyj heurystyki** — skanowanie zawartości wyświetlanych stron ma wykorzystywać [analizę heurystyczną](#) (*dynamiczna emulacja instrukcji skanowanego obiektu w wirtualnym środowisku*).
- **Skanowane porty** — to pole zawiera listę standardowych numerów portów http. Jeśli konfiguracja komputera różni się od standardowej, można zmienić numery portów zgodnie z potrzebami.
- **Maksymalny rozmiar części skanowanego pliku** — jeśli wyświetlana strona zawiera pliki, można skanować ich zawartość jeszcze przed pobraniem na dysk twardy. Ponieważ jednak skanowanie obszernych plików zajmuje dłuższy czas, otwieranie stron WWW może zostać znacznie spowolnione. Za pomocą tego suwaka można określić maksymalny rozmiar plików, które mają być skanowane przez składnik [Ochrona Sieci](#). Nawet jeśli pobierany plik jest większy od wybranego limitu i nie zostanie przeskanowany przez Ochronę Sieci, nie zmniejsza to Twojego bezpieczeństwa: jeśli plik jest zainfekowany, składnik [Ochrona rezydentna](#) natychmiast to wykryje.
- **Wyklucz hosta/adres IP/domenę** — w polu można wpisać dokładną nazwę serwera (*host, adres IP, adres IP z maską lub adres URL*) lub domenę, które nie mają być skanowane przez składnik [Ochrona Sieci](#). Wykluczac należy tylko hosty, co do których istnieje absolutna pewność, że nie stanowią zagrożenia.

## 10.6.2. Komunikatory internetowe

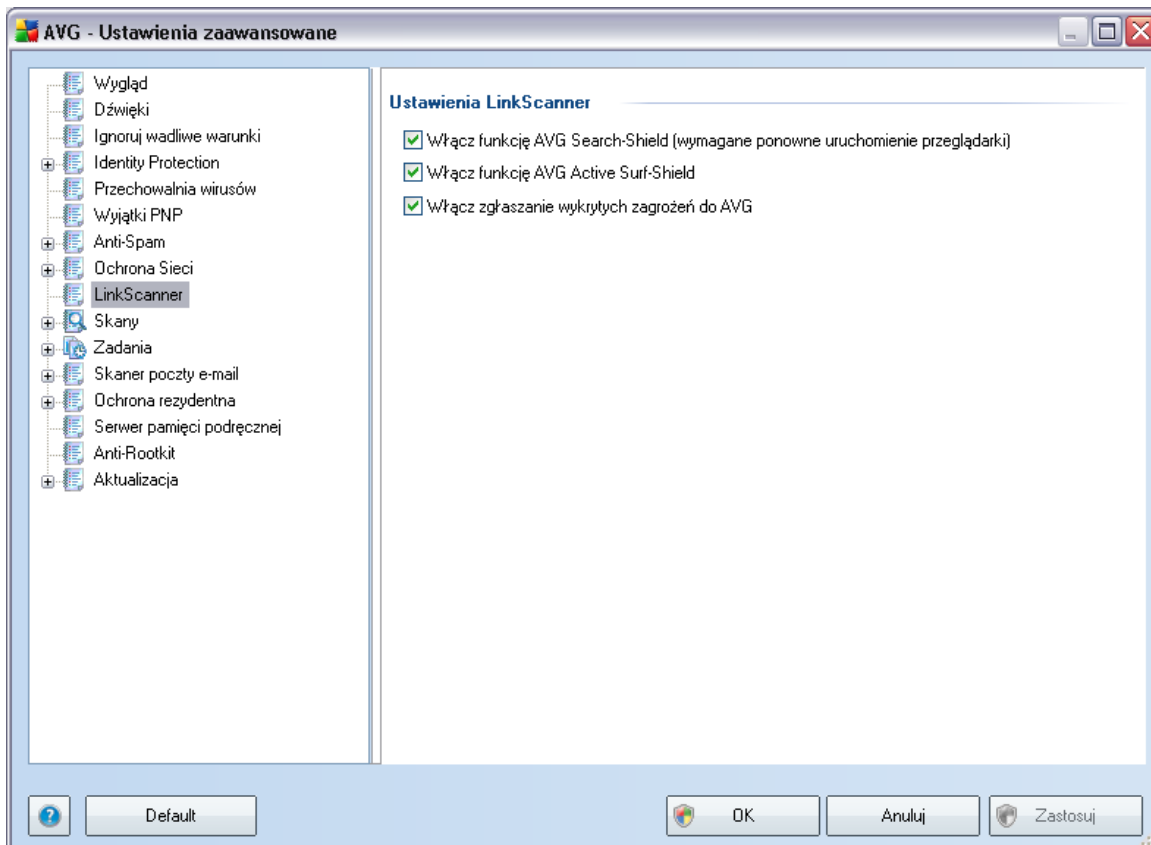


W oknie dialogowym **Ochrona komunikatorów internetowych** można edytować ustawienia składowego **Ochrona Sieci** dotyczące skanowania plików wymienianych za pośrednictwem komunikatorów internetowych. Obecnie obsługiwane są trzy komunikatory: **ICQ**, **MSN** i **Yahoo** — jeśli składowik **Ochrona Sieci** ma sprawdzać, czy komunikacja danego komunikatora jest bezpieczna, należy zaznaczyć odpowiednie pole wyboru.

Aby szczegółowo określić zaufane i blokowane kontakty, należy przejść do odpowiedniego okna dialogowego (**ICQ – Zaawansowane**, **MSN – Zaawansowane** lub **Yahoo – Zaawansowane**) i stworzyć **biała listę** (listę użytkowników, którzy będą mogli przysyłać wiadomości) oraz **czarna listę** (użytkowników, którzy mają być blokowani).

## 10.7. LinkScanner

Okno dialogowe **Ustawienia składnika LinkScanner** umożliwia włączenie/wyłączenie podstawowych funkcji składnika **LinkScanner**:



- **Włącz składnik AVG Search-Shield** (opcja domyślnie włączona) — umożliwia sprawdzanie zawartości stron pojawiających się w wynikach wyszukiwania serwisów Google, Yahoo, Bing, Yandex, Altavista i Baidu i wyświetlanie odpowiednich ikon powiadomien.
- **Włącz funkcję AVG Active Surf-Shield** — (domyślnie włączona): aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (w czasie rzeczywistym). Znane złośliwe witryny i ich niebezpieczna zawartość blokowane są już w momencie otwarcia ich przez użytkownika za pomocą przeglądarki (lub jakiegokolwiek innej aplikacji korzystającej z protokołu HTTP).
- **Włącz zgłaszanie wykrytych zagrożeń do firmy AVG** — (domyślnie

włączone): należy zaznaczyć to pole, aby włączyć raportowanie exploitów oraz niebezpiecznych witryn znalezionych przy użyciu funkcji **AVG Active Surf-Shield** lub **AVG Search-Shield**. Informacje te są przekazywane do naszej bazy danych.

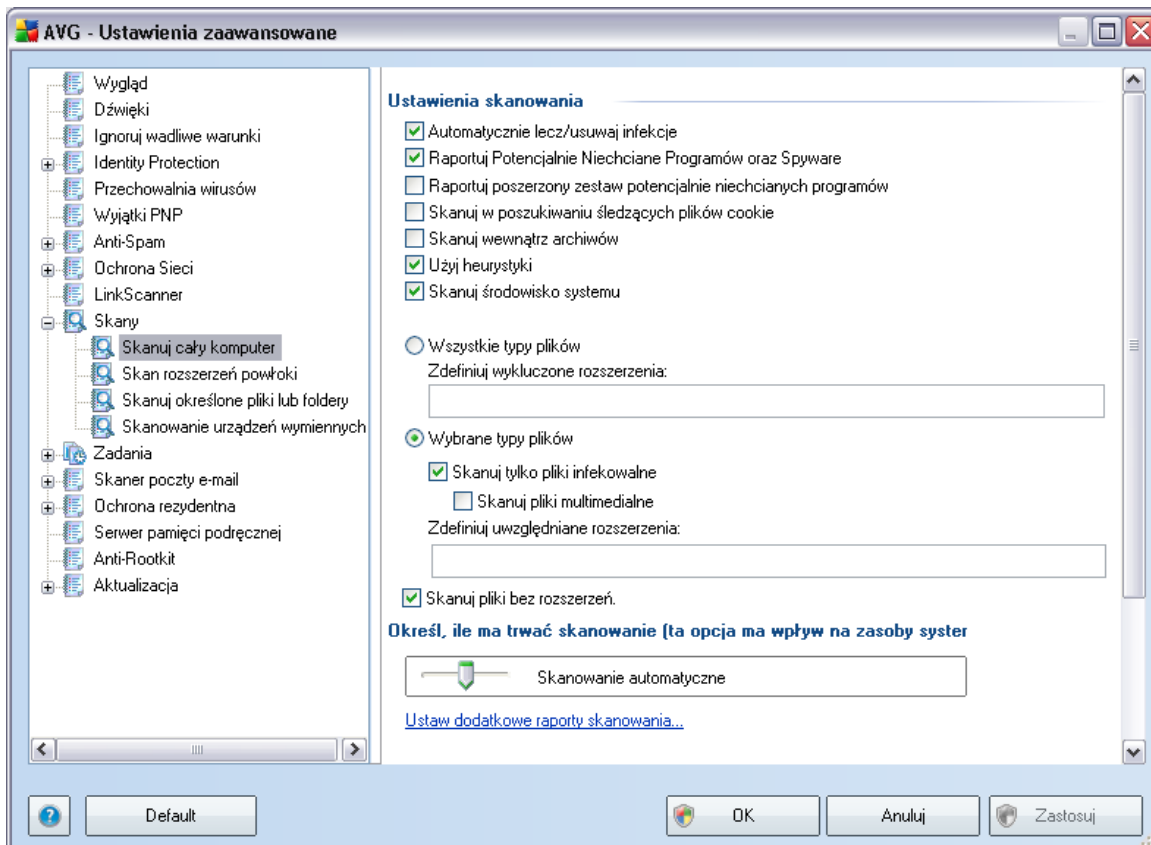
## 10.8. Skany

Zaawansowane ustawienia skanowania podzielone są na trzy kategorie odnoszące się do określonych typów testów zdefiniowanych przez producenta AVG:

- **Skany całego komputera** — standardowe, wstępnie zdefiniowane skanowanie całego komputera.
- **Skany rozszerzenia powłoki** — skanowanie wybranych obiektów bezpośrednio z interfejsu Eksploratora Windows.
- **Skany określonych plików lub folderów** — standardowe, wstępnie zdefiniowane skanowanie określonych obszarów komputera.
- **Skany urządzeń wymiennych** — skanowanie urządzeń wymiennych podłączonych do komputera.

### 10.8.1. Skan całego komputera

Opcja **Skanuj cały komputer** umożliwia edycję parametrów jednego ze wstępnie zdefiniowanych testów: [Skan całego komputera](#):



#### Ustawienia skanowania

Sekcja **Ustawienia skanowania** zawiera listę parametrów silnika skanującego:

- **Automatycznie lecz/usuwać infekcje** — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).
- **Raportuj zagrożenia potencjalnie niechcianymi programami i oprogramowaniem szpiegującym** (opcja domyślnie włączona) —

zaznaczenie tego pola powoduje włączenie silnika **Anti-Spyware** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). [Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie.](#) Nie zaleca się wyłączenia tej opcji — znacząco zwiększa ona poziom ochrony komputera.

- **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości [oprogramowania szpiegującego](#), czyli programów, które są zupełnie bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.
- **Skanuj w poszukiwaniu śledzących plików cookie** — ten parametr składnika [Anti-Spyware](#) określa, że skanowanie ma wykrywać pliki cookie (*pliki cookie są w protokole HTTP używane do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach, na przykład preferencji wyglądu witryny czy zawartości koszyków w sklepach internetowych*).
- **Skanuj wewnątrz archiwów** — parametr ten określa, czy skanowanie ma obejmować wszystkie pliki — nawet te znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** — analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) jest jedną z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj środowisko systemu** — skanowanie obejmie także obszary systemowe komputera.

Następnie należy zdecydować, czy skanowane mają być

- **Wszystkie typy plików** z opcja zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami (*po zapisaniu przecinki zostają zamienione na średniki*) rozszerzeń plików, które mają nie być skanowane;
- **Wybrane typy plików** — skanowane będą tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowanie skróci się jeszcze bardziej, ponieważ takie pliki często są*

duże, a nie są podatne na infekcje). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

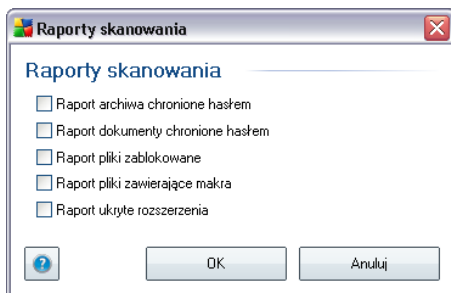
- Opcjonalnie można zdecydować o **skanowaniu plików bez rozszerzenia** — ta opcja jest domyślnie włączona i zaleca się niezmiianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

### Priorytet procesu skanowania

W sekcji **Priorytet procesu skanowania** można szczegółowo określić zadana prędkość skanowania, w zależności od wykorzystania zasobów systemowych. Domyślnie wartość tej opcji jest na średnim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jeśli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowolnić działanie innych procesów i aplikacji (*opcji można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

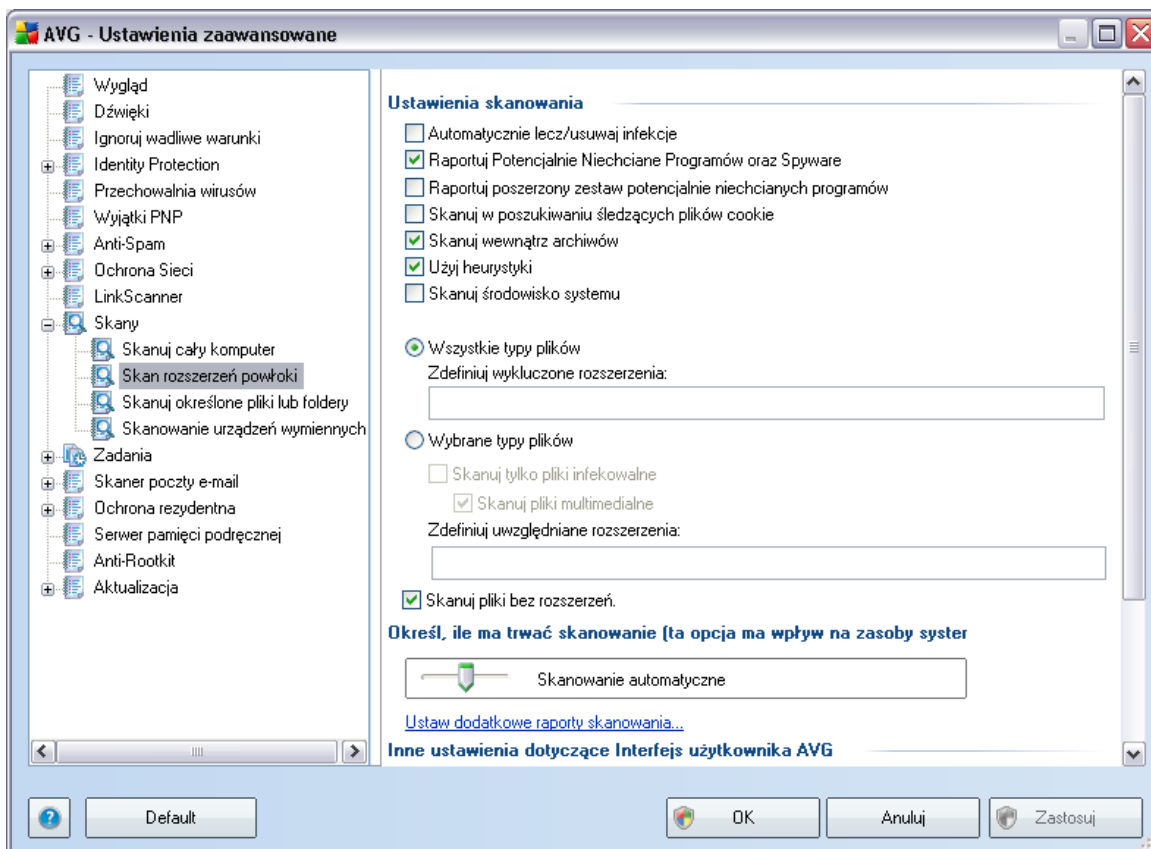
### Ustaw dodatkowe raporty skanowania...

Kliknięcie linku **Ustaw dodatkowe raporty skanowania...** powoduje otwarcie osobnego okna dialogowego **Raporty skanowania**, w którym można określić szczegółowość raportów, zaznaczając zadane elementy:



### 10.8.2. Skan rozszerzenia powłoki

Analogicznie do [Skanu całego komputera](#), test **Skan rozszerzenia powłoki** także oferuje szereg opcji silnika skanującego, zdefiniowanych wstępnie przez dostawcę oprogramowania AVG. W tym przypadku konfiguracja odnosi się do [skanowania określonych obiektów bezpośrednio z interfejsu Eksploratora Windows](#) (*rozszerzenie powłoki*); zobacz rozdział [Skanowanie z poziomu Eksploratora Windows](#):

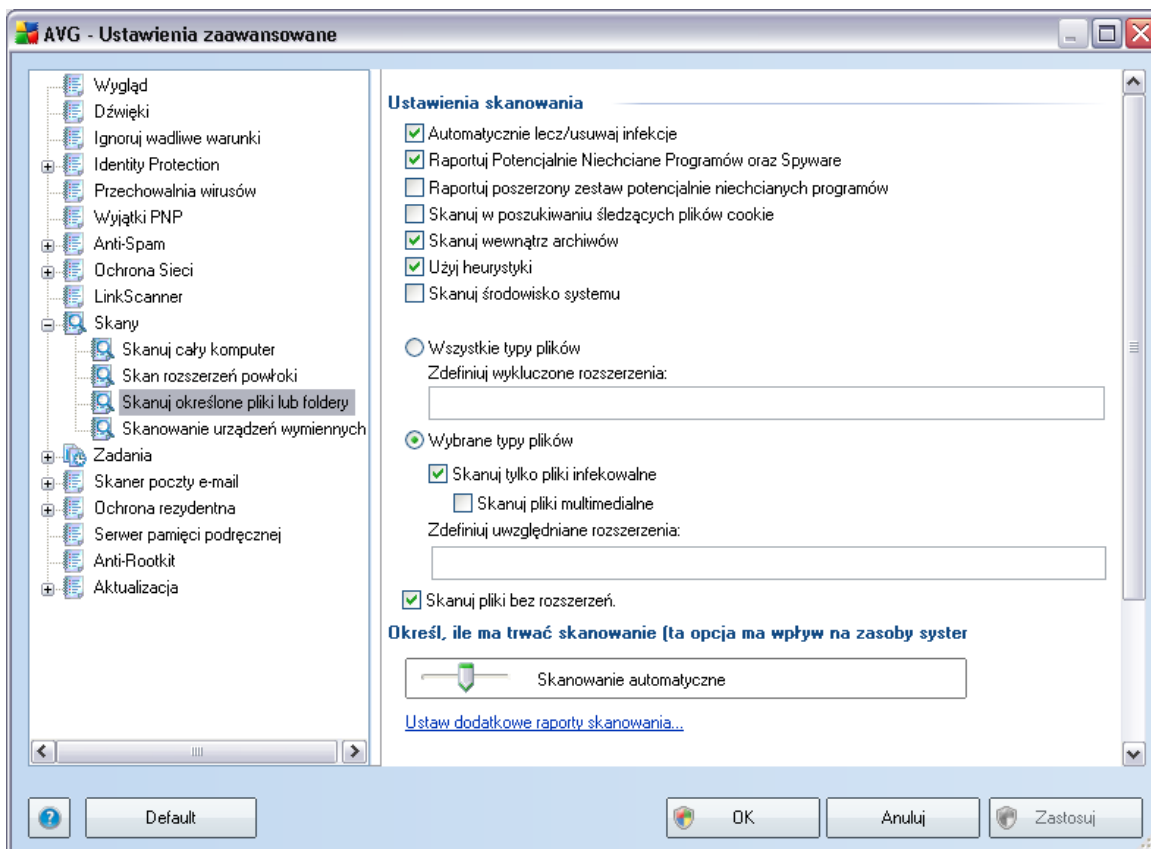


Lista parametrów jest identyczna jak dla testu [Skan całego komputera](#). Ustawienia domyślne są jednak inne: większość opcji [skanu całego komputera](#) jest aktywna, natomiast w przypadku [skanu rozszerzenia powłoki \(Skanowanie z poziomu Eksploratora Windows\)](#) wybrane są tylko najistotniejsze parametry.

**Uwaga:** Opis poszczególnych parametrów można znaleźć w rozdziale [Zaawansowane ustawienia AVG / Skany / Skan całego komputera](#).

### 10.8.3. Skan określonych plików lub folderów

Interfejs edycji testu [Skan określonych plików lub folderów](#) jest identyczny jak w przypadku [Skanu całego komputera](#). Wszystkie opcje konfiguracyjne są takie same, jednak ustawienia domyślne dla [skanu całego komputera](#) są bardziej rygorystyczne:

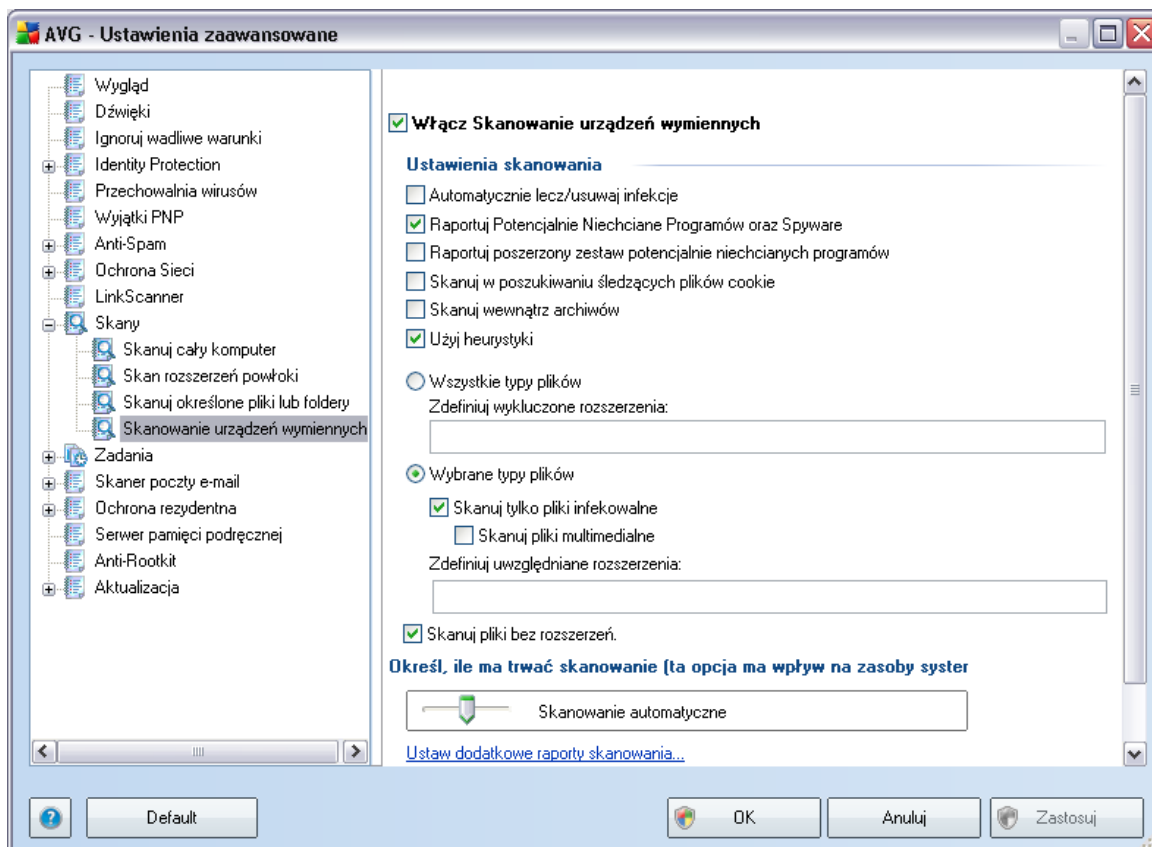


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych do **skanowania określonych plików lub folderów!**

**Uwaga:** Opis poszczególnych parametrów można znaleźć w rozdziale **Zaawansowane ustawienia AVG / Skany / Skan całego komputera.**

#### 10.8.4. Skan urządzeń wymiennych

Okno z opcjami ***Skanu urządzeń wymiennych*** jest także bardzo podobne do okna [Skan całego komputera](#):



***Skan urządzeń wymiennych*** jest uruchamiany automatycznie po podłączeniu do komputera dowolnego urządzenia wymiennego. Domyslnie jest on wyłączony. Skanowanie urządzeń wymiennych w poszukiwaniu potencjalnych zagrożeń jest jednak bardzo ważne, ponieważ są one częstym źródłem infekcji. Jeśli skan ma być uruchamiany automatycznie, należy zaznaczyć opcję ***Włącz skanowanie urządzeń wymiennych***.

***Uwaga:*** Opis poszczególnych parametrów można znaleźć w rozdziale [Zaawansowane ustawienia AVG / Skany / Skan całego komputera](#).

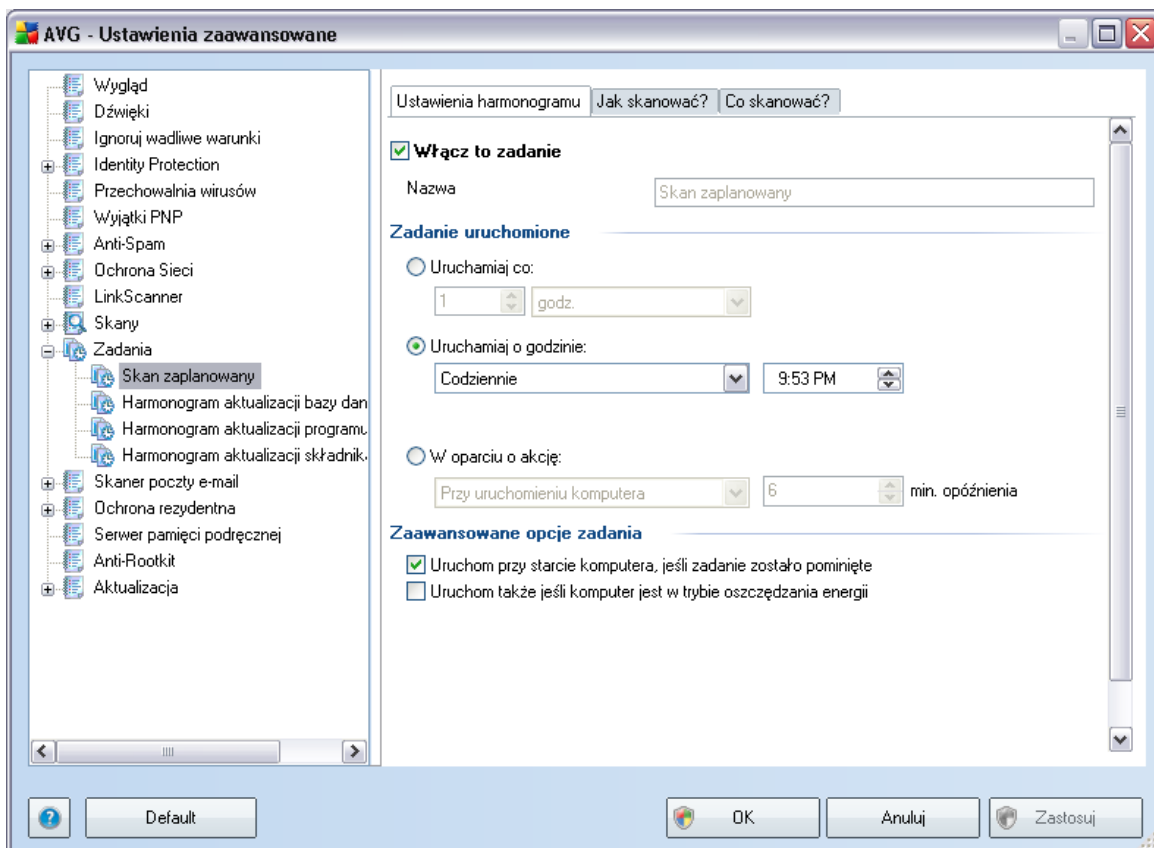
## 10.9. Zaplanowane zadania

W oknie **Zadania** można edytować domyślne ustawienia następujących pozycji:

- [Skan zaplanowany](#)
- [Harmonogram aktualizacji bazy wirusów](#)
- [Harmonogram aktualizacji programu](#)

### 10.9.1. Skan zaplanowany

Parametry skanowania zaplanowanego można edytować (*albo utworzyć nowy harmonogram*) na trzech kartach:



Na karcie **Ustawienia harmonogramu** można zaznaczyć/odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowany test lub włączyć go ponownie, gdy zajdzie taka potrzeba.

W polu tekstowym **Nazwa** (*wylaczone dla harmonogramów domyślnych*) wyświetlana jest nazwa przypisana do danego harmonogramu przez producenta programu. W przypadku nowych harmonogramów (*aby dodać harmonogram, należy kliknąć prawym przyciskiem myszy element **Skan zaplanowany** w drzewie nawigacji po lewej*) można określić własną nazwę, a wspomniane pole tekstowe jest edytowalne. Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości.

**Przykład:** Nazwy takie jak „Nowy skan” lub „Mój skan” nie są odpowiednie, ponieważ nie informują o tym, co jest przedmiotem skanowania. Przykładem dobrej, opisowej nazwy jest „Skan obszarów systemowych”. Ponadto, nie ma potrzeby określać w nazwie skanowania, czy skanowany jest cały komputer, czy tylko jego wybrane obszary — własne testy użytkownika są zawsze specyficznym [skanowaniem określonych plików lub folderów](#).

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

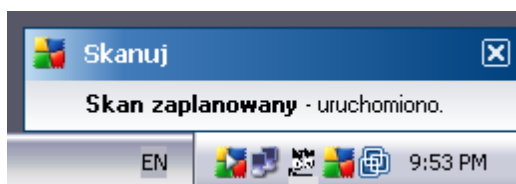
### Zadanie uruchomione

W tym miejscu można określić, jak często ma być uruchamiane nowe skanowanie. Uruchamianie skanowania może być powtarzane w określonych odstępach czasu (**Uruchamiaj co**) lub w zadanych momentach (**Uruchamiaj o określonej godzinie**), a także na skutek wystąpienia określonego zdarzenia (**akcja powiązana z uruchomieniem komputera**).

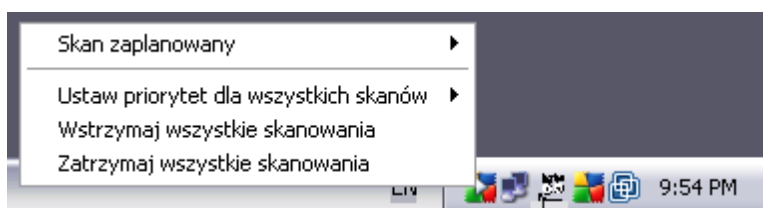
### Zaawansowane opcje harmonogramu

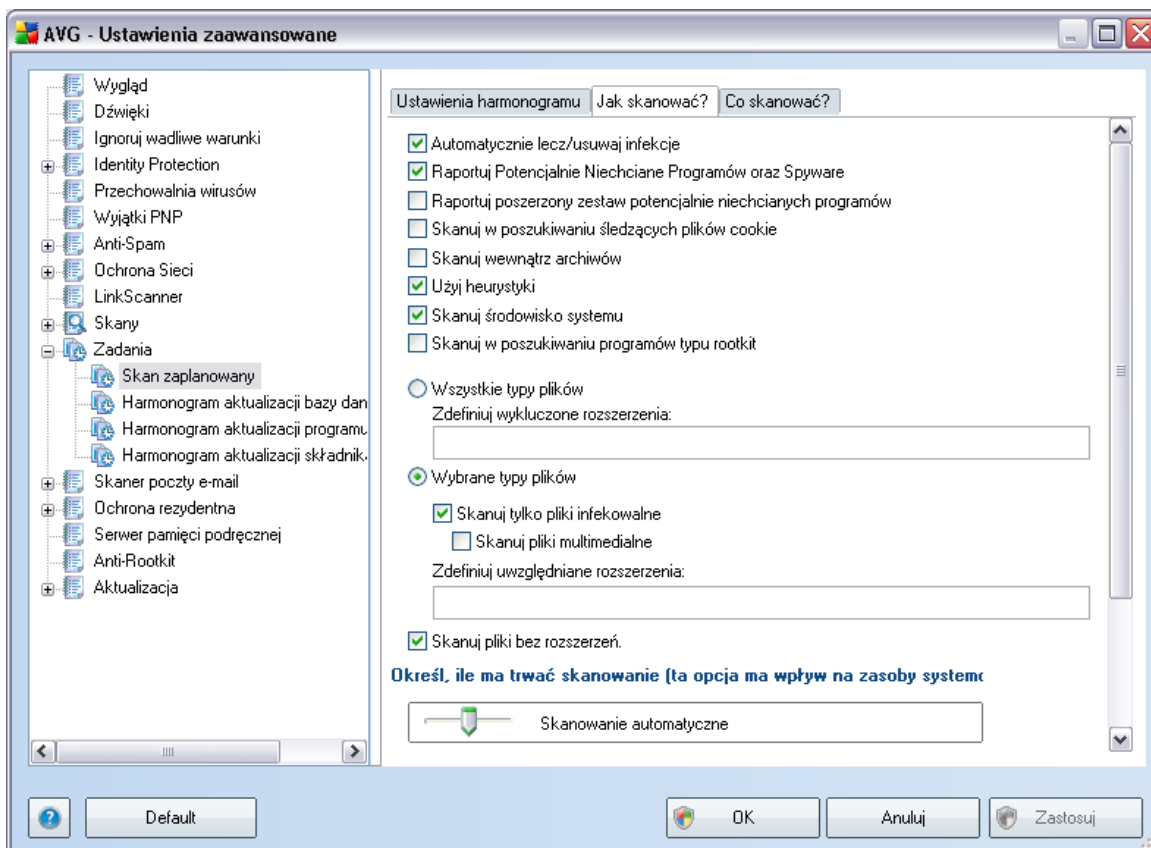
Ta sekcja umożliwia zdefiniowanie warunków uruchamiania skanowania w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

Po rozpoczęciu zaplanowanego skanu, nad [ikoną AVG na pasku zadań](#) wyświetlone zostanie odpowiednie powiadomienie:



Następnie pojawi się tam nowa [ikona AVG](#) (kolorowa, z białą strzałką — jak powyżej), która informuje o uruchomieniu skanowania. Kliknięcie jej prawym przyciskiem myszy pozwala wyświetlić menu kontekstowe, dzięki któremu można wstrzymać lub anulować skanowanie:





Karta **Jak skanować?** zawiera listę parametrów testu, które można włączyć lub wyłączyć. Domyślnie większość funkcji jest włączona, a odpowiadające im ustawienia są stosowane podczas skanowania. Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachowując wstępnie zdefiniowaną konfigurację:

- **Automatycznie lecz/usuwać infekcje** — jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbe automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).
- **Raportuj zagrożenia potencjalnie niechcianymi programami i oprogramowaniem szpiegującym** (opcja domyślnie włączona) — zaznaczenie tego pola powoduje włączenie silnika [Anti-Spyware](#) i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). [Oprogramowanie szpiegujące należy do nietypowej](#)

[kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie.](#) Nie zaleca się wyłączenia tej opcji — znacząco zwiększa ona poziom ochrony komputera.

- **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości [oprogramowania szpiegującego](#), czyli programów, które są zupełnie bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.
- **Skanuj w poszukiwaniu śledzących plików cookie** (opcja domyślnie włączona) — ten parametr składownika [Anti-Spyware](#) określa, czy wykrywane mają być pliki cookie (używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach - np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** — (domyślnie włączona) parametr ten określa, czy skanowanie ma obejmować wszystkie pliki, nawet te znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** — (domyślnie włączona) analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny) jest jedną z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj środowisko systemu** — (domyślnie włączona) skanowanie obejmie także obszary systemowe komputera.
- **Skanuj w poszukiwaniu programów typu rootkit** — zaznaczenie tej pozycji pozwala dołączyć wykrywanie programów typu rootkit do operacji skanowania całego komputera. Test Anti-Rootkit można także uruchomić niezależnie, dzięki interfejsowi składownika [Anti-Rootkit](#)

Następnie należy zdecydować, czy skanowane mają być

- **Wszystkie typy plików** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami (po zapisaniu przecinki zostają zamienione na średniki) rozszerzeń plików, które mają nie być skanowane;
- **Wybrane typy plików** — skanowane będą tylko pliki infekowalne (pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne), z uwzględnieniem plików

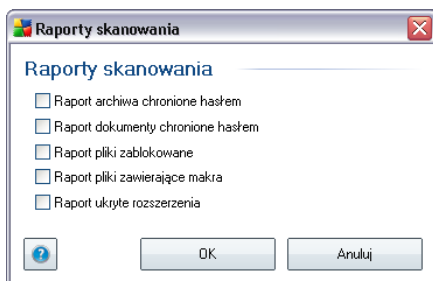
multimedialnych (plików wideo i audio — jeśli to pole pozostanie niezaznaczone, czas skanowanie skróci się jeszcze bardziej, ponieważ takie pliki często są duże, a nie są podatne na infekcje). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

- Opcjonalnie można zdecydować o **skanowaniu plików bez rozszerzenia** — ta opcja jest domyślnie włączona i zaleca się niezmienną tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

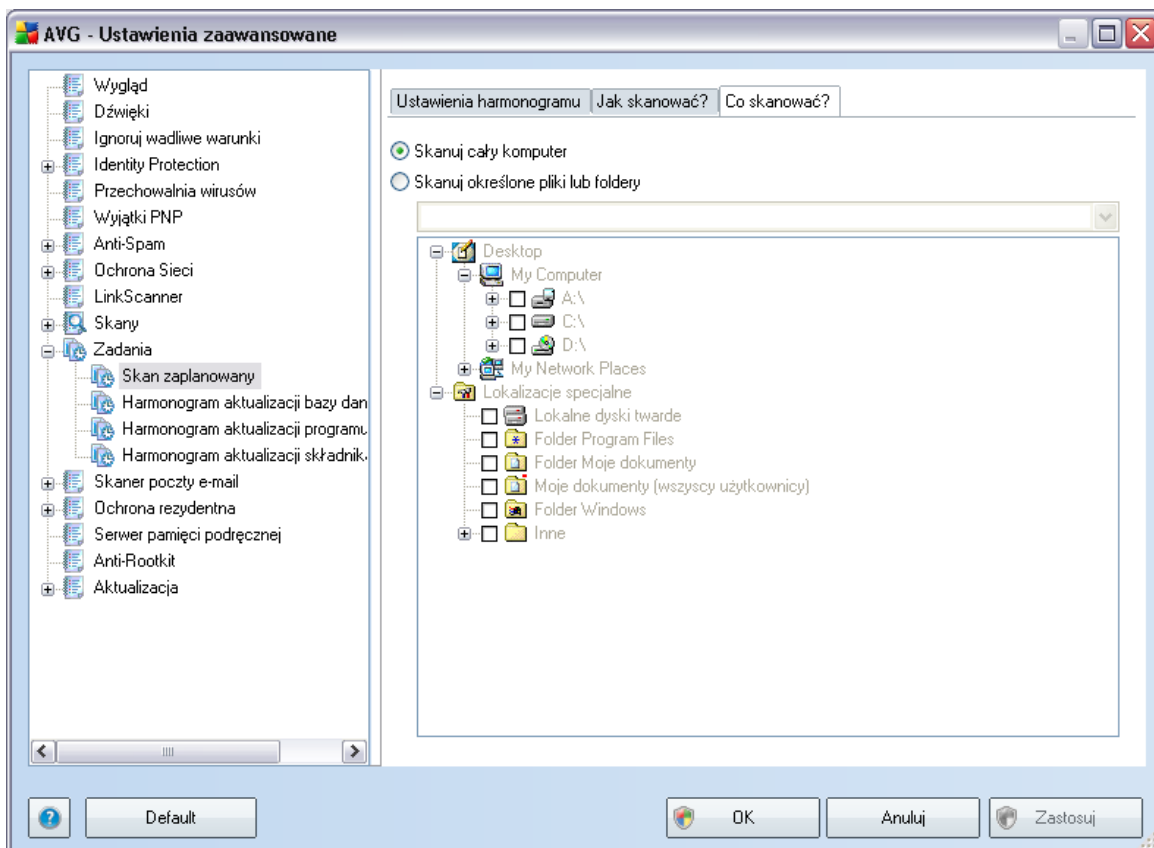
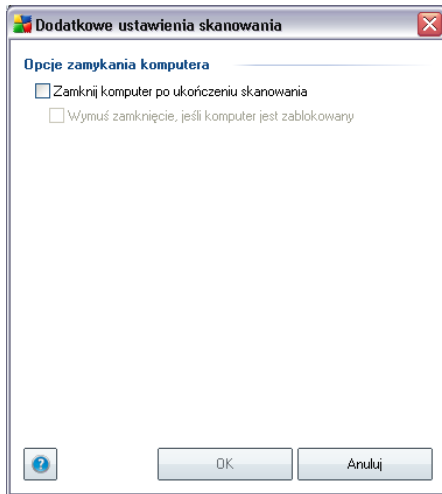
### Priorytet procesu skanowania

W sekcji **Priorytet procesu skanowania** można szczegółowo określić zadana prędkość skanowania, w zależności od wykorzystania zasobów systemowych. Domyślnie wartość tej opcji jest na średnim poziomie, co oznacza automatyczne ustalenie wykorzystania zasobów. Jeśli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowolnić działanie innych procesów i aplikacji (opcji można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

Kliknięcie linku **Ustaw dodatkowe raporty skanowania...** powoduje otwarcie osobnego okna dialogowego **Raporty skanowania**, w którym można określić szczegółowość raportów, zaznaczając zadane elementy:

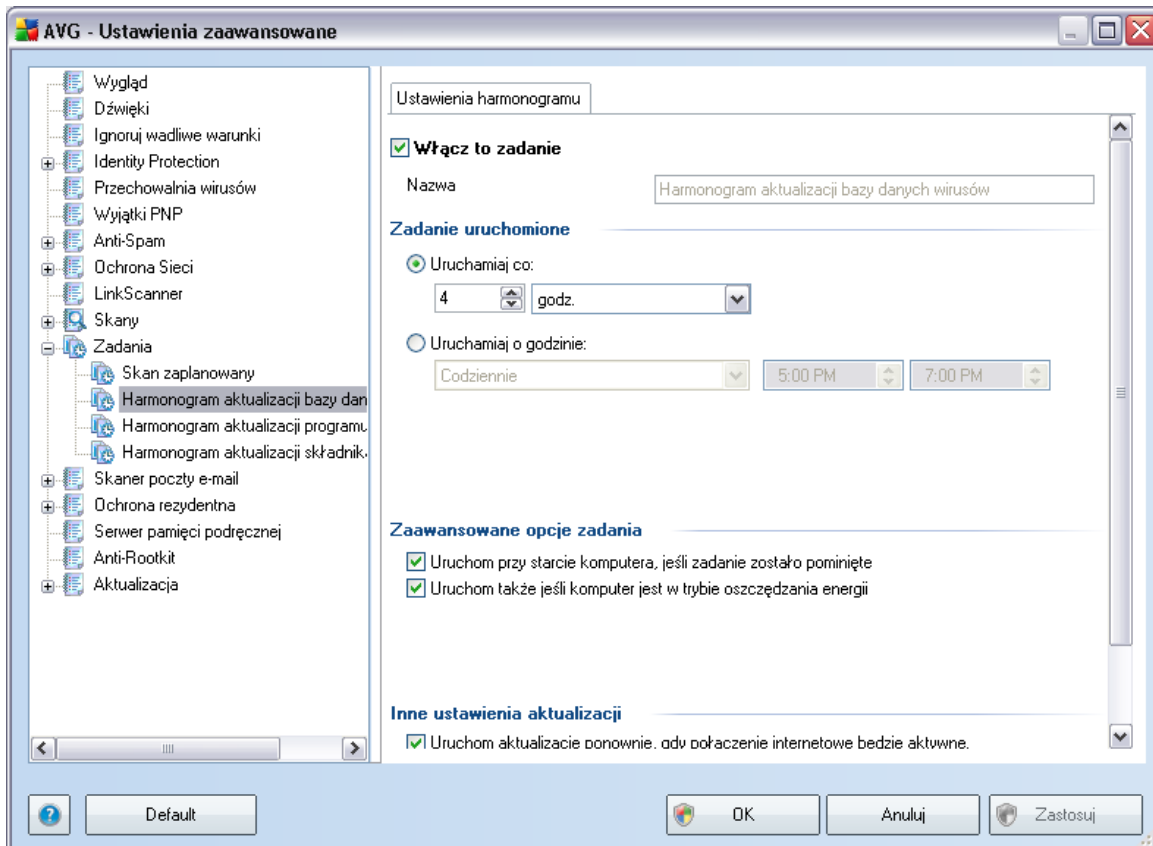


**Dodatkowe ustawienia skanowania** — link ten pozwala otworzyć nowe okno dialogowe **Opcje zamykania komputera**, w którym można określić, czy komputer ma być zamykany automatycznie po zakończeniu procesu skanowania. Wybranie tej opcji (**Zamknij komputer po ukończeniu skanowania**) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (**Wymus zamknięcie, jeśli komputer jest zablokowany**).



Na karcie **Co skanowac?** można określić, czy planowane jest [skanowanie całego komputera](#), czy [skanowanie określonych plików lub folderów](#). W przypadku skanowania określonych plików lub folderów, w dolnej części okna dialogowego aktywowane jest drzewo katalogów, w którym można wybrać obiekty do przeskanowania.

## 10.9.2. Harmonogram aktualizacji bazy wirusów



Na karcie **Ustawienia harmonogramu** można odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowaną aktualizację bazy wirusów i włączyć ją ponownie dopiero gdy zajdzie taka potrzeba. Podstawowe opcje harmonogramu aktualizacji bazy wirusów dostępne są w składniku [Menedżer aktualizacji](#). W niniejszym oknie można ustawić szczegółowe parametry harmonogramu. W polu tekstowym **Nazwa** (wylaczone dla harmonogramów domyślnych) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta programu.

### Zadanie uruchomione

W tej sekcji należy określić interwał dla planowanych aktualizacji bazy danych wirusów. Można określić, że uruchamianie aktualizacji będzie następować stale co pewien czas (**Uruchom co ...**) lub definiując określoną datę i godzinę (**Uruchom o określonej godzinie ...**).

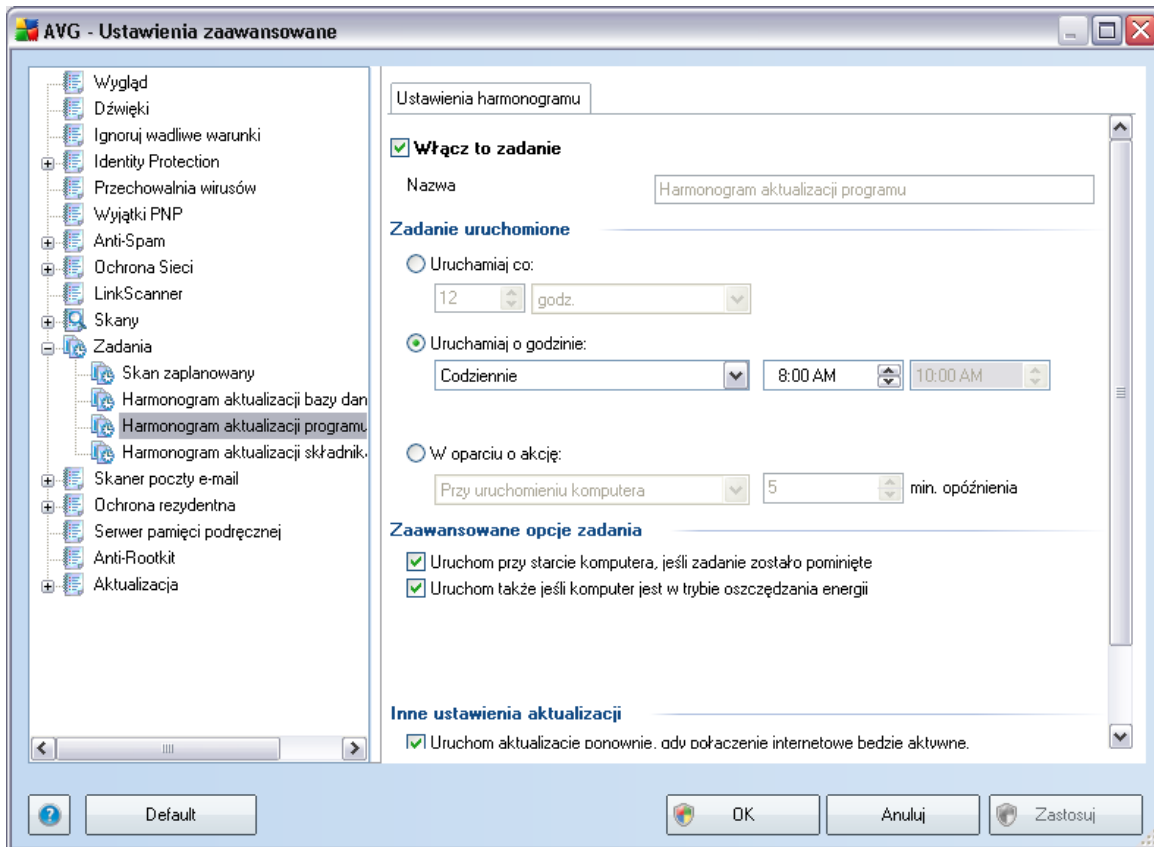
### **Zaawansowane opcje harmonogramu**

Ta sekcja umożliwi zdefiniowanie warunków uruchamiania aktualizacji bazy wirusów w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

### **Inne ustawienia aktualizacji**

Na koniec należy zaznaczyć pole wyboru **Uruchom aktualizacje natychmiast po nawiązaniu połączenia z internetem**, aby upewnić się, że jeśli połączenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie się, po ponownym połączeniu z internetem aktualizacja zostanie rozpoczęta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o określonej godzinie, nad [ikoną systemu AVG na pasku systemowym](#) wyświetlone zostanie odpowiednie powiadomienie (przy domyślnej konfiguracji zastosowanej w sekcji [Ustawienia zaawansowane/Wygląd](#)).



Na karcie **Ustawienia harmonogramu** można odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowaną aktualizację programu i włączyć ją ponownie dopiero gdy zajdzie taka potrzeba. W polu tekstowym **Nazwa** (wylaczone dla harmonogramów domyślnych) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta programu.

### Zadanie uruchomione

W tym miejscu należy określić interwał dla nowo zaplanowanych aktualizacji programu. Uruchamianie aktualizacji może być powtarzane w określonych odstępach czasu (**Uruchamiam co**) lub w zadanych momentach (**Uruchamiam o określonej godzinie**), a także na skutek wystąpienia określonego zdarzenia (**akcja powiązana z uruchomieniem komputera**).

### Zaawansowane opcje harmonogramu

Ta sekcja umożliwia zdefiniowanie warunków uruchamiania aktualizacji programu w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

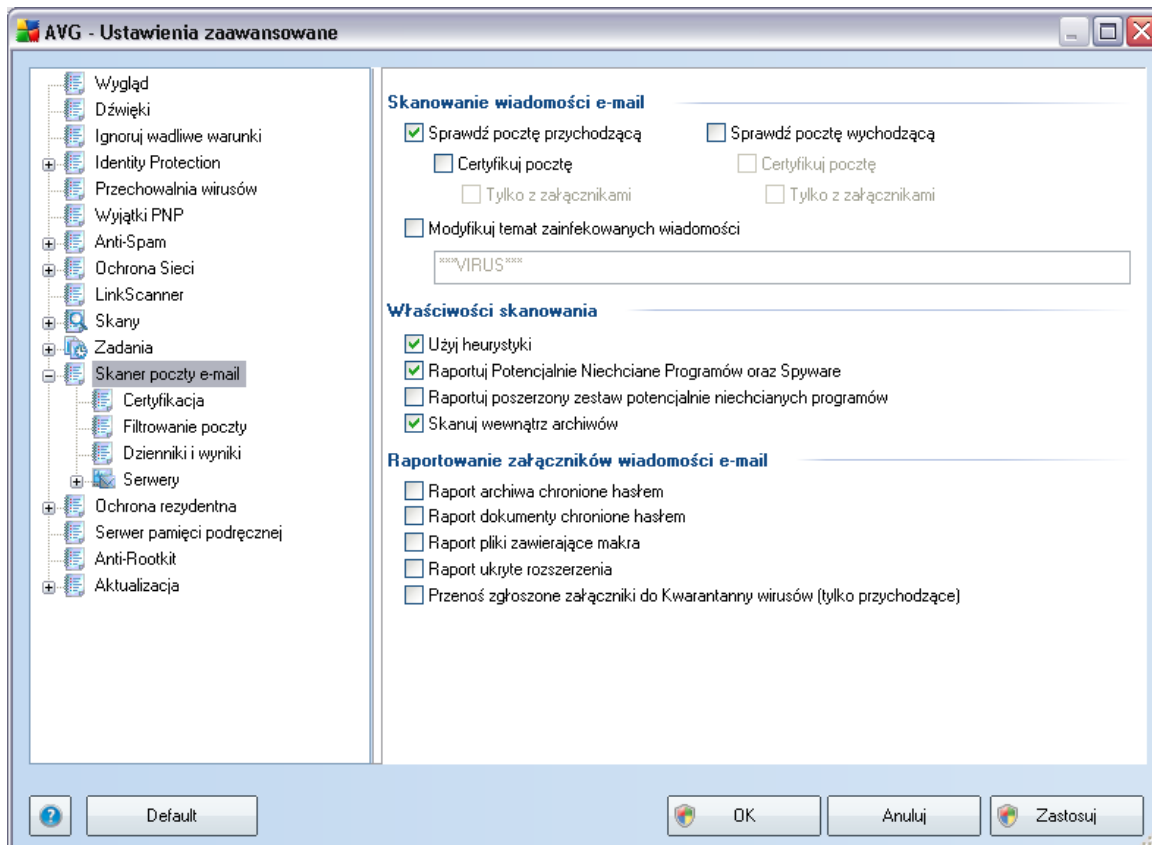
### Inne ustawienia aktualizacji

Na koniec należy zaznaczyć pole wyboru **Uruchom aktualizacje natychmiast po nawiązaniu połączenia z internetem**, aby upewnić się, że jeśli połączenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie się, po ponownym połączeniu z internetem aktualizacja zostanie rozpoczęta na nowo.

Po uruchomieniu zaplanowanej aktualizacji o określonej godzinie, nad [ikoną systemu AVG na pasku systemowym](#) wyświetlone zostanie odpowiednie powiadomienie (przy domyślnej konfiguracji zastosowanej w sekcji [Ustawienia zaawansowane/Wygląd](#)).

**Uwaga:** Jeśli zaplanowane skanowanie i zaplanowana aktualizacja nałożą się, proces aktualizacji będzie miał pierwszeństwo i skanowanie zostanie przerwane.

## 10.10. Skaner poczty e-mail



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

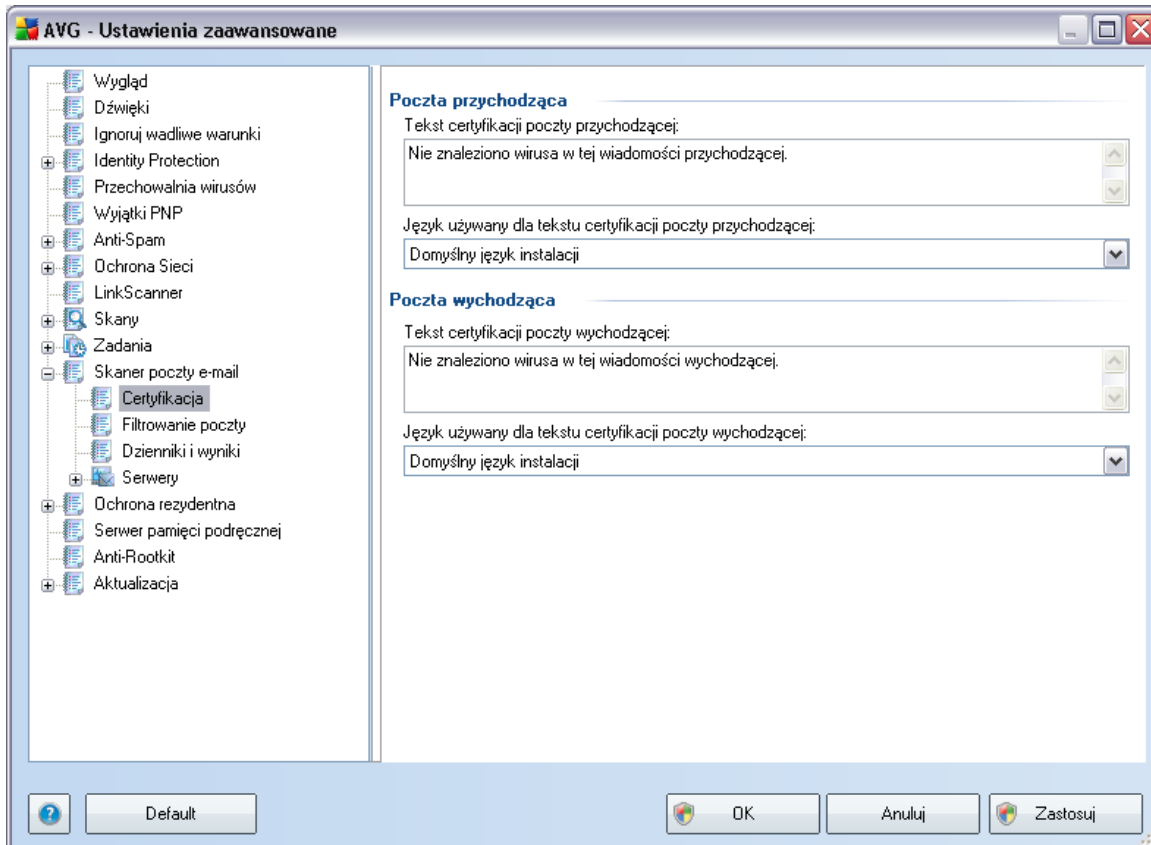
- **Skanowanie wiadomości e-mail** — w tej sekcji można określić następujące podstawowe ustawienia, dla przychodzących i/lub wychodzących wiadomości e-mail:
  - Czy wiadomości e-mail mają być skanowane w poszukiwaniu wirusów.
  - Czy na końcu każdej wolnej od wirusów wiadomości e-mail ma być dodawany tekst certyfikujący. Tekst może zostać dostosowany w oknie dialogowym [Certyfikacja](#)
  - Czy tekst certyfikacji ma być dodawany tylko do wiadomości z załącznikami.

Aby **modyfikować temat zainfekowanych wiadomości**, należy zaznaczyć odpowiednie pole i wpisać zadany tekst. Wartość ta będzie dodawana do tematu każdej zainfekowanej wiadomości, aby ułatwić jej zidentyfikowanie i odfiltrowanie. Wartość domyślna to **\*\*\*WIRUS\*\*\***; zaleca się jej zachowanie.

- **Właściwości skanowania** — w tej sekcji można określić sposób skanowania wiadomości e-mail:
  - **Użyj analizy heurystycznej** — zaznaczenie tego pola umożliwia korzystanie z [analizy heurystycznej](#) podczas skanowania wiadomości e-mail. Gdy ta opcja jest włączona, możliwe jest filtrowanie załączników nie tylko według ich rozszerzenia, ale również na podstawie ich właściwej zawartości. Opcje filtrów mogą zostać dostosowane w oknie [Filtrowanie poczty](#).
  - **Raportuj zagrożenia potencjalnie niechcianymi programami i oprogramowaniem szpiegującym** (opcja domyślnie włączona) — zaznaczenie tego pola powoduje włączenie silnika **Anti-Spyware** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). [Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie.](#) Nie zaleca się wyłączenia tej opcji — znacząco zwiększa ona poziom ochrony komputera.
  - **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości [oprogramowania szpiegującego](#), czyli programów, które są zupełnie bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.
  - **Skanuj wewnątrz archiwów** — zaznaczenie tego pola umożliwia skanowanie zawartości archiwów dołączonych do wiadomości e-mail.
- **Zgłaszanie załączników poczty e-mail** — w tej sekcji można skonfigurować dodatkowe raporty dotyczące potencjalnie niebezpiecznych lub podejrzanych plików. Należy zwrócić uwagę na fakt, że Skaner poczty e-mail nie wyświetla zazwyczaj żadnych komunikatów z ostrzeżeniem, a jedynie dodaje na końcu wiadomości tekst certyfikacji. Historie działań tego składowika można przejrzeć w oknie [Zagrożenia wykryte przez Skaner poczty e-mail](#).

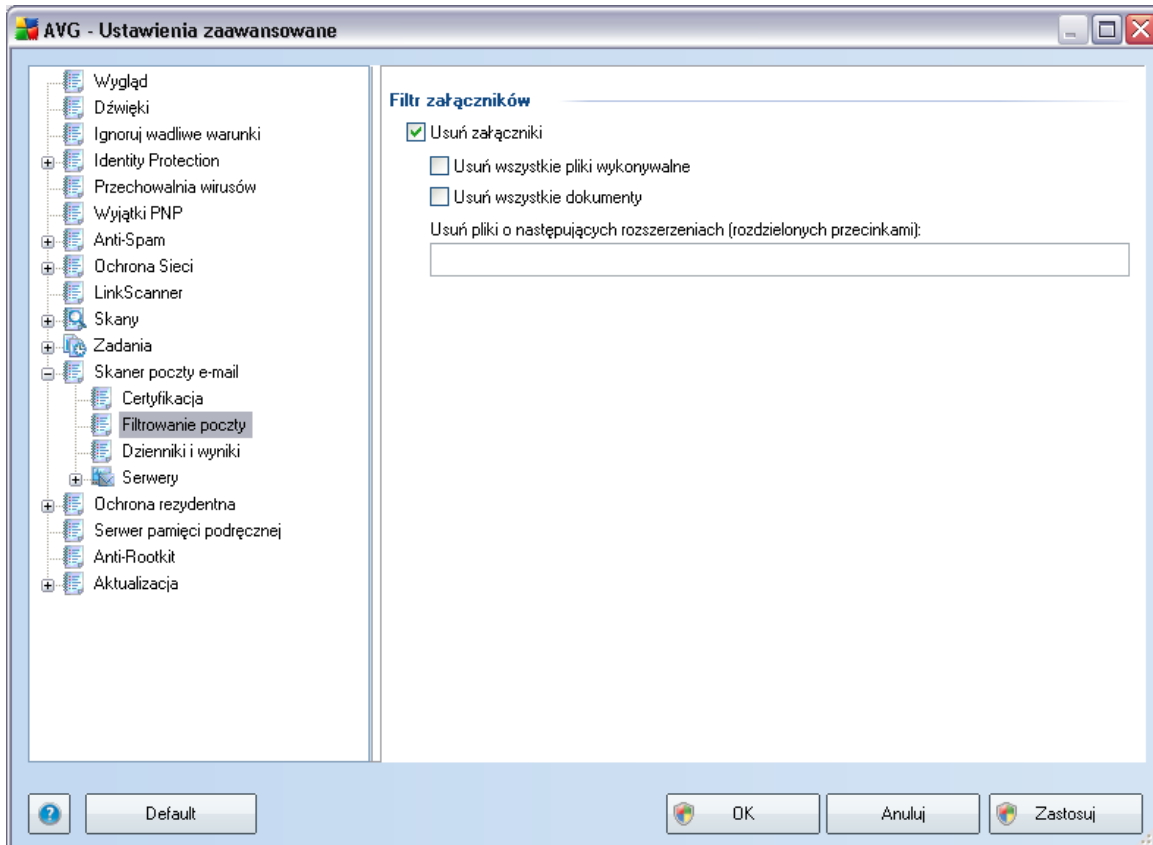
- **Raportuj archiwa chronione haslem** — archiwów (ZIP, RAR itp.) chronionych haslem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.
- **Raportuj dokumenty chronione haslem** — dokumentów chronionych haslem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.
- **Raportuj pliki zawierające makra** — makro to predefiniowana sekwencja kroków mająca ułatwić wykonywanie określonych czynności (szeroko znane są np. makra programu MS Word). Makra mogą być potencjalnie niebezpieczne — warto zaznaczyć to pole, aby mieć pewność, że pliki zawierające makra będą raportowane jako podejrzane.
- **Raportuj ukryte rozszerzenia** — ukryte rozszerzenia mogą maskować podejrzane pliki wykonywalne (np. plik.txt.exe) jako niegroźne pliki tekstowe (np. plik.txt). Należy zaznaczyć to pole wyboru, aby zgłaszać je jako potencjalnie niebezpieczne.
- **Przenos raportowane załączniki do Przechowalni wirusów** — należy określić, czy system ma powiadamiać pocztą e-mail o archiwach zabezpieczonych hasłem, dokumentach zabezpieczonych hasłem, plikach zawierających makra i/lub plikach o ukrytych rozszerzeniach, które zostaną wykryte jako załączniki do skanowanych wiadomości e-mail. Należy także określić, czy w przypadku wykrycia takiej wiadomości podczas skanowania zainfekowany obiekt ma zostać przeniesiony do [Przechowalni wirusów](#).

### 10.10.1. Certyfikacja



W oknie **Certyfikacja** można szczegółowo określić treść certyfikatu oraz jego język. Ustawienia te należy wprowadzić osobno dla **wiadomości przychodzących** i **wychodzących**.

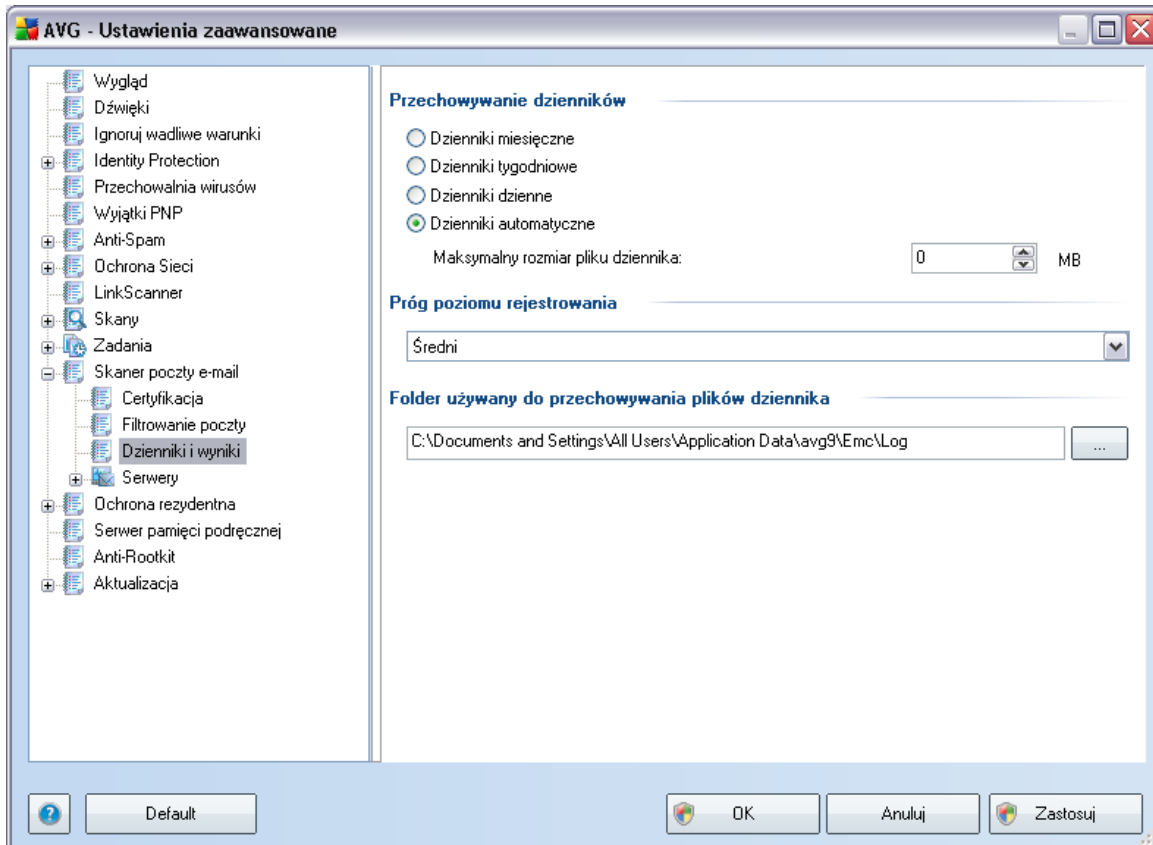
## 10.10.2. Filtrowanie poczty



W oknie **Filtr załączników** można ustawić parametry skanowania załączników e-mail. Opcja **Usun załączniki** jest domyślnie wyłączona. Jeśli zostanie włączona, wszystkie załączniki wiadomości zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, będą automatycznie usuwane. Aby określić typy załączników, które mają być usuwane, należy zaznaczyć odpowiednią opcję:

- **Usun wszystkie pliki wykonywalne** — usunięte będą wszystkie pliki \*.exe.
- **Usun wszystkie dokumenty** — usunięte zostaną wszystkie pliki \*.doc, \*.docx, \*.xls, \*.xlsx.
- **Usun pliki o następujących rozszerzeniach oddzielonych przecinkami** — usunięte będą wszystkie pliki o zdefiniowanych rozszerzeniach.

### 10.10.3. Dzienniki i Wyniki

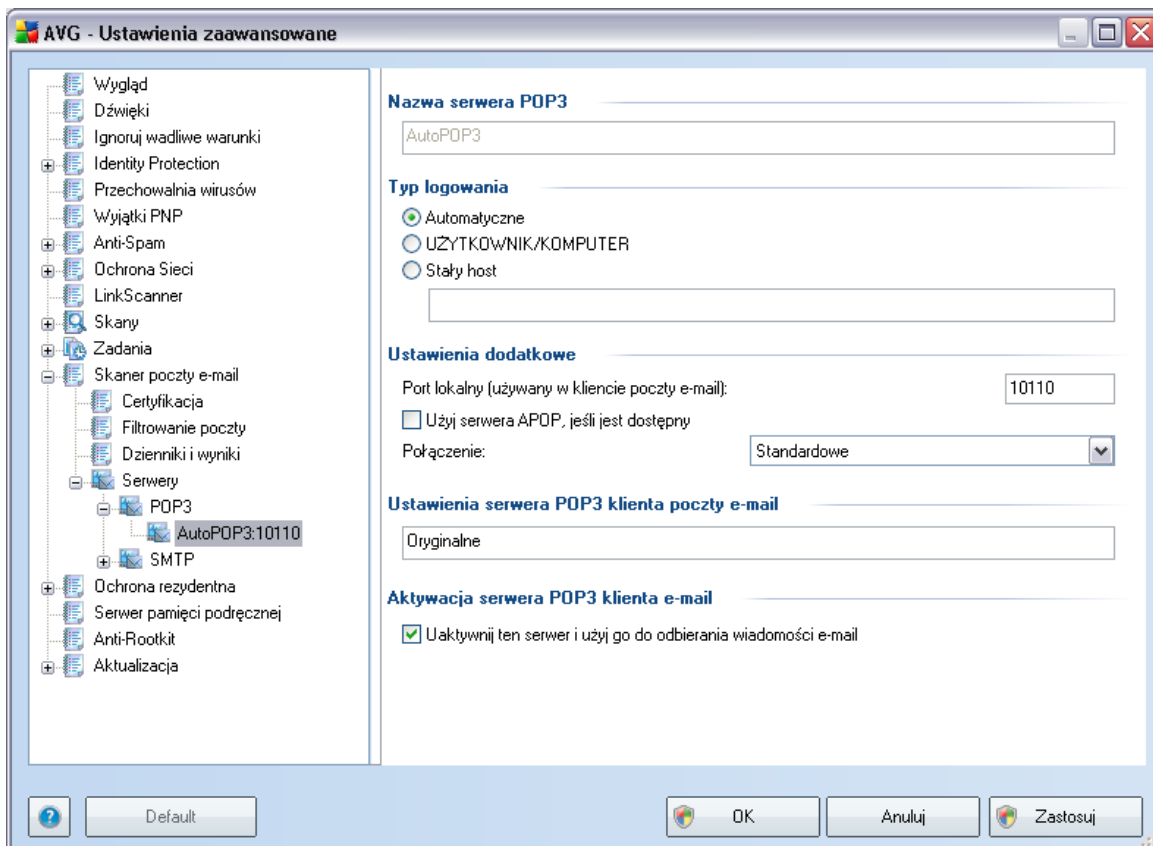


W oknie **Dzienniki i wyniki** można określić parametry przechowywania wyników skanowania poczty e-mail. Okno to podzielone jest na dwa obszary:

- **Przechowywanie dzienników** — pozwala zdecydować, czy informacje o skanowaniu poczty e-mail mają być rejestrowane codziennie, co tydzień, co miesiąc itd.; można tu także określić maksymalny rozmiar pliku dziennika (w MB).
- **Próg poziomu rejestrowania** — domyślnie ustawiony jest poziom średni; można wybrać niższy (*rejestrowanie podstawowych informacji o połączeniu*) lub wyższy (*rejestrowanie całego ruchu*).
- **Folder używany do przechowywania plików dziennika** — pozwala określić, gdzie mają znajdować się pliki dziennika.

#### 10.10.4. Serwery

W sekcji **Serwery** edytować można parametry wirtualnych serwerów [Skanera poczty e-mail](#) lub zdefiniować nowy (klikając przycisk **Dodaj nowy serwer**).



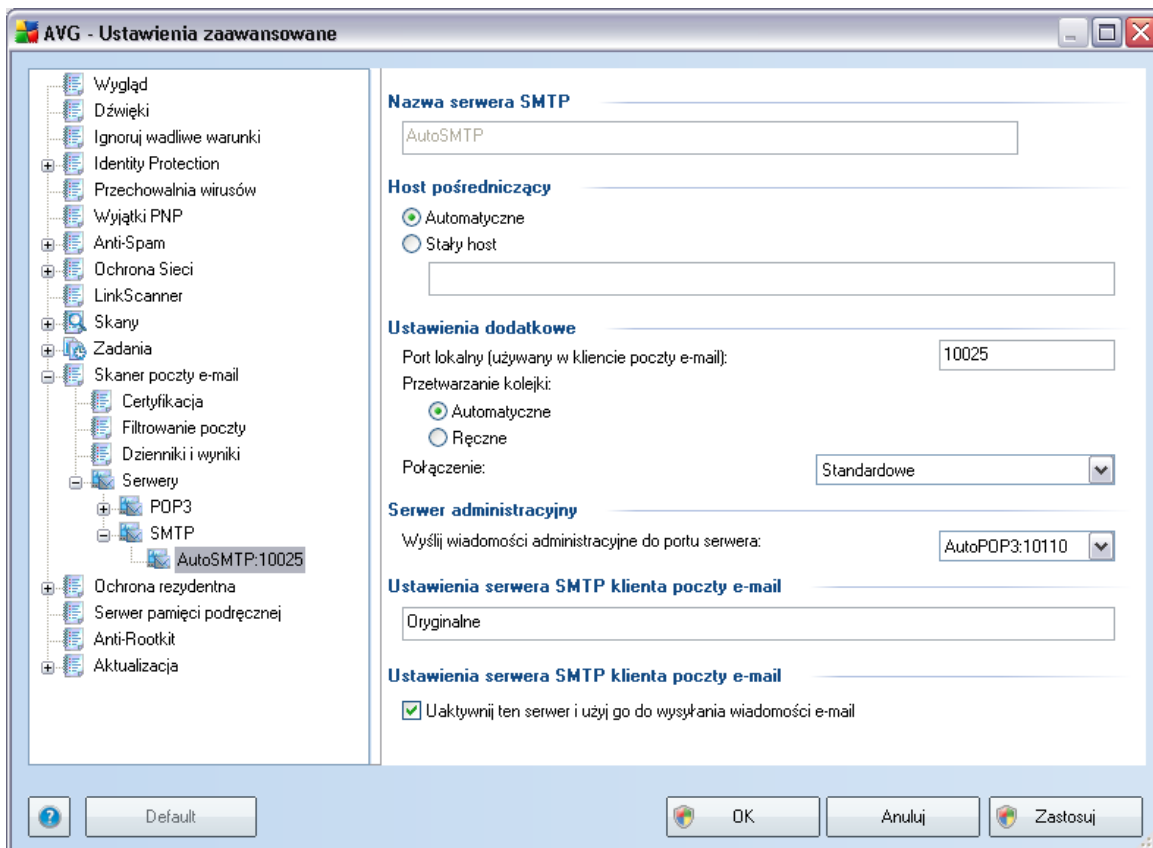
W tym oknie dialogowym (dostępnym z menu **Serwery / POP3**) można zdefiniować (na potrzeby [Skanera poczty e-mail](#)) nowy serwer poczty przychodzącej, korzystający z protokołu POP3:

- **Nazwa serwera POP3** — należy wpisać nazwę serwera lub zachować domyślną nazwę AutoPOP3.
- **Typ logowania** — definiuje metodę określania serwera pocztowego dla wiadomości przychodzących:
  - **Automatycznie** — logowanie jest przeprowadzane automatycznie

zgodnie z ustawieniami klienta poczty e-mail.

- **UZYTKOWNIK/KOMPUTER** — najprostsza i najczęściej używana metoda ustalania docelowego serwera pocztowego jest metoda proxy. Stosując te metody, jako część loginu użytkownika należy podać jego nazwę lub adres (lub także port), oddzielając ją znakiem /. Na przykład dla konta użytkownik1 na serwerze pop.domena.com z numerem portu 8200 należy stosować login użytkownik1/pop.domena.com:8200.
- **Staly host** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Login użytkownika pozostaje niezmienny. Jako nazwy można użyć nazwy domeny (na przykład pop.acme.com) lub adresu IP (na przykład 123.45.67.89). Jeśli serwer pocztowy używa niestandardowego portu, można określić go po dwukropku zaraz za nazwą serwera (na przykład pop.domena.com:8200). Standardowym portem protokołu POP3 jest 110.
- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
  - **Port lokalny** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.
  - **Użyj serwera APOP, jeśli jest dostępny** — opcja ta zapewnia bezpieczniejsze logowanie na serwerze pocztowym. Gwarantuje to, że [Skaner poczty e-mail](#) będzie używał alternatywnej metody przekazywania hasła użytkownika, polegającej na wysłaniu go w formie zaszyfrowanej, która korzysta ze zmiennego klucza nadesłanego przez serwer. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
  - **Polaczenie** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (zwykle/SSL/domyslnie SSL). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
- **Ustawienia serwera POP3 klienta poczty e-mail** — w tym obszarze znajdują się informacje dotyczące poprawnego skonfigurowania ustawień klienta poczty e-mail służących do sprawdzania poczty przychodzącej przez [Skaner poczty e-mail](#). Informacje te stanowią podsumowanie odpowiednich parametrów określonych w całej konfiguracji AVG.

- **Aktywacja serwera POP 3 klienta poczty e-mail** — opcje te należy zaznaczyć/odznaczyć, aby aktywować/wyłączyć określony serwer POP3.



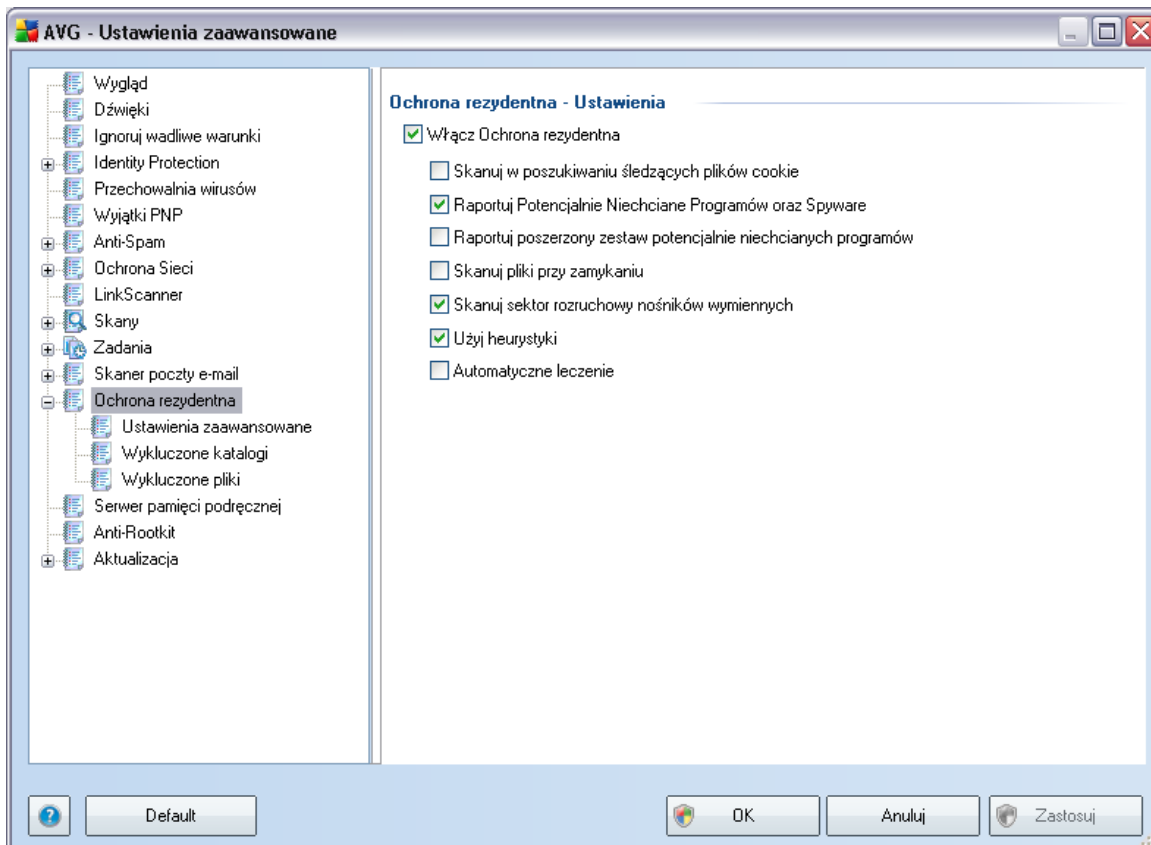
W tym oknie dialogowym (dostępnym z menu **Serwery / SMTP**) można zdefiniować (na potrzeby **Skamera poczty e-mail**) nowy serwer poczty przychodzącej, korzystający z protokołu SMTP:

- **Nazwa serwera SMTP** — należy wpisać nazwę serwera lub zachować domyślną nazwę AutoSMTP.
- **Host pośredniczący** — definiuje metodę określania serwera pocztowego dla wiadomości wychodzących:
  - **Automatyczne** — logowanie jest przeprowadzane automatycznie, zgodnie z ustawieniami klienta poczty e-mail

- **Staly host** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Jako nazwy można użyć domeny (na przykład smtp.domena.com) lub adresu IP (na przykład 123.45.67.89). Jeśli serwer pocztowy używa niestandardowego portu, można określić go po dwukropku zaraz za nazwą serwera (np. smtp.acme.com:8200). Standardowym portem protokołu SMTP jest port 25.
- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
  - **Port lokalny** — określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port komunikacji SMTP.
  - **Przetwarzanie kolejki** — określa zachowanie [skanera poczty e-mail](#) podczas przetwarzania wymagań dotyczących wysyłania wiadomości e-mail:
    - Automatycznie — poczta wychodząca jest natychmiast dostarczana (wysyłana) do docelowego serwera pocztowego.
    - Reczne — wiadomości są umieszczane w kolejce wiadomości wychodzących i wysyłane w późniejszym terminie.
  - **Polaczenie** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (zwykle/SSL/domyslnie SSL). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
- **Serwer administracyjny** — zawiera numer portu serwera używanego do zwrotnego dostarczania raportów administracyjnych. Takie wiadomości są generowane, kiedy np. serwer docelowy jest niedostępny lub odrzuca wiadomość wychodzącą.
- **W sekcji** Ustawienia serwera SMTP klienta poczty e-mail znajdują się zalecenia dotyczące takiej konfiguracji klienta poczty, która umożliwi wysyłanie wiadomości do aktualnie modyfikowanego serwera. Informacje te stanowią podsumowanie odpowiednich parametrów określonych w całej konfiguracji AVG.
- **Aktywacja serwera SMTP klienta poczty e-mail** — zaznacz lub usuń zaznaczenie tego pola, aby włączyć/wyłączyć określony powyżej serwer SMTP.

## 10.11. Ochrona rezydentna

Składnik **Ochrona Rezydentna** zapewnia aktywną ochronę plików i folderów przed wirusami, oprogramowaniem szpiegującym i innymi zagrożeniami.



W oknie **Ustawienia Ochrony rezydentnej** można całkowicie włączyć lub wyłączyć **Ochronę Rezydentną**, zaznaczając lub odznaczając pole **Włącz Ochronę Rezydentną** (opcja ta jest domyślnie włączona). Ponadto, można aktywować tylko wybrane funkcje **Ochrony Rezydentnej**:

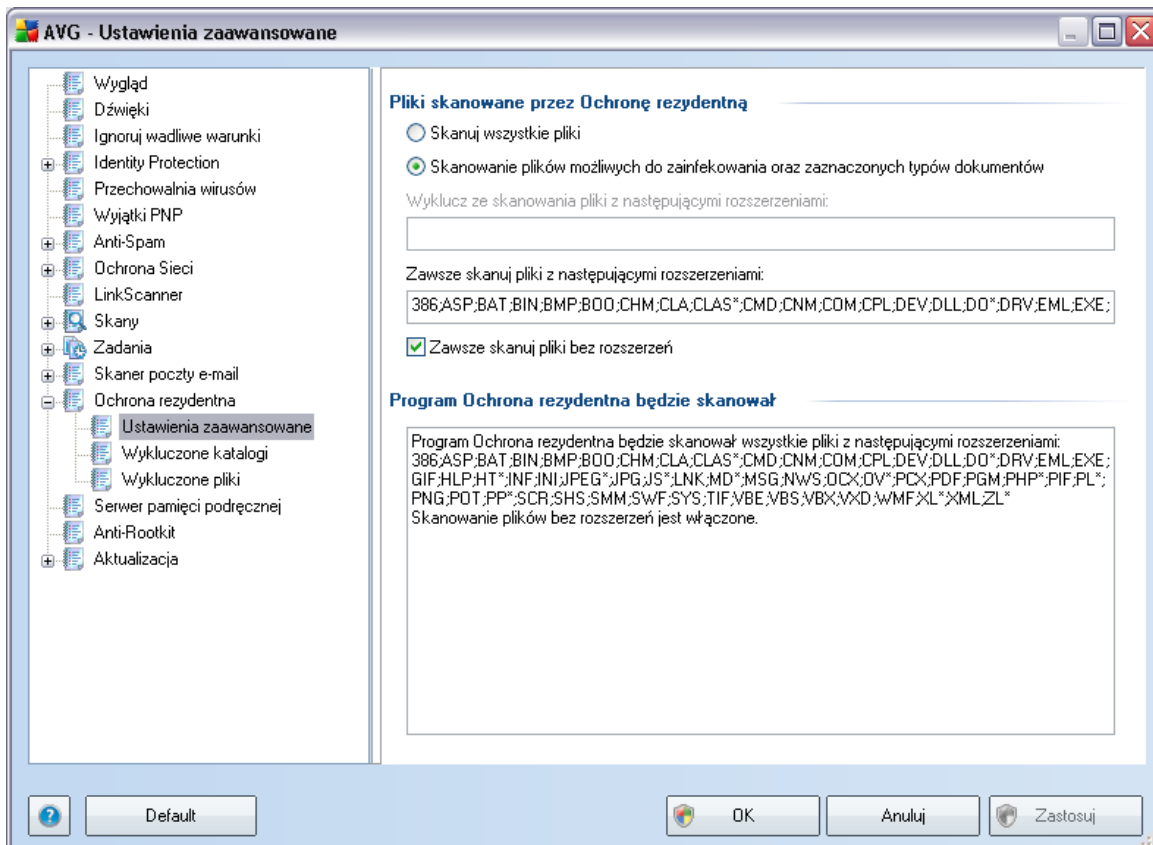
- **Skanuj w poszukiwaniu śledzących plików cookie** — parametr ten określa, czy w czasie skanowania mają być wykrywane pliki cookie. (Pliki cookie w protokole HTTP są używane do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach — np. preferencje dotyczące wyglądu witryny lub zawartość koszyka w sklepach internetowych.)
- **Raportuj zagrożenia potencjalnie niechcianymi programami i**

**oprogramowaniem szpiegującym** (opcja domyślnie włączona) — zaznaczenie tego pola powoduje włączenie silnika **Anti-Spyware** i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). [Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie.](#) Nie zaleca się wyłączenia tej opcji — znacząco zwiększa ona poziom ochrony komputera.

- **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości [oprogramowania szpiegującego](#), czyli programów, które są zupełnie bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.
- **Skanuj pliki przy zamykaniu** — oznacza, że system AVG skanuje aktywne obiekty (np. aplikacje, dokumenty itp.) nie tylko przy ich otwieraniu, ale także przy zamykaniu. Funkcja ta pomaga chronić komputer przed pewnymi typami bardziej skomplikowanych wirusów.
- **Skanuj sektor rozruchowy nośników wymiennych** — (domyślnie włączona)
- **Użyj heurystyki** — (domyślnie włączona) [do wykrywania będzie używana heurystyka](#) (dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej).
- **Automatyczne leczenie** — każda wykryta infekcja będzie automatycznie leczona (o ile jest to możliwe).

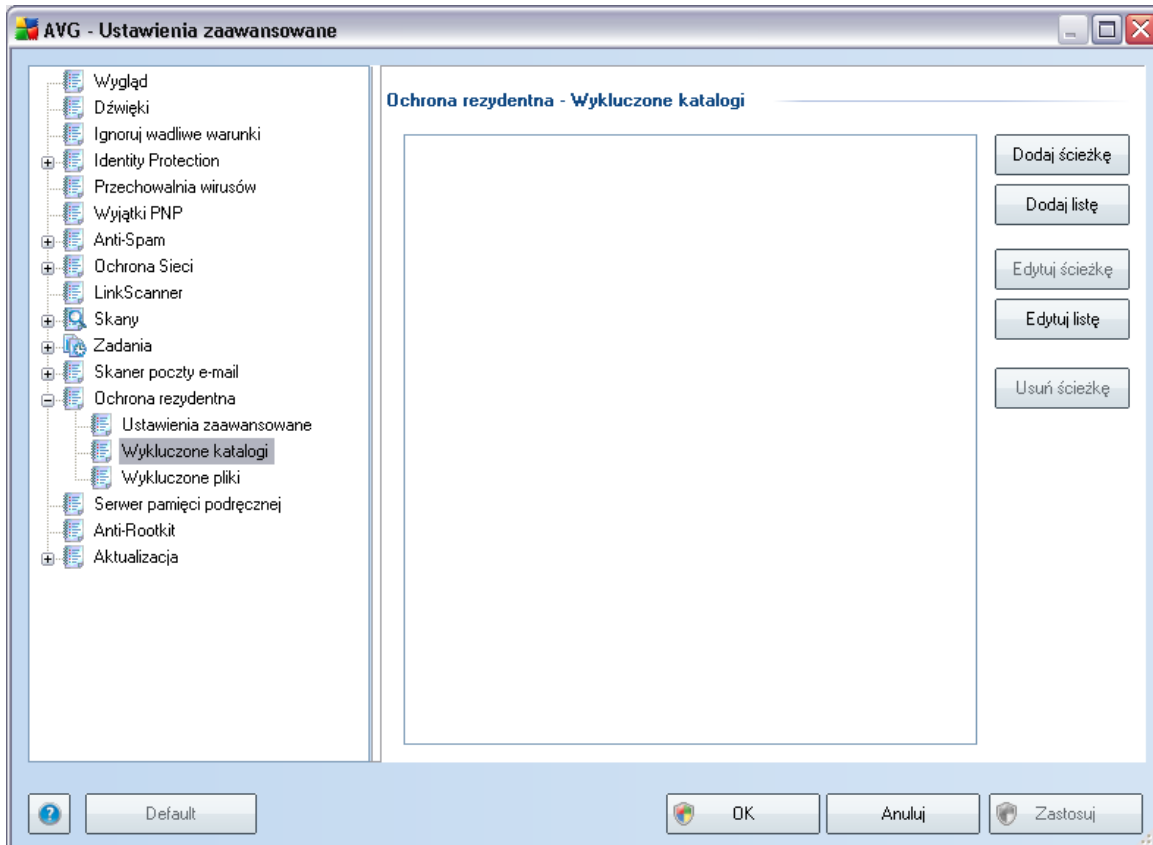
### 10.11.1. Ustawienia zaawansowane

W oknie **Pliki skanowane przez Ochronę Rezydentną** można określić, które pliki mają być skanowane (według ich rozszerzeń):



Zdecyduj, czy chcesz skanować tylko pliki infekowalne - jeśli tak, będziesz mógł określić listę rozszerzeń plików, które mają być wykluczone ze skanowania, oraz listę tych, które mają być zawsze skanowane.

### 10.11.2. Wykluczenia katalogów



Okno **Ochrona rezydentna – Wykluczone katalogi** pozwala definiować foldery, które mają być wykluczone ze skanowania przez **Ochronę Rezydentną**.

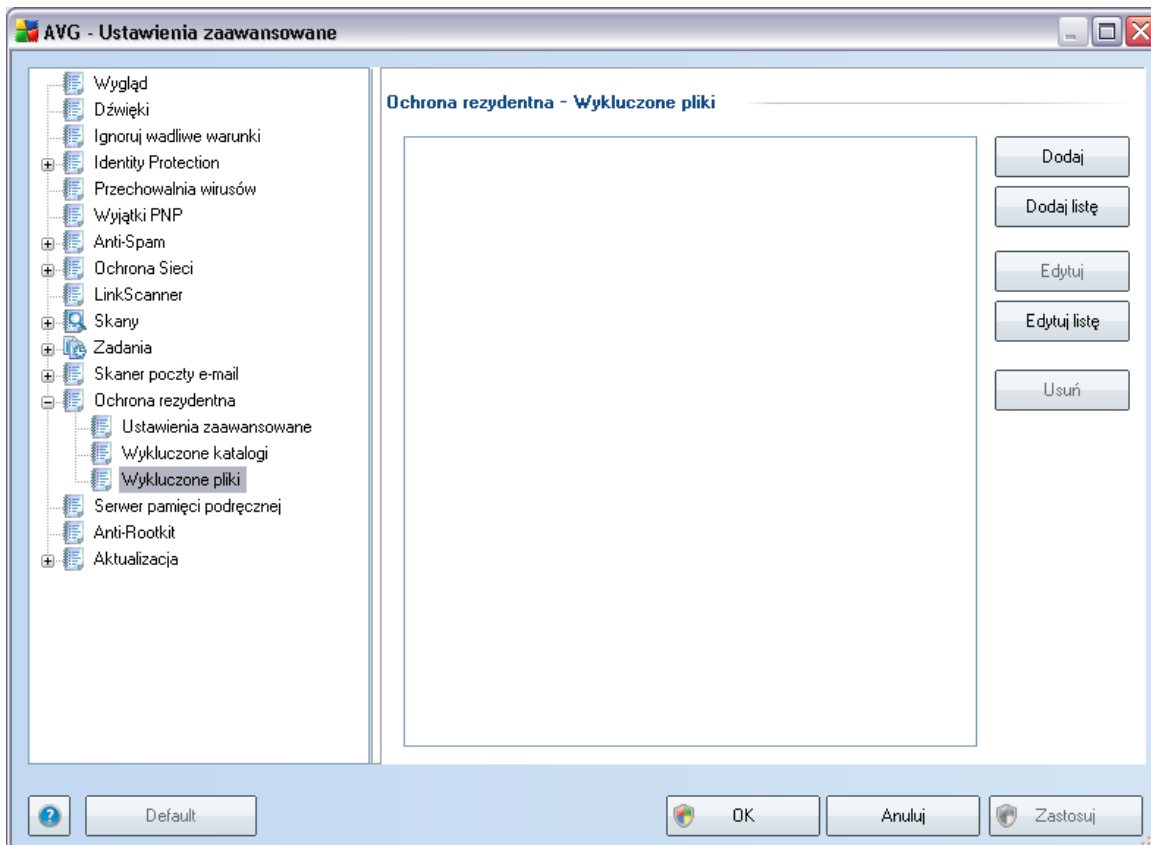
**Jesli nie jest to konieczne, zdecydowanie zalecamy nie wykluczać żadnych katalogów ze skanowania!**

W bieżącym oknie dostępne są następujące przyciski kontrolne:

- **Dodaj ścieżkę**— umożliwia określenie folderów, które mają zostać wykluczone ze skanowania, przez wybranie ich kolejno w drzewie obrazującym strukturę katalogów.
- **Dodaj listę**— umożliwia podanie listy katalogów, które zostaną wykluczone ze skanowania przez **Ochronę Rezydentną**.
- **Edytuj ścieżkę**— umożliwia edycję ścieżki do wybranego folderu.

- **Edytuj listę**— umożliwia edycje listy folderów.
- **Usuń ścieżkę**— umożliwia usunięcie z listy wybranego folderu.

### 10.11.3. Wykluczone pliki



Okno dialogowe **Ochrona rezydentna – wykluczone pliki** zachowuje się w taki sam sposób co poprzednio opisane okno **Ochrona rezydentna – wykluczone katalogi**, ale zamiast folderów można w nim określić pliki, które mają zostać wykluczone ze skanowania przez **Ochronę rezydentną**.

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

W bieżącym oknie dostępne są następujące przyciski kontrolne:

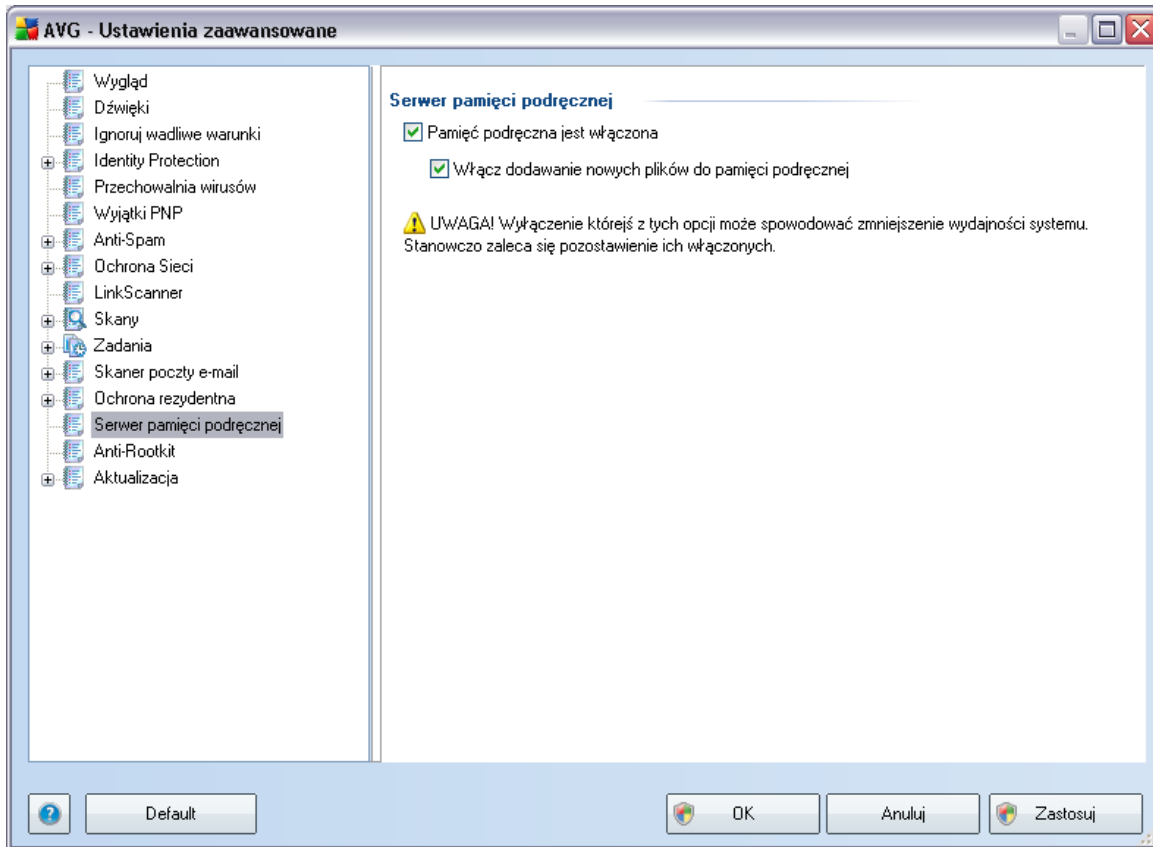
- **Dodaj**— umożliwia określenie katalogów, które mają zostać wykluczone ze

skanowania, przez wybranie ich kolejno w drzewie nawigacyjnym dysku lokalnego.

- **Dodaj liste**— umożliwia podanie listy plików, które zostaną wyłączone ze skanowania przez składnik [Ochrona rezydentna](#).
- **Edytuj** — umożliwia edycje określonej ścieżki dostępu do wybranego pliku.
- **Edytuj liste** — umożliwia edycje listy plików.
- **Usun**— umożliwia usunięcie z listy ścieżki dostępu do wybranego pliku.

### 10.12. Serwer pamięci podręcznej

Funkcja **Serwer pamięci podręcznej** to tak naprawdę proces mający na celu przyspieszenie skanowania (*skanowania na zadanie, zaplanowanego skanowania całego komputera, skanowania składnika [Ochrona rezydentna](#)*). Zbiera i przechowuje informacje na temat bezpiecznych plików (*takich jak pliki systemowe z podpisem cyfrowym itp.*) — pliki te są wówczas uważane za bezpieczne i pomijane podczas skanowania.

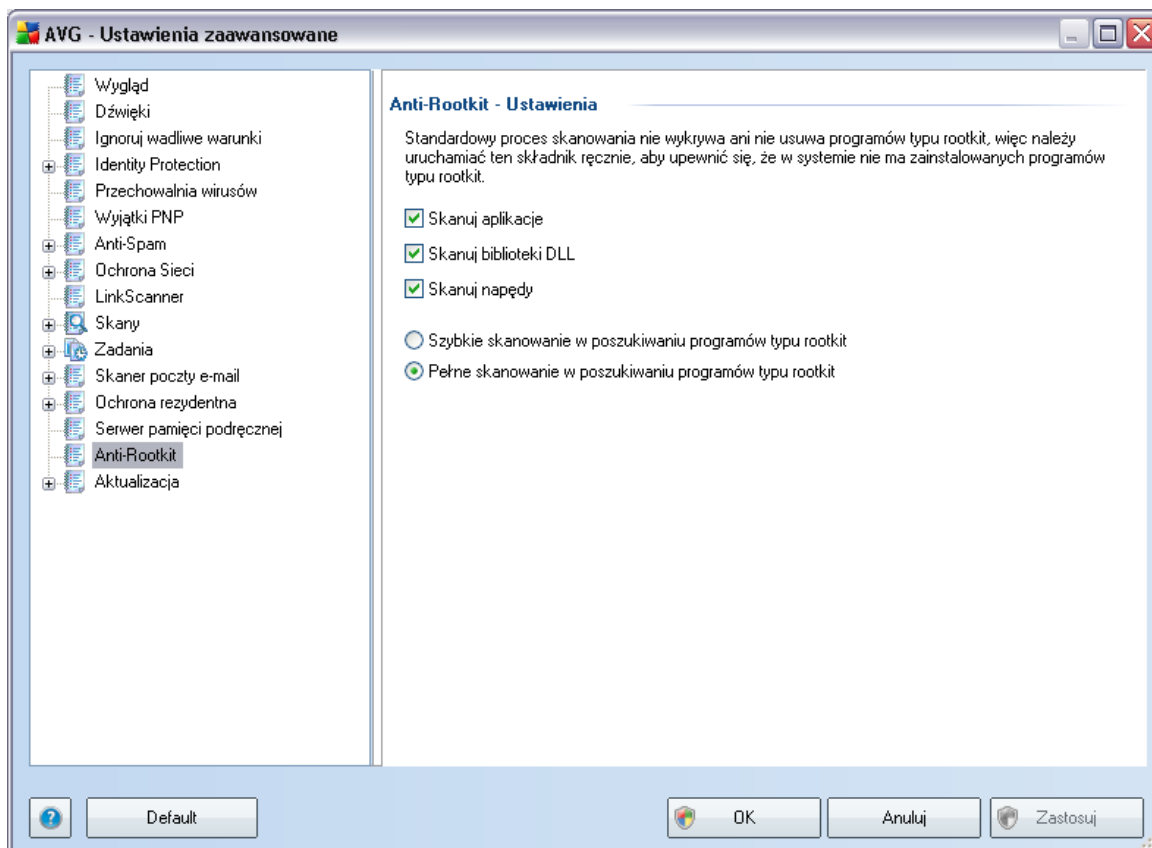


Okno dialogowe ustawien zawiera dwie opcje:

- **Włączona pamięć podręczna** (opcja domyślnie włączona) — usunięcie zaznaczenia tego pola powoduje wyłączenie funkcji **Serwer pamięci podręcznej** i opróżnienie pamięci podręcznej. Należy pamiętać, że skanowanie może spowodować działanie komputera i zmniejszyć jego ogólną wydajność, ponieważ każdy plik używany w danej chwili będzie skanowany w poszukiwaniu wirusów i oprogramowania szpiegującego.
- **Włącz dodawanie nowych plików do pamięci podręcznej** (opcja domyślnie włączona) — usunięcie zaznaczenia tego pola umożliwia wyłączenie funkcji dodawania kolejnych plików do pamięci podręcznej. Wszystkie pliki zapisane w pamięci podręcznej są w niej przechowywane dopóki funkcja nie zostanie zupełnie wyłączona lub do czasu kolejnej aktualizacji bazy danych wirusów.

## 10.13. Anti-Rootkit

W tym oknie dialogowym można edytować konfigurację składnika **Anti-Rootkit**:



Wszystkie funkcje składnika **Anti-Rootkit** dostępne w tym oknie dialogowym można także edytować bezpośrednio w **interfejsie składnika Anti-Rootkit**.

Zaznacz odpowiednie pola wyboru, aby określić obiekty, które mają być skanowane:

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

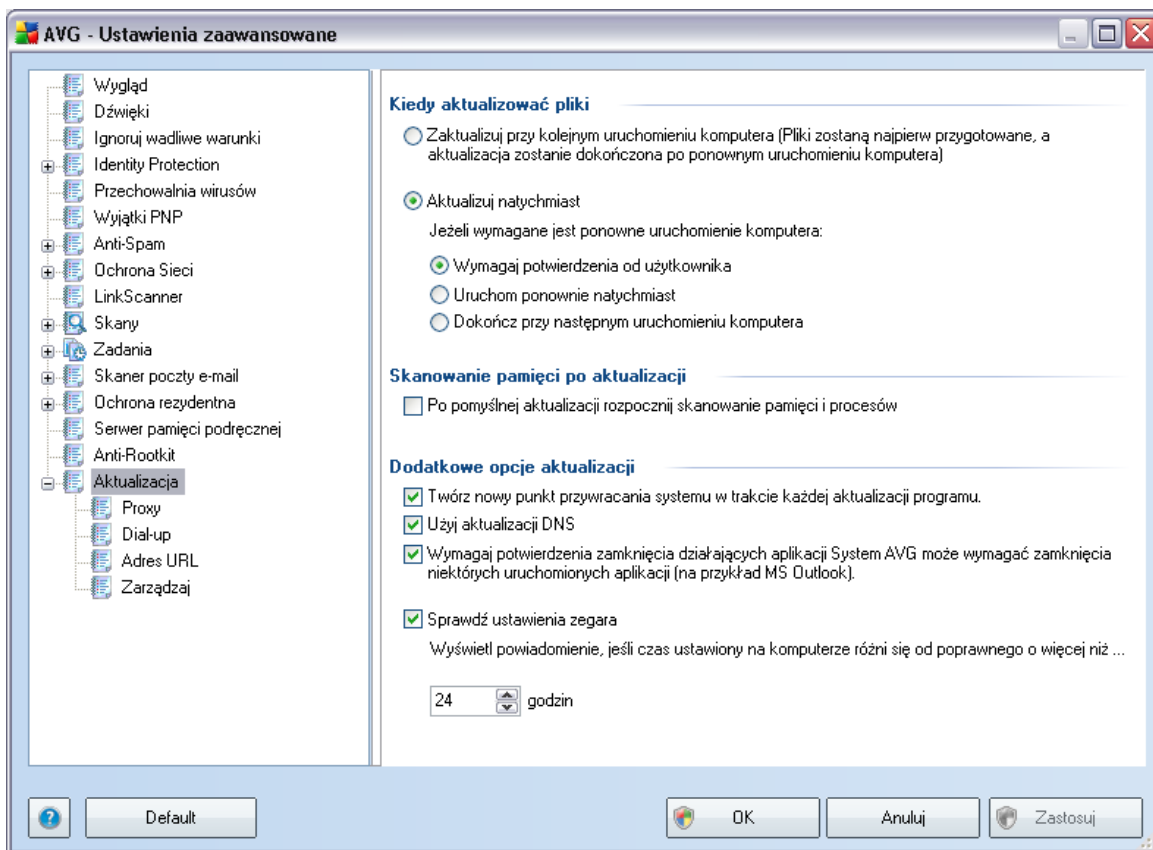
Następnie należy wybrać tryb skanowania w poszukiwaniu programów typu rootkit:

- **Szybkie skanowanie w poszukiwaniu programów typu rootkit** — skanuje

wszystkie uruchomione procesy, załadowane sterowniki i folder systemowy (zazwyczaj `c:\Windows`)

- **Pelne skanowanie w poszukiwaniu programów typu rootkit** — skanuje wszystkie uruchomione procesy, załadowane sterowniki i folder systemowy (zazwyczaj `c:\Windows`) oraz wszystkie dyski lokalne (w tym dyski flash, ale bez uwzględnienia napędów dyskietek/plyt CD)

## 10.14. Aktualizacja



Kliknięcie pozycji **Aktualizacja** otwiera nowe okno dialogowe, w którym można określić ogólne parametry [aktualizacji AVG](#):

### Kiedy aktualizować pliki

W tej sekcji można wybrać jedną z dwóch metod: zaplanowanie [aktualizacji](#) na

najbliższy restart komputera lub uruchomienie [aktualizacji](#) natychmiast. Domyślnie wybrana jest opcja natychmiastowa, ponieważ zapewnia ona maksymalny poziom bezpieczeństwa. Zaplanowanie aktualizacji na kolejne uruchomienie komputera zaleca się tylko w przypadku, gdy komputer jest regularnie restartowany (co najmniej raz dziennie).

Przy pozostawieniu konfiguracji domyślnej (natychmiastowe uruchomienie), można określić warunki ewentualnego restartu komputera:

- **Wymagaj potwierdzenia od użytkownika** — przed [zakonczeniem aktualizacji system zapyta użytkownika o pozwolenie na restart komputera](#).
- **Uruchom ponownie natychmiast** — komputer zostanie automatycznie zrestartowany zaraz po zakończeniu [procesu aktualizacji](#) — potwierdzenie ze strony użytkownika nie jest wymagane.
- **Dokończ przy następnym uruchomieniu komputera** — zakończenie [aktualizacji](#) zostanie odłożone do najbliższego restartu komputera. Należy pamiętać, że opcja ta jest zalecana tylko w przypadku, gdy komputer jest regularnie uruchamiany (co najmniej raz dziennie).

### **Skanowanie pamięci po aktualizacji**

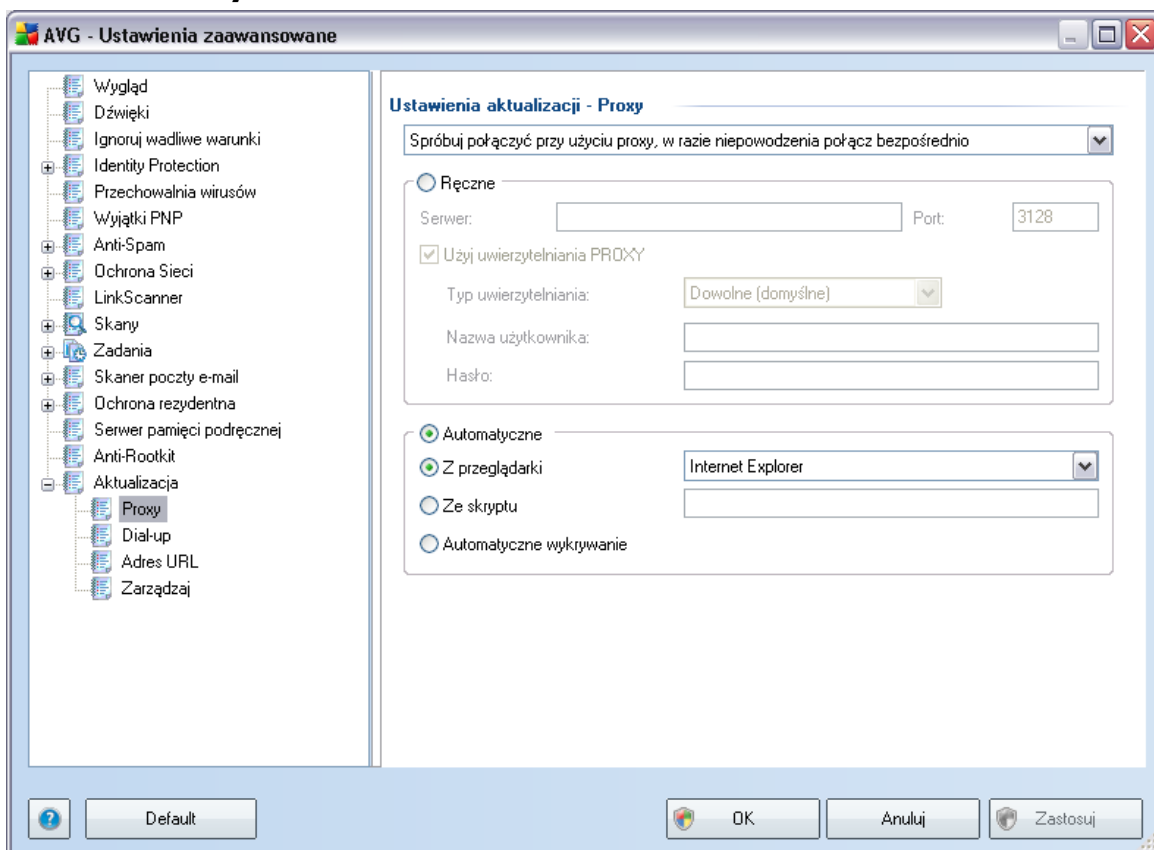
Pole to należy zaznaczyć, jeśli po każdej pomyslniej aktualizacji system ma uruchamiać skanowanie pamięci. Pobrana aktualizacja mogła zawierać nowe definicje wirusów, które mogą zostać zastosowane podczas takiego skanowania.

### **Dodatkowe opcje aktualizacji**

- **Twórz nowy punkt przywracania systemu po każdej aktualizacji programu** — przed każdym uruchomieniem aktualizacji systemu AVG tworzony będzie punkt przywracania systemu. Przy jego użyciu możliwe będzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Aby przywrócić system, należy wybrać kolejno: Start / Wszystkie programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoswiadczonym użytkownikom! Aby korzystać z tej funkcji, pole wyboru musi pozostać zaznaczone.
- **Użyj aktualizacji DNS** — zaznacz to pole, aby potwierdzić, że chcesz używać metody wykrywania nowych aktualizacji, która ogranicza ilość danych przesyłanych między serwerem aktualizacyjnym a klientem AVG.

- **Wymagaj potwierdzenia zamknięcia działających aplikacji** (domyślnie włączona) — daje pewność, że żadne działające aplikacje nie zostaną zamknięte bez potwierdzenia ze strony użytkownika, jeśli do zakończenia aktualizacji będzie wymagane ponowne uruchomienie komputera.
- **Sprawdź ustawienia zegara** — zaznacz to pole jeśli chcesz, aby program AVG wyświetlił powiadomienie, gdy różnica między właściwym a lokalnym czasem komputera przekroczy określona wartość.

### 10.14.1. Proxy



Serwer proxy jest samodzielnym serwerem lub uruchomiona na komputerze usługa gwarantująca bezpieczniejsze połączenie internetowe. Zgodnie z określonymi w Twojej sieci zasadami, połączenie internetowe może odbywać się bezpośrednio lub poprzez serwer proxy. Można także zezwolić na korzystanie z obu opcji jednocześnie. Dlatego też w oknie **Ustawienia aktualizacji – Proxy** należy najpierw wybrać jedną z dostępnych opcji:

- **Używaj proxy**
- **Nie używaj serwera proxy** — ustawienia domyślne
- **Spróbuj połączyć przy użyciu proxy, a w razie niepowodzenia połącz bezpośrednio**

W przypadku wybrania opcji użycia serwera proxy należy podać dalsze informacje. Ustawienia serwera mogą zostać skonfigurowane ręcznie lub automatycznie.

### Konfiguracja ręczna

W przypadku wybrania konfiguracji ręcznej (zaznaczenie opcji **Recznie** aktywuje odpowiednią sekcję) należy podać następujące informacje:

- **Serwer** — określ adres IP lub nazwę serwera
- **Port** — określ numer portu umożliwiającego dostęp do internetu (*domyślnie jest to port 3128, ale może być ustawiony inaczej; w przypadku wątpliwości należy skontaktować się z administratorem sieci*).

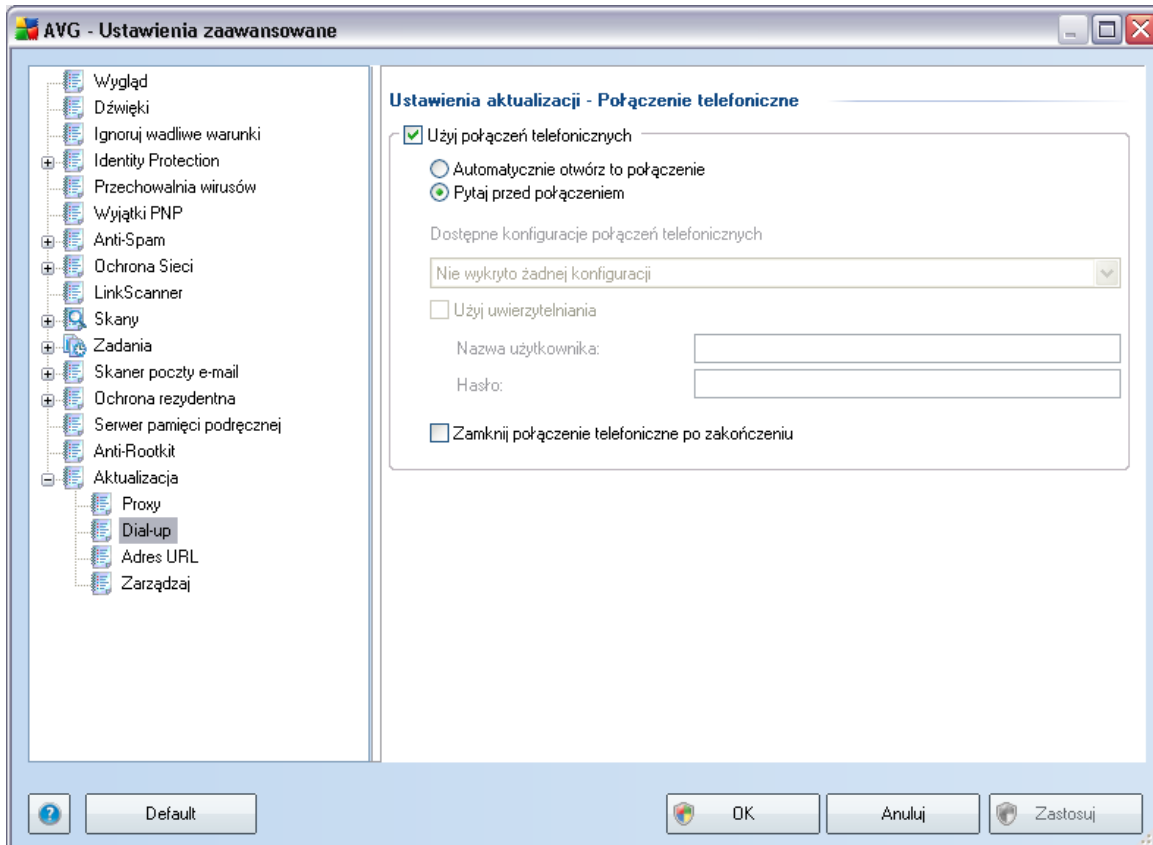
Zdarza się, że na serwerze proxy dla każdego użytkownika skonfigurowane są odrębne reguły. Jeśli serwer proxy jest skonfigurowany w ten sposób, należy zaznaczyć opcję **Użyj uwierzytelniania PROXY**, aby serwer weryfikował nazwę użytkownika i hasło przed nawiązaniem połączenia.

### Konfiguracja automatyczna

W przypadku wybrania konfiguracji automatycznej (zaznaczenie opcji **Automatycznie** aktywuje odpowiedni obszar okna dialogowego) należy wskazać, skąd ma zostać pobrana konfiguracja proxy:

- **Z przeglądarki** — konfiguracja zostanie odczytana z domyślnej przeglądarki internetowej.
- **Ze skryptu** — konfiguracja zostanie odczytana z pobranego skryptu zawierającego funkcje zwracające adres serwera proxy.
- **Automatyczne wykrywanie** — konfiguracja zostanie wykryta automatycznie bezpośrednio na serwerze proxy.

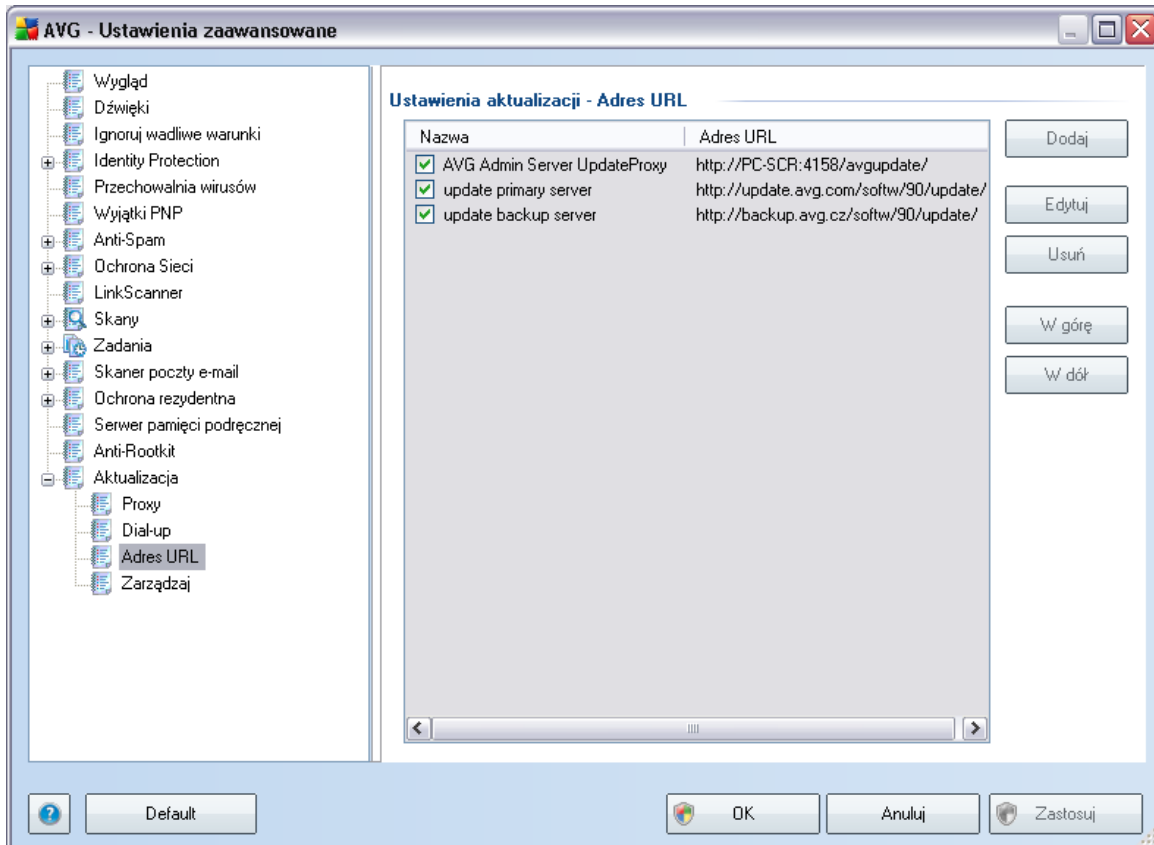
## 10.14.2. Połączenie telefoniczne



Wszystkie opcjonalne parametry podawane w oknie **Ustawienia aktualizacji – Połączenie telefoniczne** odnoszą się do połączenia dial-up z internetem. Pola tego okna pozostają nieaktywne aż do zaznaczenia opcji **Użyj połączeń telefonicznych**.

Należy określić, czy połączenie z internetem zostanie nawiązane automatycznie (**Automatycznie otwórz to połączenie**), czy też realizację połączenia należy zawsze potwierdzać ręcznie (**Pytaj przed połączeniem**). W przypadku łączenia automatycznego należy także określić, czy połączenie ma być zamykane natychmiast po zakończeniu aktualizacji (**Zamknij połączenie telefoniczne po zakończeniu**).

### 10.14.3. URL

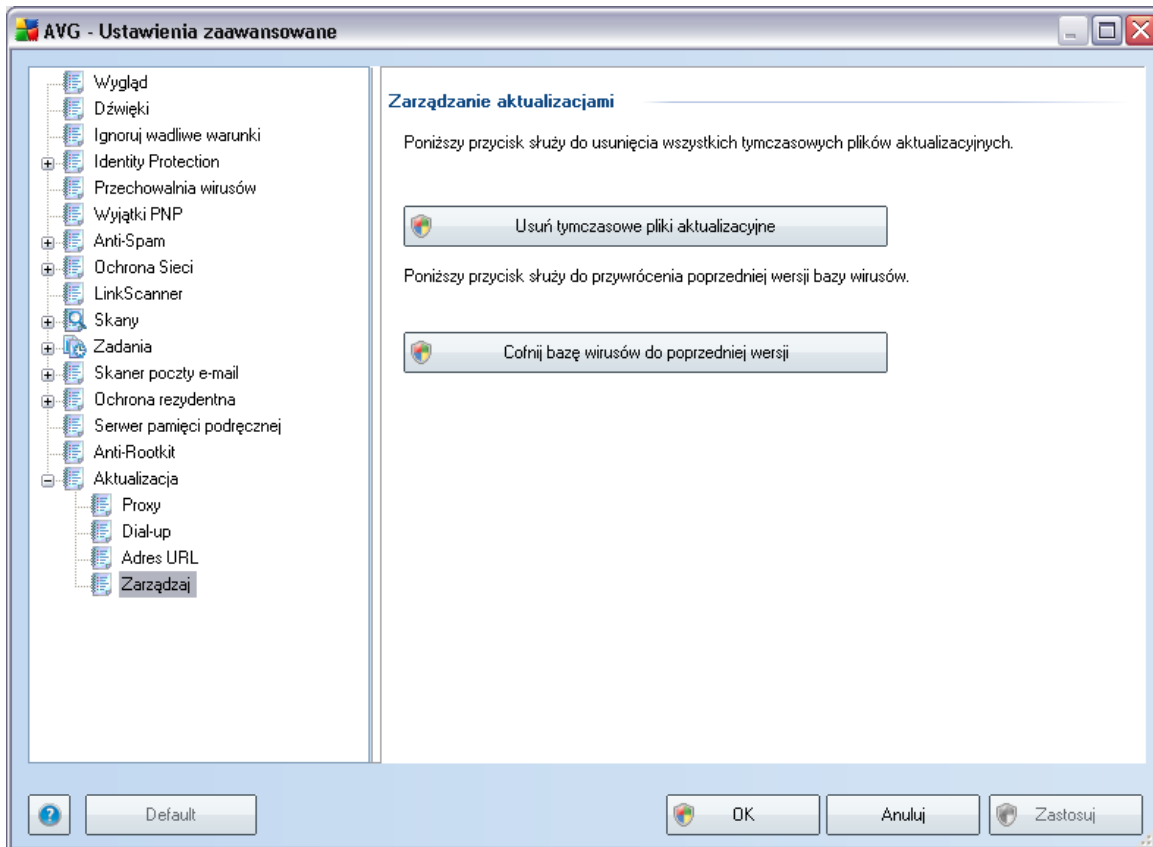


W oknie **URL** znajduje się lista adresów internetowych, z których można pobierać pliki aktualizacyjne. Listę i jej elementy można modyfikować za pomocą następujących przycisków kontrolnych:

- **Dodaj**— powoduje otwarcie okna dialogowego umożliwiającego określenie nowego adresu URL, który zostanie dodany do listy.
- **Edytuj** — powoduje otwarcie okna dialogowego umożliwiającego edycję parametrów wybranego adresu URL.
- **Usuń**— powoduje usunięcie wybranego adresu z listy.
- **W górę**— przenosi wybrany adres URL o jedną pozycję w górę.
- **W dół** — przenosi wybrany adres URL o jedną pozycję w dół.

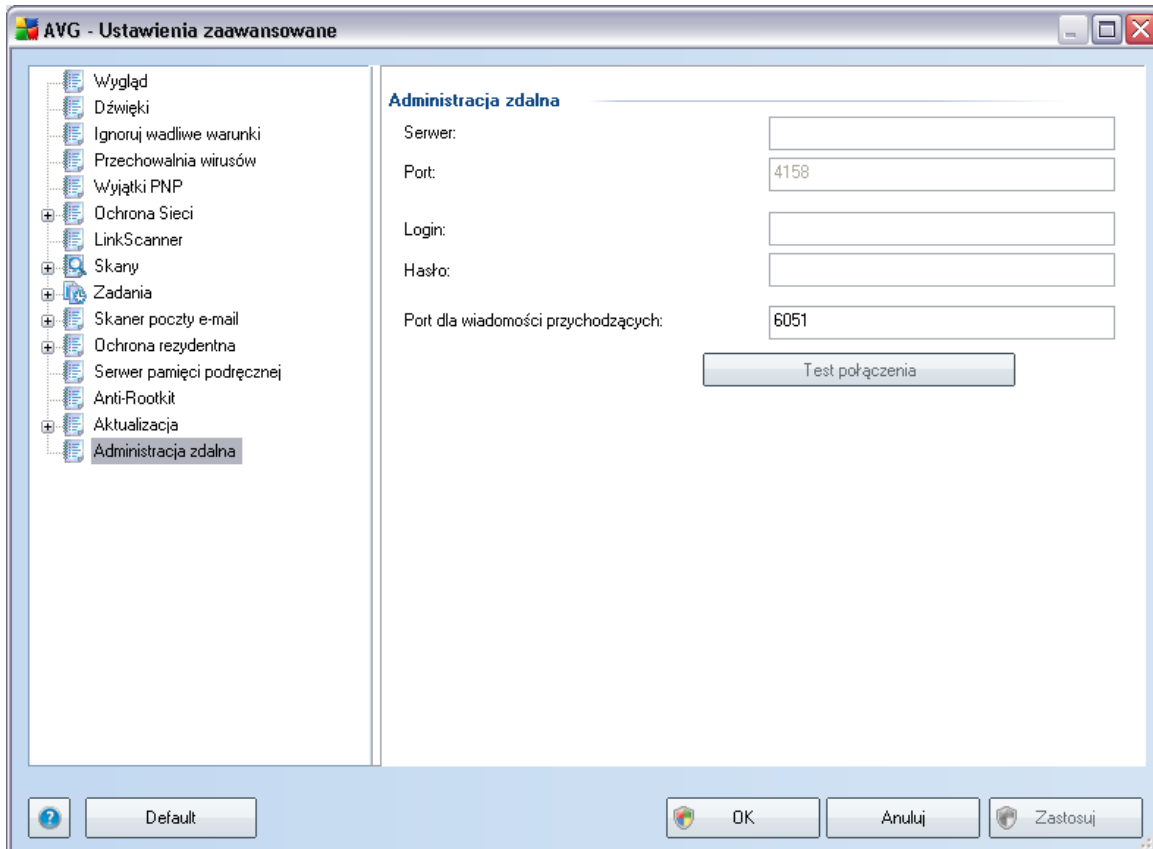
#### 10.14.4. Zarządzaj

Okno dialogowe **Zarządzaj** zawiera dwa przyciski:



- **Usun tymczasowe pliki aktualizacyjne** — pozwala usunac z dysku twardego wszystkie zbędne pliki aktualizacyjne (sa one domyślnie przechowywane przez 30 dni)
- **Cofnij baze wirusów do poprzedniej wersji** — pozwala usunac z dysku twardego ostatnia wersje bazy wirusów i przywrócić ja do poprzedniego stanu (nowa baza bedzie czescia najbliższej aktualizacji)

## 10.15. Administracja zdalna



Ustawienia **Administracji zdalnej** określają sposób łączenia się stacji roboczej AVG z systemem administracji zdalnej. Jeśli dana stacja ma łączyć się ze zdalnym serwerem administracyjnym, należy określić następujące parametry:

- **Serwer** — nazwa (lub adres IP) serwera, na którym zainstalowano oprogramowanie AVG Admin Server.
- **Port** — numer portu, przez który klient AVG komunikuje się z serwerem AVG Admin Server (za domyślny uważany jest port 4158 — jeśli ma być używany, nie trzeba go wprowadzać).
- **Nazwa logowania** — jeśli używana jest opcja bezpiecznej komunikacji między klientem AVG i oprogramowaniem AVG Admin Server, należy podać nazwę użytkownika ...



- **Hasło** — wymagane, jeśli podano login.
- **Port dla wiadomości przychodzących** — numer portu, na którym klient AVG odbiera wiadomości od serwera AVG Admin Server.

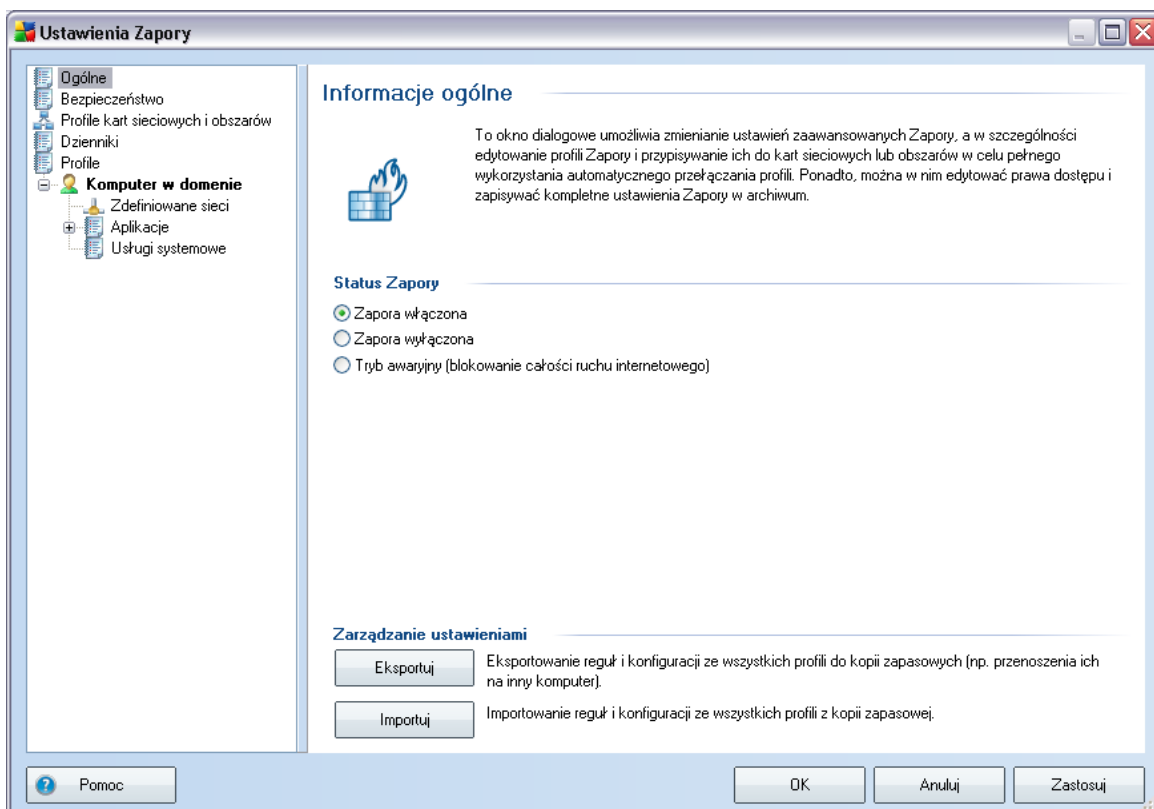
Przycisk **Testuj połączenie** pozwala sprawdzić, czy wszystkie powyższe dane są prawidłowe i zapewnia pomyślne połączenie z bazą danych DataCenter.

**Uwaga:** Szczegółowy opis funkcji administracji zdalnej zawiera dokumentacja programu *AVG Network Edition*.

## 11. Ustawienia Zapory

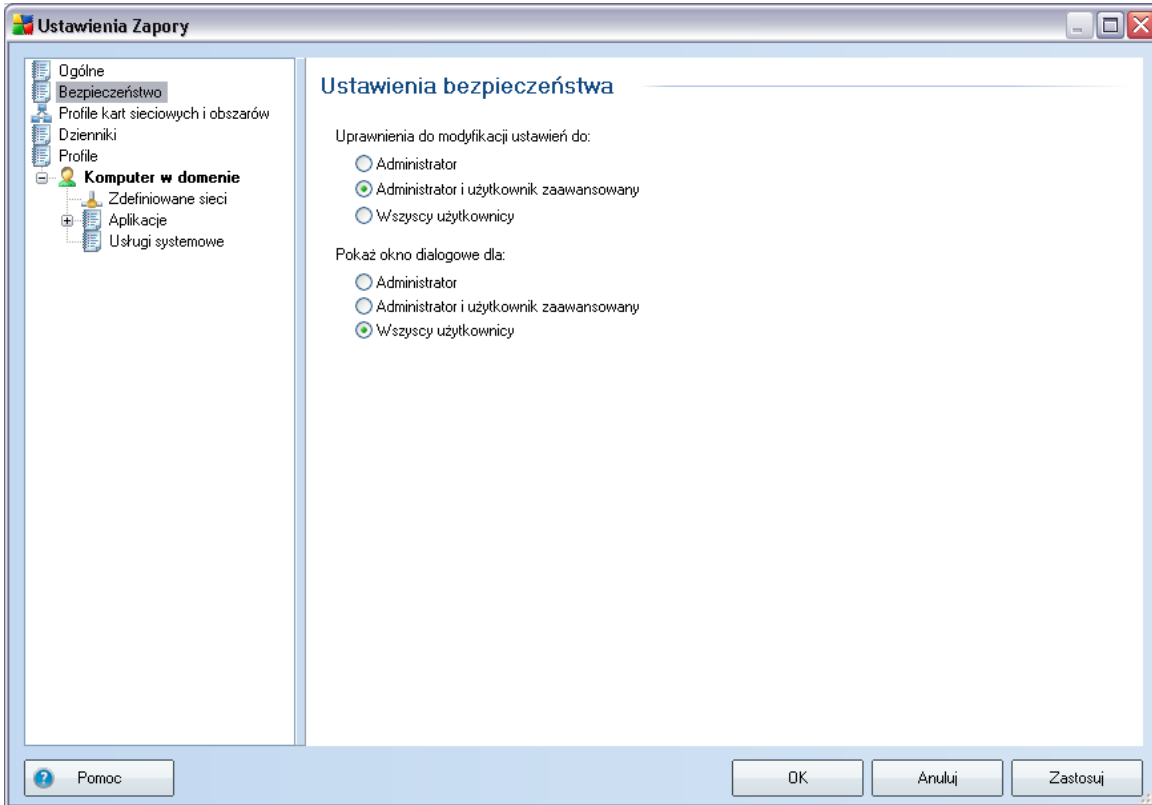
Konfiguracja **Zapory** otwierana jest w nowym oknie, gdzie w kilku sekcjach można określić nawet najbardziej zaawansowane parametry tego składnika. **Jednakże edycja zaawansowanej konfiguracji powinna być dokonywana jedynie przez ekspertów i doświadczonych użytkowników.**

### 11.1. Ogólne



W oknie **Informacje ogólne** można **wyeksportować / zaimportować konfigurację** Zapory, tzn. wyeksportować zdefiniowane reguły i ustawienia **Zapory** do pliku kopii zapasowej lub też zaimportować do programu cały plik tego typu.

## 11.2. Bezpieczeństwo



W oknie **Ustawienia bezpieczeństwa** można zdefiniować ogólne reguły zachowania **Zapory** niezależnie od wybranego profilu:

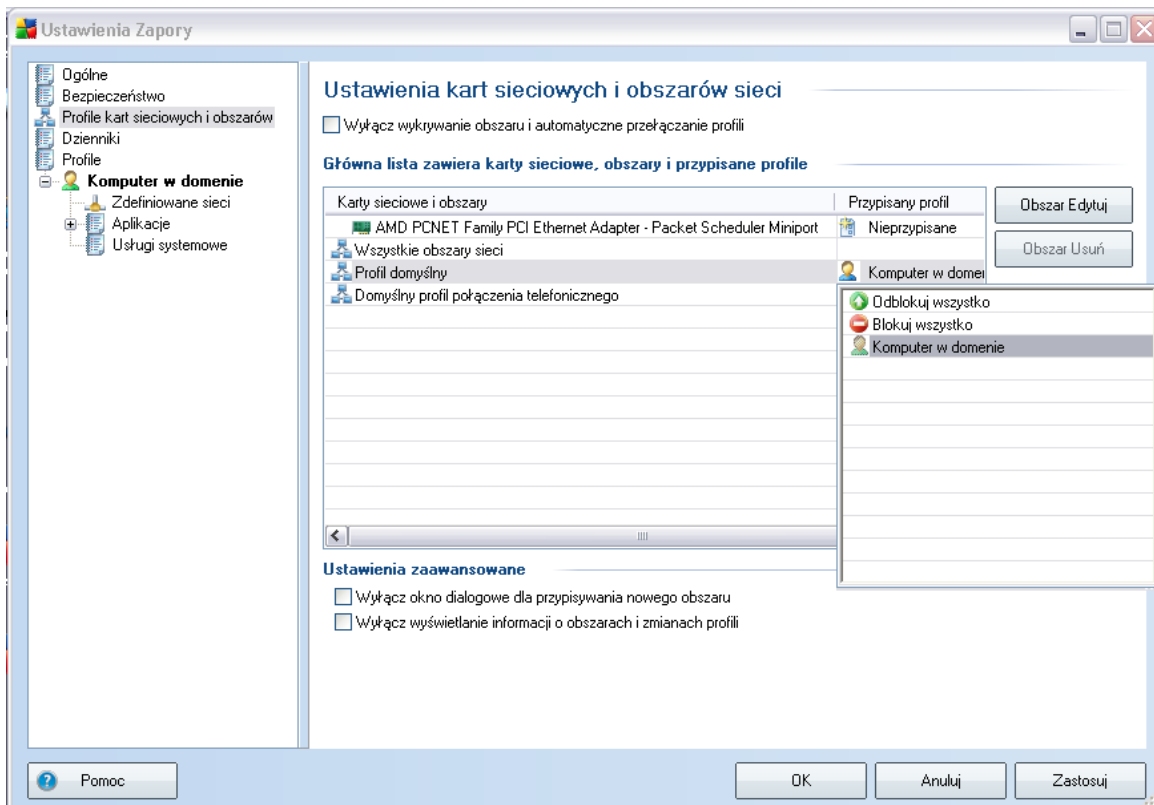
- **Pozwól modyfikować ustawienia:** — należy określić, kto może zmieniać konfigurację składnika **Zapora**.
- **Pokaż okno dialogowe:** — należy określić, komu można wyświetlać okna potwierdzeń Zapory (*okna dialogowe z prośbą o podjęcie decyzji w sytuacji nieobjętej żadną regułą Zapory*).

W obu wypadkach można przypisać konkretne uprawnienie jednej z następujących grup użytkowników:

- **Administratorom** — posiadają oni całkowitą kontrolę nad komputerem i możliwość przydzielania użytkownikom do grup z określonymi uprawnieniami.

- o **Administratorom i użytkownikom uprzywilejowanym** — administrator może przydzielić dowolnego użytkownika do uprzywilejowanej grupy (*Użytkownicy uprzywilejowani*) oraz określić uprawnienia jej członków.
- o **Wszyscy użytkownicy** — pozostali użytkownicy (nie przydzieleni do żadnej konkretnej grupy).

### 11.3. Profile kart sieciowych i obszarów



W oknie **Ustawienia kart sieciowych i obszarów** można edytować ustawienia związane z przypisywaniem zdefiniowanych profili do konkretnych kart i sieci:

- **Wyłącz wykrywanie obszaru i automatyczne przełączanie profili** — do każdego typu interfejsu sieciowego można przypisać jeden ze zdefiniowanych profili (odpowiednio dla poszczególnych obszarów). Jeśli nie chcesz tworzyć własnych, konkretnych profili, używany będzie jeden wspólny profil zdefiniowany na podstawie [typu komputera](#) i [sposobu połączenia z internetem](#) określonych podczas [procesu instalacji](#). Jeśli jednak postanowisz zróżnicować



portów itp.) na dwóch następujących kartach:

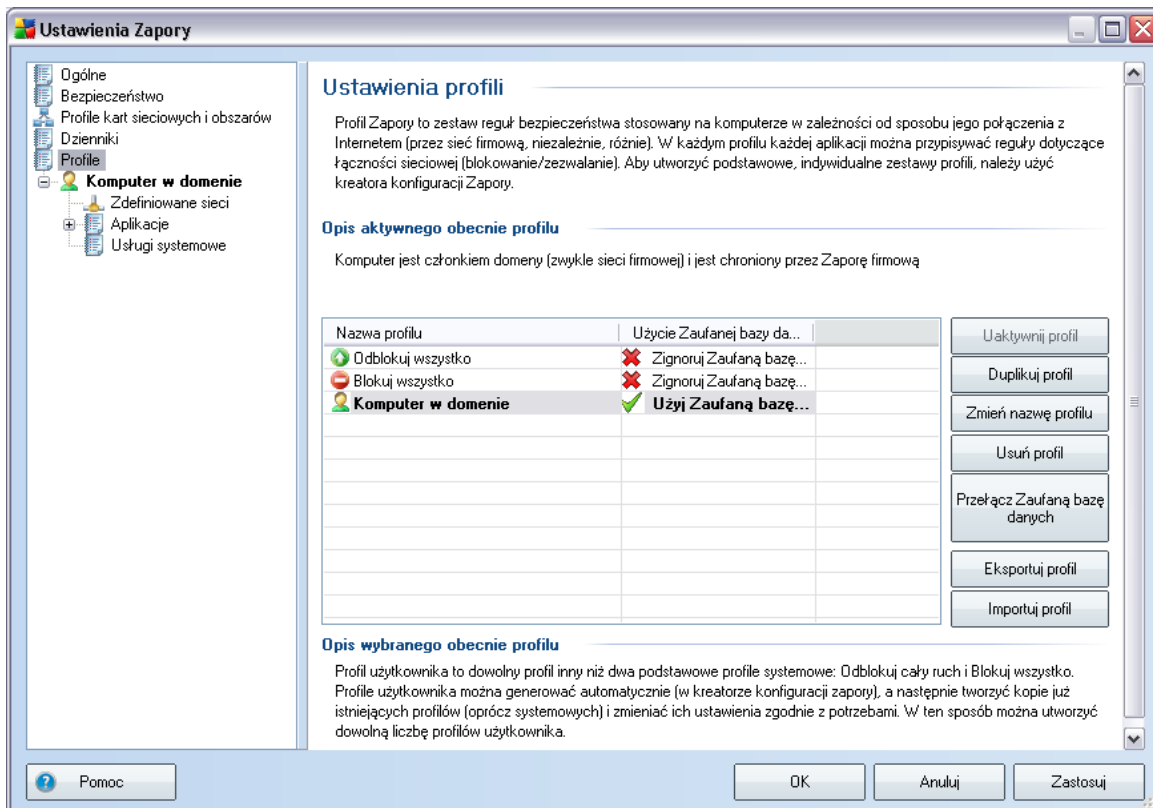
- **Dzienniki sieciowe** — zawiera informacje o aktywności wszystkich aplikacji, które próbowały połączyć się z siecią.
- **Dzienniki Trusted Database** — *Trusted Database* to wewnętrzna baza danych systemu AVG zbierająca informacje na temat certyfikowanych i zaufanych aplikacji, dla których komunikacja w trybie online jest zawsze dozwolona. Za pierwszym razem, kiedy nowa aplikacja próbuje się połączyć z siecią (np. gdy jeszcze nie została utworzona reguła zapory dla tej aplikacji), konieczna jest decyzja, czy zezwolic na komunikację sieciową. Najpierw system AVG przeszukuje bazę *Trusted Database*. Jeśli aplikacja znajduje się na liście, dostęp do sieci zostanie jej automatycznie umożliwiony. Dopiero wtedy, gdy w naszej bazie danych nie ma żadnych informacji na temat tej aplikacji, zostanie wyświetlone oddzielne okno dialogowe z pytaniem, czy dostęp do sieci powinien zostać odblokowany.

### Przyciski kontrolne

- **Pomoc** — otwiera okno dialogowe z powiązаныmi tematami pomocy.
- **Odśwież listę** — wszystkie zarejestrowane parametry można uporządkować według wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) — wystarczy kliknąć odpowiedni nagłówek kolumny. Użyj przycisku **Odśwież listę**, aby zaktualizować wyświetlane informacje.
- **Opróżnij listę** — pozwala usunąć wszystkie wpisy.

## 11.5. Profile

W oknie **Ustawienia profili** można znaleźć listę dostępnych profili.



Wszystkie [profile](#) (prócz systemowych) mogą być edytowane w tym oknie dialogowym przy użyciu następujących przycisków kontrolnych:

- **Uaktywnij profil** — przycisk ten ustawia wybrany profil jako aktywny, co oznacza, że konfiguracja wybranego profilu będzie używana przez **Zapórę** do sterowania ruchem w sieci.
- **Duplikuj profil** — tworzy kopie wybranego profilu. Później będzie można przeprowadzić edycję i zmienić nazwę kopii, aby utworzyć nowy profil na podstawie istniejącego.
- **Zmień nazwę profilu** — umożliwi zdefiniowanie nowej nazwy dla wybranego profilu.

- **Usun profil** — usuwa wybrany profil z listy.
- **Wlacz/wylacz Trusted Database** — umożliwia danemu profilowi korzystanie z bazy *Trusted Database* (*Trusted Database to wewnętrzna baza danych AVG, zbierająca informacje na temat certyfikowanych i zaufanych aplikacji, którym bez obaw można zezwolić na połączenie z internetem.*)
- **Eksportuj profil** — zapisuje konfigurację wybranego profilu w pliku, którego będzie można użyć w przyszłości.
- **Importuj profil** — konfiguruje ustawienia wybranego profilu na podstawie danych zapisanych w pliku konfiguracyjnym.
- **Pomoc** — otwiera okno dialogowe z powiązaniem tematem pomocy.

W dolnej części okna dialogowego można znaleźć opis profilu wybranego z powyższej listy.

Menu nawigacyjne znajdujące się po lewej stronie zmienia odzwierciedla listę profili wyświetloną w oknie **Profile**. Każdy zdefiniowany profil tworzy jedną gałąź należącą do grupy **Profile**. Konkretny profil można edytować w kolejnych oknach dialogowych (*identycznych dla wszystkich profili*):

### 11.5.1. Informacje o profilu



Okno dialogowe **Informacje o profilu** to pierwsze z okien sekcji, w której można edytować konfigurację wybranego profilu w osobnych oknach dialogowych dotyczących jego określonych parametrów.

- **Dla tego profilu użyj bazy Trusted Database** (*opcja domyślnie włączona*) — te opcje należy zaznaczyć, aby aktywować bazę *Trusted Database* (czyli *wewnętrzna baza danych systemu AVG zbierająca informacje o zaufanych i certyfikowanych aplikacjach korzystających z komunikacji online. Jeśli dla danej aplikacji nie ma jeszcze określonych reguł, konieczne jest sprawdzenie, czy aplikacja może uzyskać dostęp do sieci. System AVG przeszukuje najpierw bazę Trusted Database i jeżeli dana aplikacja jest na liście, zostanie uznana za bezpieczna i będzie jej umożliwiona komunikacja poprzez sieć. W innym przypadku zostanie wyświetlone zapytanie, czy komunikacja przez sieć dla danej aplikacji powinna zostać odblokowana*) dla określonego profilu.
- **Wlacz obsługę sieci maszyn wirtualnych** (*domyślnie wylaczone*) — zaznaczenie tej pozycji pozwala maszynom wirtualnym VMware łączyć się

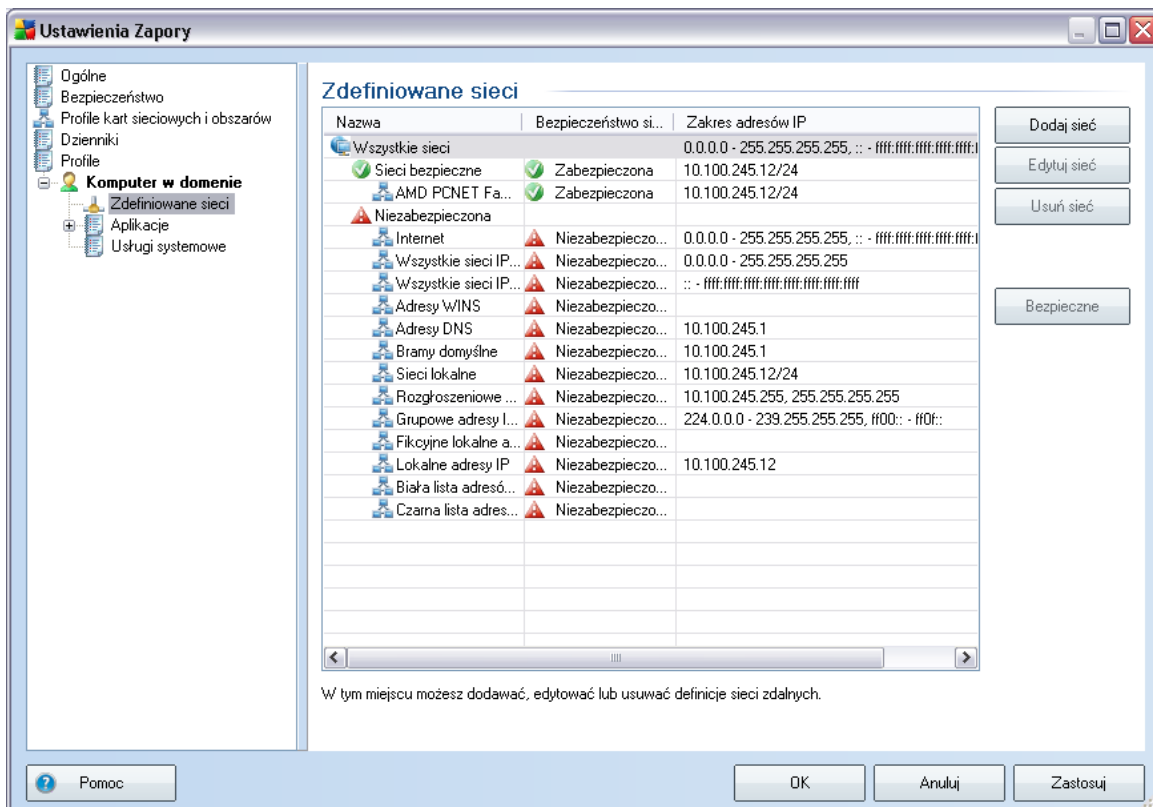
bezpośrednio z sieciami.

## Ustawienia trybu gry

W sekcji **Ustawienia trybu gry** można określić czy komunikaty **Zapory** mają być wyświetlane nawet podczas działania aplikacji pełnoekranowych (*sa to na ogół gry, ale dotyczy to również wszelkich innych aplikacji, takich jak np. prezentacje PPT*). Komunikaty informacyjne mogą być w pewnym stopniu irytujące.

Jeśli zostanie zaznaczona opcja **Wylacz powiadomienia Zapory w czasie gry**, z menu rozwijanego znajdującego się poniżej należy wybrać akcję, która ma podjąć Zaporę, gdy nowa aplikacja spróbuje nawiązać połączenie z siecią (*aby nie wyświetlać komunikatu z pytaniem o dostęp*). Wszystkie takie aplikacje mogą być odblokowane lub zablokowane.

### 11.5.2. Zdefiniowane sieci



The screenshot shows the 'Ustawienia Zapory' (Firewall Settings) window. The left sidebar shows a tree view with 'Zdefiniowane sieci' (Defined Networks) selected. The main area displays a table of defined networks with columns for 'Nazwa' (Name), 'Bezpieczeństwo sieci' (Network Security), and 'Zakres adresów IP' (IP Address Range). Buttons for 'Dodaj sieć' (Add network), 'Edytuj sieć' (Edit network), and 'Usuń sieć' (Remove network) are visible on the right. A 'Bezpieczne' (Safe) button is also present. At the bottom, there are 'Pomoc' (Help), 'OK', 'Anuluj' (Cancel), and 'Zastosuj' (Apply) buttons.

Nazwa	Bezpieczeństwo sieci	Zakres adresów IP
Wszystkie sieci	Zabezpieczona	0.0.0.0 - 255.255.255.255, :: - ffff:ffff:ffff:ffff
Sieci bezpieczne	Zabezpieczona	10.100.245.12/24
AMD PCNET Fa...	Zabezpieczona	10.100.245.12/24
Niezabezpieczona	Niezabezpieczona	
Internet	Niezabezpieczona	0.0.0.0 - 255.255.255.255, :: - ffff:ffff:ffff:ffff
Wszystkie sieci IP...	Niezabezpieczona	0.0.0.0 - 255.255.255.255
Wszystkie sieci IP...	Niezabezpieczona	:: - ffff:ffff:ffff:ffff:ffff:ffff
Adresy WINS	Niezabezpieczona	
Adresy DNS	Niezabezpieczona	10.100.245.1
Bramy domyślne	Niezabezpieczona	10.100.245.1
Sieci lokalne	Niezabezpieczona	10.100.245.12/24
Rozgłoszeniowe ...	Niezabezpieczona	10.100.245.255, 255.255.255.255
Grupowe adresy I...	Niezabezpieczona	224.0.0.0 - 239.255.255.255, ff00:: - ffff::
Fikcyjne lokalne a...	Niezabezpieczona	
Lokalne adresy IP	Niezabezpieczona	10.100.245.12
Biała lista adresó...	Niezabezpieczona	
Czarna lista adres...	Niezabezpieczona	

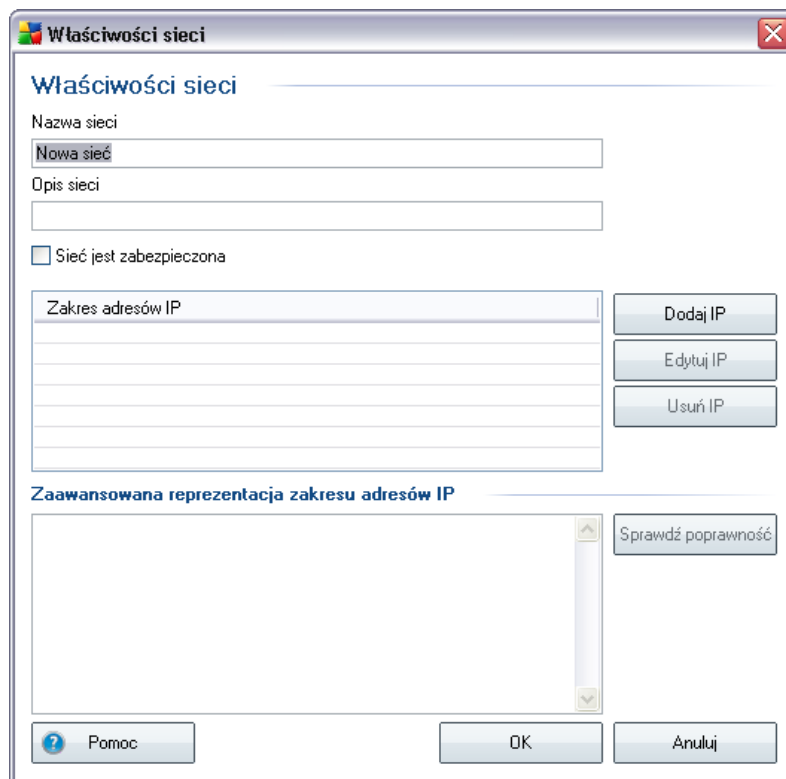
W tym miejscu możesz dodawać, edytować lub usuwać definicje sieci zdalnych.

Okno dialogowe **Zdefiniowane sieci** zawiera listę wszystkich sieci, z którymi połączony jest Twój komputer. Dla każdej wykrytej sieci wyświetlane są następujące informacje:

- **Sieci** — lista nazw wszystkich sieci, do których podłączony jest komputer.
- **Bezpieczeństwo sieci** — domyślnie wszystkie sieci uważane są za niebezpieczne i tylko w przypadku pewności, że dana sieć (i odpowiednia karta sieciowa) jest godna zaufania, można przypisać jej takie ustawienie (w tym celu należy kliknąć na liście pozycję odpowiadającą tej sieci i wybrać z menu kontekstowego opcję *Bezpieczna*). Wszystkie bezpieczne karty sieciowe i odpowiadające im sieci zostaną wzięte pod uwagę przy przyznawaniu dostępu aplikacjom, dla których zastosowano reguły Odblokuj bezpieczne
- **Zakres adresów IP** — każda sieć zostanie automatycznie wykryta i określona w formie zakresu adresów IP

### Przyciski kontrolne

- **Dodaj sieć** — otwiera okno dialogowe **Właściwości sieci**, w którym można edytować parametry nowo zdefiniowanej sieci:



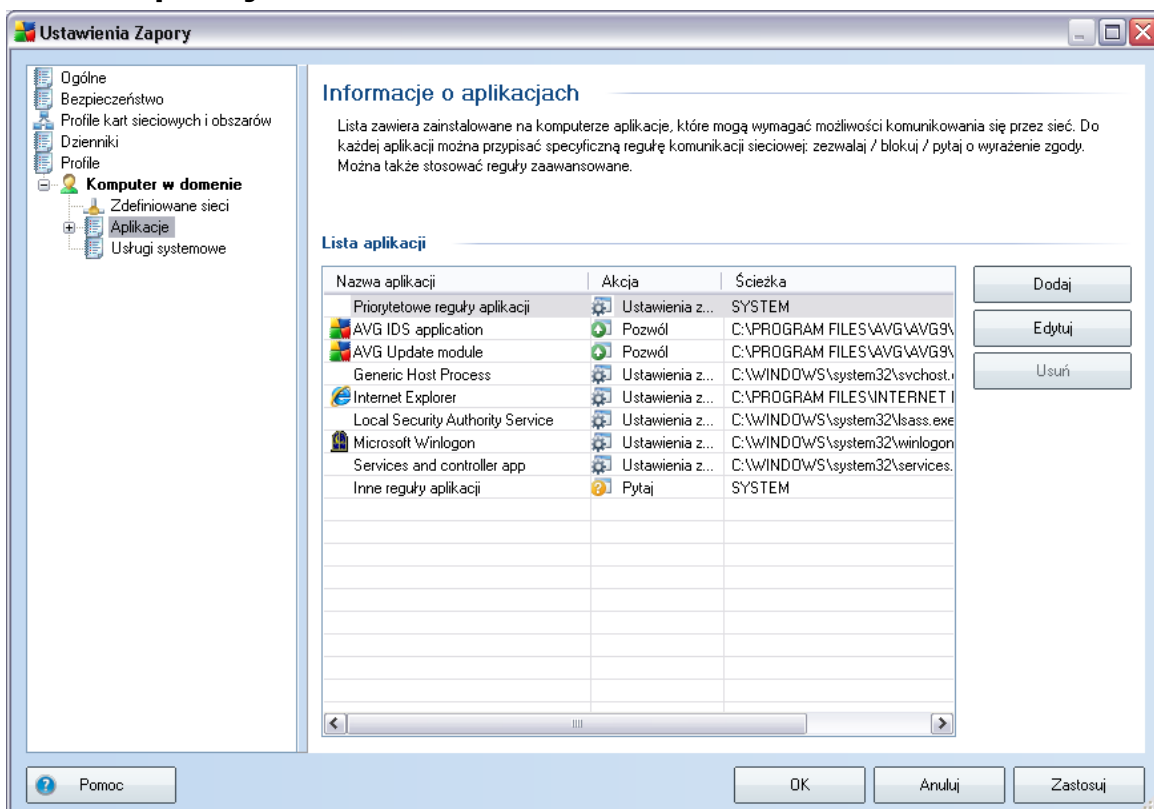
Możliwe jest w nim określenie **nazwy sieci**, wprowadzenie **opisu sieci** i zdecydowanie, czy oznaczyć ją jako bezpieczna. Adres sieci może być określony ręcznie w odrębnym oknie dialogowym otwieranym za pomocą przycisku **Dodaj adres IP** (można też użyć przycisków **Edytuj adres IP/ Usun adres IP**). W tym oknie można określić sieć, podając zakres adresów IP lub maskę.

W wypadku dużej liczby sieci, które mają być zdefiniowane jako części nowo utworzonej sieci, można użyć opcji **Zaawansowana reprezentacja zakresu adresów IP**: należy w tym celu wpisać listę wszystkich sieci do odpowiedniego pola tekstowego (*obsługiwane są wszystkie standardowe formaty*) i kliknąć przycisk **Sprawdź**, aby upewnić się, że format został rozpoznany. Następnie należy kliknąć przycisk **OK**, aby potwierdzić i zapisać dane.

- **Edytuj sieć** – powoduje otwarcie okna dialogowego **Właściwości sieci** (patrz wyżej), w którym można edytować parametry zdefiniowanej sieci (*okno to jest identyczne jak podczas dodawania nowej sieci. Zobacz opis w poprzednim akapicie*).





- **Usun siec** — usuwa zapis dotyczący wybranej sieci z listy sieci.
- **Oznacz jako bezpieczna** — domyślnie wszystkie sieci uważane są za niebezpieczne i tylko w przypadku pewności, że dana sieć jest godna zaufania, można przypisać jej takie ustawienie (*i na odwrót: gdy sieć została oznaczona jako bezpieczna, tekst przycisku zostaje zmieniony na "Oznacz jako niezabezpieczona"*).
- **Pomoc** — otwiera okno dialogowe z powiązaniem tematu pomocy.

### 11.5.3. Aplikacje



W oknie dialogowym **Informacje o aplikacjach** wyświetlana jest lista wszystkich zainstalowanych aplikacji, które komunikują się z siecią, oraz ikony reprezentujące przypisane do nich akcje:

-  Odblokuj komunikacje dla wszystkich sieci

-  Odblokuj komunikacje tylko dla sieci zdefiniowanych jako bezpieczne
-  Zablokuj komunikacje
-  Wyświetlaj zapytanie w oknie dialogowym (*użytkownik będzie mógł w określonym momencie podjąć decyzje o odblokowaniu lub zablokowaniu komunikacji*)
-  Zdefiniowano ustawienia zaawansowane

Aplikacje wyświetlane na liście zostały wykryte na komputerze (*i przypisano im odpowiednie akcje*) podczas wyszukiwania przeprowadzanego przez [kreatora konfiguracji składnika Firewall](#) albo później (w przypadku nieznannej lub nowo zainstalowanej aplikacji).

***Uwaga: Należy pamiętać, że tylko aplikacje już zainstalowane mogą zostać wykryte, więc dla zainstalowanej później nowej aplikacji konieczne będzie zdefiniowanie reguł. Domyślnie, kiedy nowa aplikacja próbuje połączyć się z siecią po raz pierwszy, Zapora automatycznie utworzy dla niej regułę na podstawie bazy Trusted Database lub zapyta, czy komunikacja ma zostać odblokowana. W tym drugim przypadku możliwe będzie zapisanie odpowiedzi jako stałej reguły (która wówczas zostanie dodana do listy w tym oknie dialogowym).***

Mozna też zdefiniować reguły dla nowej aplikacji natychmiast, używając w tym oknie dialogowym przycisku **Dodaj** i podając szczegóły aplikacji.

Poza aplikacjami na liście wyświetlane są jeszcze dwie pozycje specjalne:

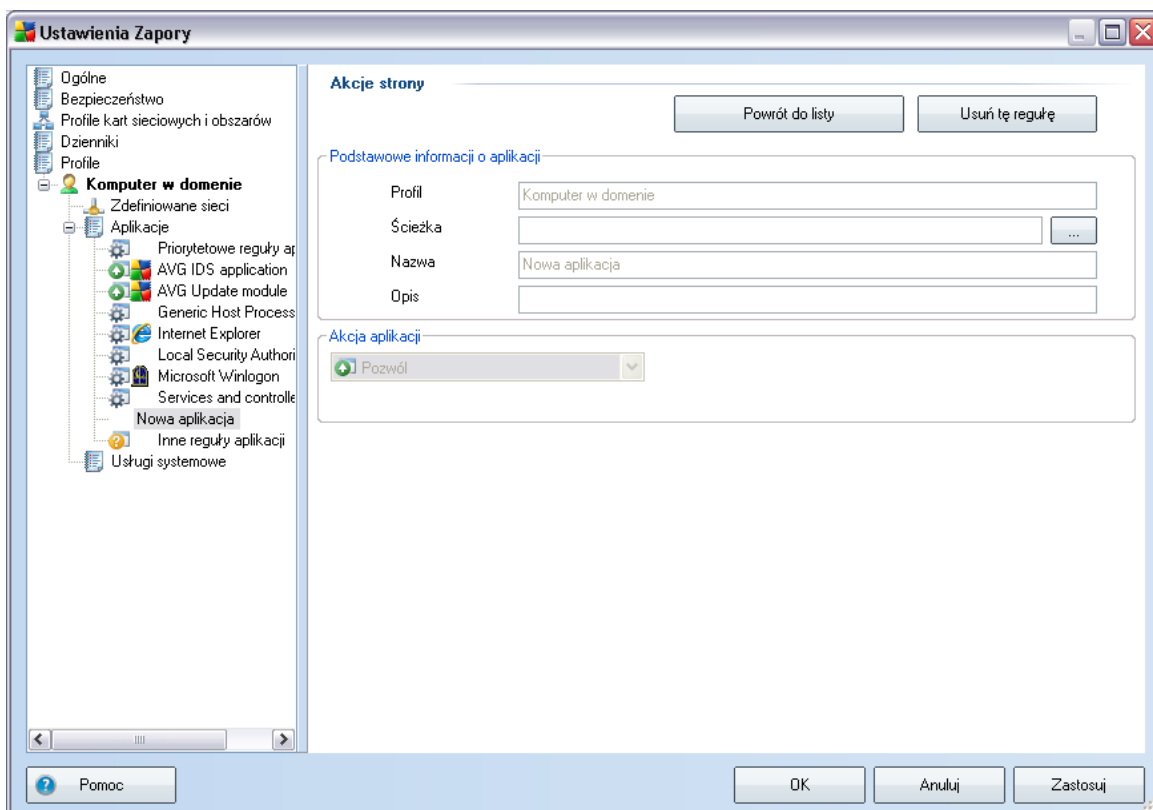
- **Priorytetowe reguły aplikacji** (*u góry listy*) są wybierane jako pierwsze i stosowane zawsze przed regułami określonej aplikacji.
- **Inne reguły aplikacji** (*na dole listy*) służą jako „rezerwa”, gdy nie są stosowane żadne określone reguły, np. dla nieznannej lub niezdefiniowanej aplikacji.

***Te pozycje mają inne opcje niż zwykłe ustawienia aplikacji i są przeznaczone tylko dla doświadczonych użytkowników. Stanowczo zalecamy niemodyfikowanie tych ustawień***

## **Przyciski kontrolne**

Listę można edytować przy użyciu następujących przycisków kontrolnych:

- **Dodaj** — otwiera puste okno dialogowe **Akcje strony** w celu zdefiniowania nowych reguł aplikacji.
- **Edytuj** — otwiera to samo okno dialogowe **Akcje strony** z odpowiednimi danymi w celu edytowania istniejącego zestawu reguł aplikacji.
- **Usun** — usuwa wybrany zbiór reguł z listy.
- **Pomoc** — otwiera okno dialogowe z powiazanym tematem pomocy.



To okno dialogowe służy do szczegółowego definiowania ustawień dla odpowiednich aplikacji.

### Akcje strony

- Πρὸςχητικὸ **Powrót do listy** umożliwia wyświetlenie przeglądu wszystkich

zdefiniowanych reguł aplikacji.






- Πρῶψχισκ **Usun te regule** umożliwia usuwanie wyświetlanej w danej chwili reguły aplikacji. Należy pamiętać, że tej czynności nie da się cofnąć!

## Podstawowe informacje o aplikacji

W tej sekcji należy wprowadzić **nazwę** aplikacji oraz jej **opis** (*opcjonalny krótki komentarz do własnego użytku*). W polu **Ścieżka** należy wprowadzić pełną ścieżkę dostępu do aplikacji (*pliku wykonywalnego*) na dysku; aplikacje można łatwo zlokalizować w drzewie katalogów, klikając przycisk „...”.

## Akcja aplikacji

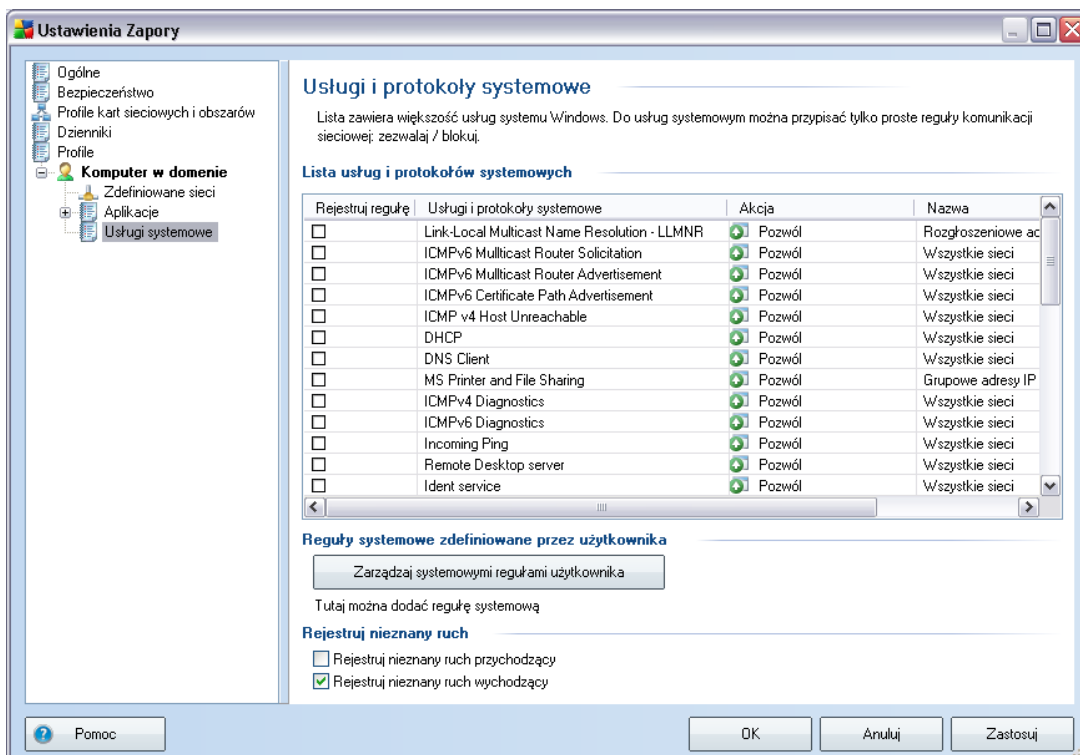
Z rozwijanego menu można wybrać reguły Zapory dla danej aplikacji, tj. jakie akcje powinien wykonać składnik, gdy aplikacja próbuje połączyć się z siecią.

-  **Odblokuj wszystkie** — umożliwia wszystkim aplikacjom dowolną komunikację ze zdefiniowanymi sieciami i kartami sieciowymi (bez żadnych ograniczeń).
-  **Odblokuj bezpieczne** — umożliwia aplikacji dostęp tylko do sieci zdefiniowanych jako bezpieczne (godne zaufania).
-  **Blokuj** — automatycznie blokuje komunikację; aplikacja nie będzie mogła uzyskać dostępu do żadnej sieci.
-  **Pytaj** — powoduje wyświetlenie okna dialogowego pozwalającego zdecydować, czy próba połączenia ma zostać w danym momencie odblokowana czy zablokowana.
-  **Ustawienia zaawansowane** — powoduje wyświetlenie dalszych opcji ustawień szczegółowych w dolnej części okna dialogowego, w sekcji **Szczegółowe reguły aplikacji**. Ustawienia szczegółowe będą stosowane zgodnie z kolejnością ich wyświetlenia na liście, w związku z czym można je **przesuwać w górę** lub **w dół** zgodnie z pożądaną kolejnością ich przetwarzania przez Zaporę. Po kliknięciu wybranej reguły z listy w dolnej części okna dialogowego zostanie wyświetlony przegląd szczegółów tej reguły. Wszystkie spośród wartości podkreślonych na niebiesko mogą zostać zmienione w odpowiednich oknach dialogowych. Aby usunąć zaznaczoną regułę, wystarczy

kliknąć przycisk **Usun**. Aby zdefiniować nową regułę, kliknij przycisk **Dodaj**, który spowoduje otwarcie okna dialogowego **Zmieni szczegóły reguły** umożliwiającego określenie niezbędnych szczegółów.




#### 11.5.4. Usługi systemowe

**Wszelkie zmiany w konfiguracji usług i protokołów systemowych powinny być wprowadzane JEDYNIEM przez doświadczonych użytkowników.**



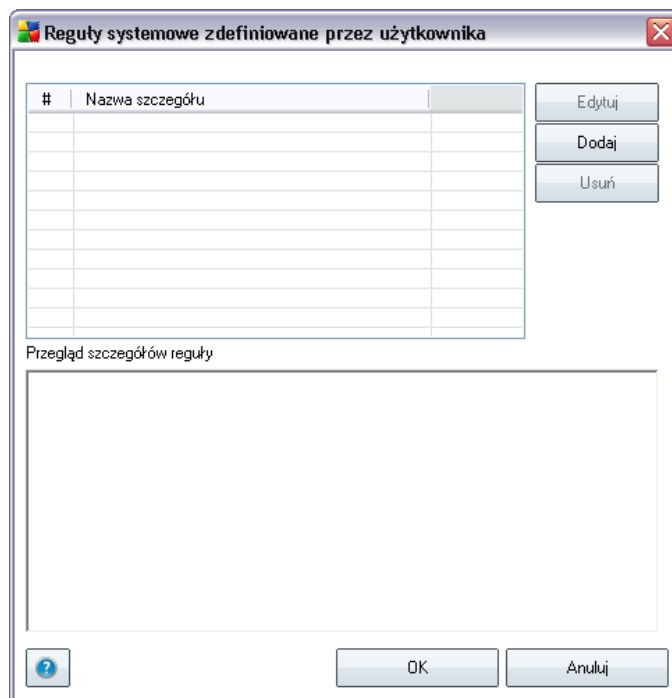
W oknie dialogowym **Usługi i protokoły systemowe** dostępna jest lista standardowych usług i protokołów systemu Windows, które mogą wymagać komunikacji poprzez sieć. Tabela zawiera następujące kolumny:

- **Rejestruj użycie reguł** — to pole pozwala włączyć funkcję zapisywania każdego użycia reguły w Dziennikach.
- **Usługi i protokoły systemowe** — w tej kolumnie wyświetlana jest nazwa odpowiedniej usługi systemowej.
- **Akcja** — w tej kolumnie wyświetlana jest ikona przypisanej akcji:

-  Odblokuj komunikacje dla wszystkich sieci
-  Odblokuj komunikacje tylko dla sieci zdefiniowanych jako bezpieczne
-  Zablokuj komunikacje
- **Sieci** — w tej kolumnie wyświetlane są informacje o tym, której sieci dotyczy dana reguła systemowa.

Lista (w tym przypisane akcje) może być edytowana przy użyciu następujących przycisków:

- Aby edytować ustawienia dowolnej pozycji z listy (w tym przypisanych akcji), należy kliknąć te pozycje prawym przyciskiem myszy i wybrać polecenie **Edytuj**.
- Aby otworzyć nowe okno dialogowe pozwalające definiować własne reguły usług systemowych (patrz ilustracja poniżej), kliknij przycisk **Zarządzaj własnymi regułami systemowymi**. Górna sekcja okna dialogowego **Reguły systemowe zdefiniowane przez użytkownika** zawiera przegląd wszystkich szczegółów edytowanej w danej chwili reguły systemowej. W dolnej sekcji wyświetlany jest wybrany szczegół. Szczegóły reguły zdefiniowanej przez użytkownika mogą być edytowane, dodawane lub usuwane za pomocą odpowiednich przycisków. Reguły zdefiniowane przez producenta mogą być jedynie edytowane:



**Ostrzeżenie:** Należy pamiętać, że szczegółowe ustawienia reguły są ustawieniami zaawansowanymi i kierowane są przede wszystkim do administratorów sieci, którzy wymagają pełnej kontroli nad konfiguracją Zapory. W przypadku braku wystarczającej wiedzy o typach protokołów, numerach portów sieciowych, adresach IP itp. nie należy modyfikować tych ustawień! Jeśli istnieje uzasadniona potrzeba zmiany tej konfiguracji, szczegółowe informacje można znaleźć w plikach pomocy dostępnych w poszczególnych oknach dialogowych.

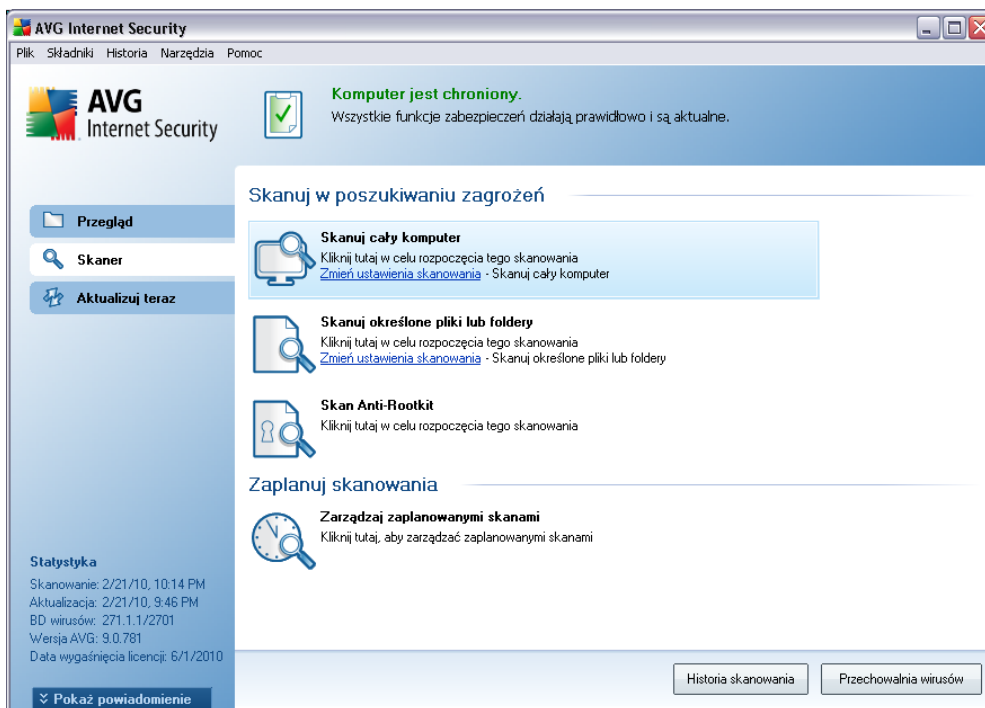
### Rejestruj nieznaną ruch

- **Rejestruj nieznaną ruch przychodzący** — to pole wyboru należy zaznaczyć, aby zapisywać w dziennikach każdą nieznaną próbę połączenia się z zewnątrz z tym komputerem.
- **Rejestruj nieznaną ruch wychodzący** — to pole wyboru należy zaznaczyć, aby zapisywać w dziennikach każdą nieznaną próbę połączenia się z tego komputera z zewnętrzną lokalizacją.

## 12. Skanowanie AVG

Skanowanie jest podstawowym elementem funkcjonowania systemu **AVG 9 Anti-Virus plus Firewall**. Możliwe jest uruchamianie testów na zadanie lub [planowanie ich okresowego przeprowadzania](#) o odpowiednich porach.

### 12.1. Interfejs skanowania



Interfejs skanera AVG dostępny jest za pośrednictwem linku **Skaner\*\*\***. Kliknięcie go otwiera okno **Skanuj w poszukiwaniu zagrożeń**. Okno to zawiera następujące elementy:

- przegląd [wstępnie zdefiniowanych testów](#) — trzy typy testów (zdefiniowane przez dostawcę oprogramowania) są gotowe do użycia na zadanie lub według utworzonego harmonogramu:
  - [Skan całego komputera](#)
  - [Skan określonych plików lub folderów](#)
  - **Skan Anti-rootkit**

- [Planowanie testów](#) — w tym obszarze można definiować nowe testy i tworzyć nowe harmonogramy w zależności od potrzeb.

### Przyciski kontrolne

Interfejs skanera zawiera następujące przyciski kontrolne:

- **Historia skanowania** — wyświetla okno dialogowe [Przegląd wyników skanowania](#), które zawiera pełną historię testów.
- **Przechowalnia wirusów** — otwiera nowe okno z zawartością [Przechowalni wirusów](#), w której izolowane są wykryte infekcje.

## 12.2. Wstępnie zdefiniowane testy

Jedną z głównych funkcji systemu **AVG 9 Anti-Virus plus Firewall** jest skanowanie na zadanie. Testy na zadanie służą do skanowania konkretnych obszarów komputera, gdy użytkownik podejrzewa obecność wirusa. Stanowczo zaleca się jednak wykonywanie tych testów regularnie, nawet w przypadku, gdy nie ma takich podejrzeń.

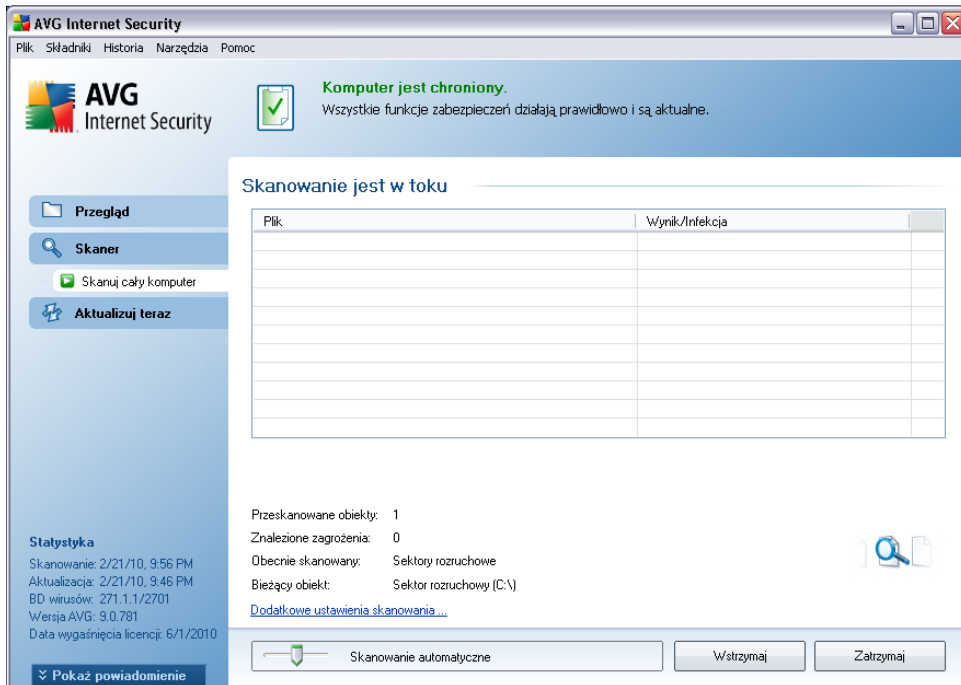
W systemie **AVG 9 Anti-Virus plus Firewall** dostępne są dwa typy skanowania zdefiniowane wstępnie przez producenta oprogramowania:

### 12.2.1. Skan całego komputera

**Skanuj cały komputer** — skanuje cały komputer w poszukiwaniu możliwych infekcji i/lub potencjalnie niechcianych programów. Test ten obejmuje wszystkie dyski twarde komputera. Wykryte infekcje są leczone lub przenoszone do [Przechowalni wirusów](#). Skanowanie całego komputera powinno być regularnie przeprowadzane co najmniej raz na tydzień.

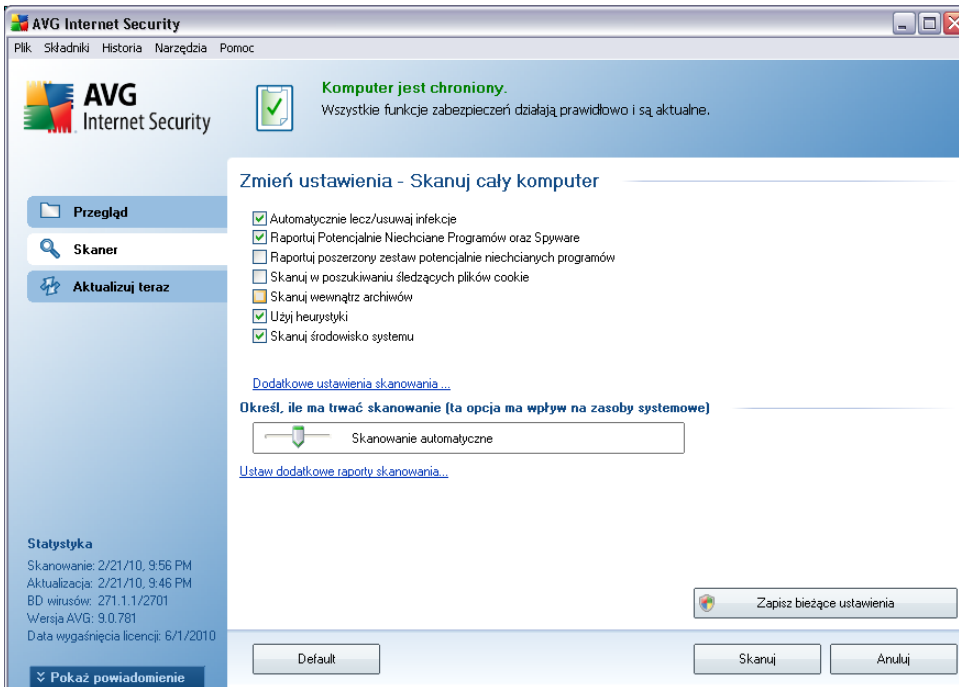
### Uruchamianie skanowania

**Skanowanie całego komputera** można uruchomić bezpośrednio z poziomu [interfejsu skanera](#), klikając ikonę odpowiedniego testu. Dla tego skanowania nie można określać dalszych ustawień; jest ono uruchamiane od razu w oknie dialogowym **Skanowanie w toku**. (patrz ilustracja). W razie potrzeby skanowanie można tymczasowo przerwać (**Wstrzymaj**) lub anulować (**Zatrzymaj**).

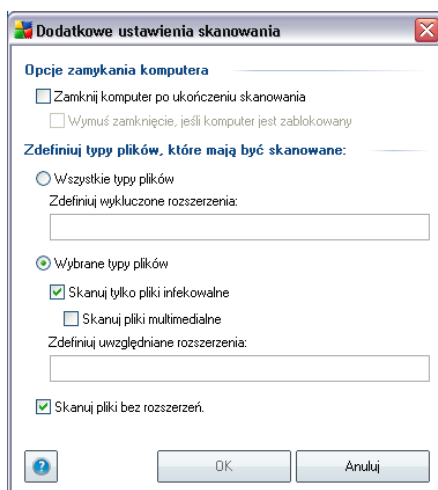


## Edycja konfiguracji skanowania

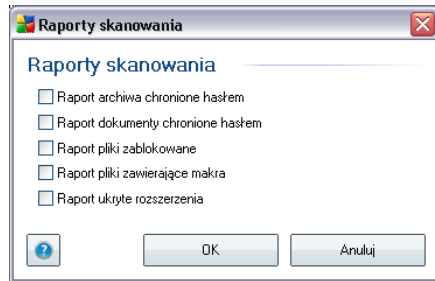
Wstępne, domyślne ustawienia testu **Skan całego komputera** można łatwo edytować. Kliknięcie linku **Zmien ustawienia skanowania** powoduje otwarcie okna dialogowego **Zmien ustawienia skanu całego komputera**. **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



- **Parametry skanowania** — na liście parametrów skanowania można włączyć/ wylączyć określone parametry w zależności od potrzeb. Większość parametrów jest domyślnie włączona i automatycznie używana podczas skanowania.
- **Dodatkowe ustawienia skanowania** — link do okna dialogowo **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:



- **Opcje wyłączenia komputera** — określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej opcji (**Zamknij komputer po ukonczeniu skanowania**) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (**Wymus zamknięcie, jeśli komputer jest zablokowany**).
- **Zdefiniuj typy plików do skanowania** — należy zdecydować, które z poniższych elementów mają być skanowane:
  - **Wszystkie typy plików** z opcja zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików, który nie powinny być skanowane;
  - **Wybrane typy plików** — skanowane będą tylko pliki infekowalne (pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne), z uwzględnieniem plików multimedialnych (plików wideo i audio — jeśli to pole zostanie niezaznaczone, czas skanowanie skróci się jeszcze bardziej, ponieważ takie pliki często są duże, a nie są podatne na infekcję). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.
  - Opcjonalnie można zdecydować o **skanowaniu plików bez rozszerzenia** — ta opcja jest domyślnie włączona i zaleca się niezmiętnie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.
- **Priorytet procesu skanowania** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślnie ustawiony jest priorytet średni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).
- **Ustaw dodatkowe raporty skanowania** — link ten pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić elementy lub zdarzenia, które mają być zgłaszane:



**Ostrzeżenie:** Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale [Skanowanie AVG / Planowanie skanowania / Jak skanować](#). Jeśli jednak domyślna konfiguracja testu **Skan całego komputera** zostanie zmieniona, nowe ustawienia można zapisać jako konfigurację domyślną, aby były używane we wszystkich przyszłych skanach całego komputera.

### 12.2.2. Skan określonych plików lub folderów

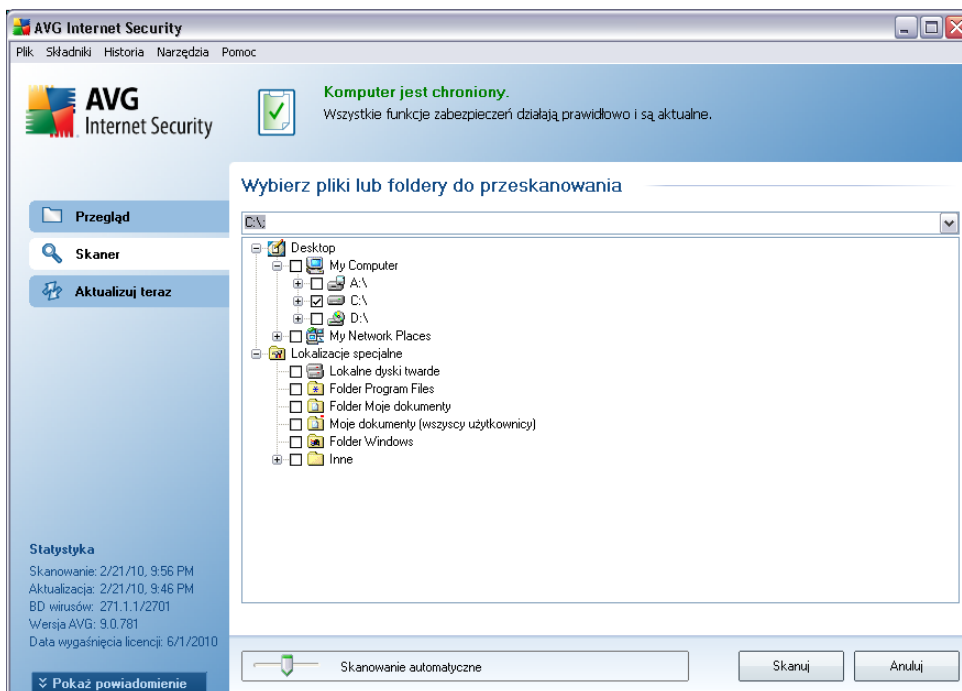
**Skan określonych plików lub folderów** — skanowane są tylko wskazane obszary komputera (wybrane foldery, a także dyski twarde, pamięci flash, CD itd.). Postępowanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu całego komputera: każdy znaleziony wirus jest leczony lub przenoszony do [Przechowalni](#). Skanowanie określonych plików lub folderów może posłużyć do utworzenia własnych testów i planowania ich zgodnie z konkretnymi potrzebami.

#### Uruchamianie skanowania

**Skanowanie określonych plików lub folderów** można uruchomić bezpośrednio z poziomu [interfejsu skanera](#), klikając ikonę testu. Wyświetlone zostanie nowe okno dialogowe **Wybierz pliki lub foldery do przeskanowania**. W drzewie katalogów należy wybrać te, które mają zostać przeskanowane. Ścieżki do wszystkich wybranych folderów zostaną wygenerowane automatycznie i wyświetlone w polu tekstowym w górnej części okna dialogowego.

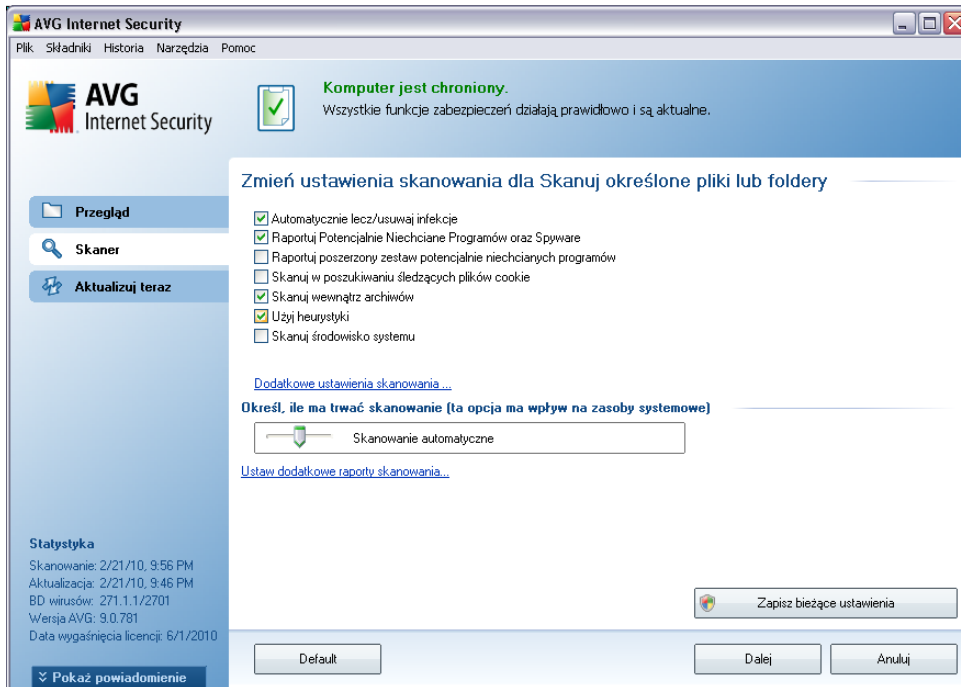
Mozna także przeskanować wybrany folder, wykluczając jednocześnie ze skanowania wszystkie jego podfoldery: należy wprowadzić znak minus „-” przed jego nazwą w wygenerowanej ścieżce (*patrz ilustracja*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „!”.

Na koniec, aby uruchomić skanowanie, należy nacisnąć przycisk **Rozpocznij skanowanie**; proces skanowania jest w zasadzie taki sam jak [skanowanie całego komputera](#).

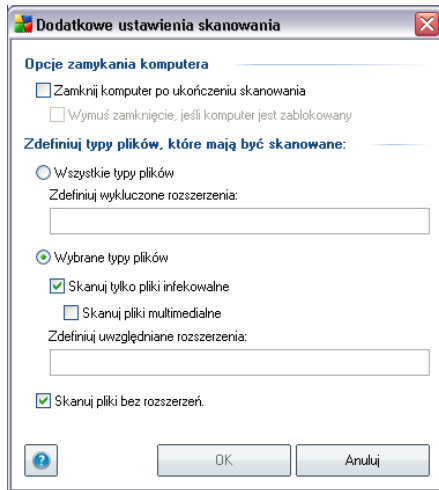


## Edycja konfiguracji skanowania

Wstępne, domyślne ustawienia testu **Skan określonych plików lub folderów** można łatwo edytować. Kliknięcie linku **Zmien ustawienia skanowania** powoduje otwarcie okna dialogowego **zmiany ustawień dla skanowania określonych plików lub folderów**. **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



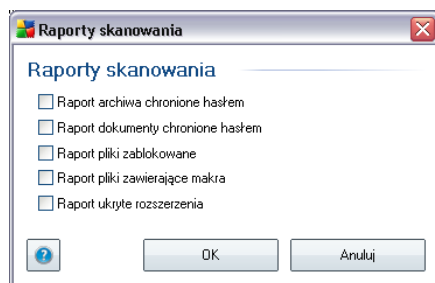
- **Parametry skanowania** — na liście parametrów skanowania można włączać/wyłączać określone parametry w zależności od potrzeb (*szczegółowy opis tych ustawień zawiera rozdział [Zaawansowane ustawienia AVG / Skany / Skanowanie określonych plików lub folderów](#)*).
- **Dodatkowe ustawienia skanowania** — link do okna dialogowego Dodatkowe ustawienia skanowania, w którym można określić następujące parametry:



- **Opcje wylaczania komputera** — okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (**Zamknij komputer po ukonczeniu skanowania**) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (**Wymus zamkniecie, jesli komputer jest zablokowany**).
- **Zdefiniuj typy plików do skanowania** — nastepnie nalezy zdecydowac, czy skanowane maja byc:
  - **Wszystkie typy plików** z opcja zdefiniowania wyjatków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;
  - **Wybrane typy plików** — skanowane beda tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe niewykonywalne*), z uwzglednieniem multimediiów (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowania skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.
  - Opcjonalnie mozna zdecydowac o **skanowaniu plików bez rozszerzenia** — ta opcja jest domyslnie włączona i zaleca sie niezmiennianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.
- **Priorytet procesu skanowania** — za pomoca suwaka mozna zmienic priorytet

procesu skanowania. Domyślnie ustawiony jest priorytet średni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).

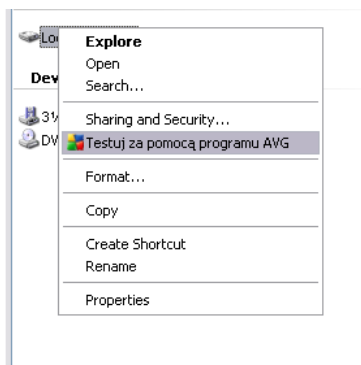
- **Ustaw dodatkowe raporty skanowania** — link ten pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić elementy lub zdarzenia, które mają być zgłaszane:



**Ostrzeżenie:** Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów — zgodnie z opisem w rozdziale [Skanowanie AVG / Planowanie skanowania / Jak skanować](#). Jeśli jednak domyślna konfiguracja testu **Skan określonych plików lub folderów** zostanie zmieniona, nowe ustawienia będzie można zapisać jako konfigurację domyślną, która będzie używana we wszystkich zdefiniowanych w przyszłości Skanach określonych plików lub folderów. Staje się ona również szablonem dla wszystkich nowych skanów zaplanowanych ([wszystkie testy użytkownika oparte są na bieżącej konfiguracji Skanu określonych plików lub folderów](#)).

### 12.3. Skan z poziomu eksploratora systemu Windows

Oprócz wstępnie zdefiniowanych skanów obejmujących cały komputer lub wybrane obszary, system **AVG 9 Anti-Virus plus Firewall** oferuje także możliwość skanowania określonych obiektów bezpośrednio z interfejsu Eksploratora Windows. Jeśli nie ma pewności co do zawartości pliku, który ma zostać otwarty, można przeskanować go „na zadanie”. W tym celu należy wykonać następujące kroki:



- W Eksploratorze Windows zaznacz plik (lub folder), który chcesz sprawdzić.
- Kliknij go prawym przyciskiem myszy, aby wyświetlić menu kontekstowe.
- Wybierz polecenie **Testuj za pomocą programu AVG**, aby system AVG przeskanował obiekt.

#### 12.4. Skan z poziomu wiersza poleceń

System **AVG 9 Anti-Virus plus Firewall** posiada opcje uruchamiania skanowania z poziomu wiersza poleceń. Opcji tej można używać na przykład na serwerach lub w czasie tworzenia skryptu wsadowego, który ma być uruchamiany po restarcie komputera. Uruchamiając skanowanie z wiersza poleceń, można używać większości parametrów dostępnych w graficznym interfejsie użytkownika AVG.

Aby uruchomić skanowanie z poziomu wiersza poleceń, należy użyć następującego polecenia w folderze, w którym zainstalowano system AVG:

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

#### Składnia polecenia

Składnia polecenia jest następująca:

- **avgscanx /parametr** ... np. **avgscanx /comp** w celu przeskanowania całego komputera
- **avgscanx /parametr /parametr** .. — jeśli używanych jest wiele parametrów, należy wpisać je w jednym wierszu, rozdzielając spacjami i ukośnikami

- jeśli parametry wymagają podania określonych wartości, (np. parametr **/scan** wymaga informacji o wybranych do przeskanowania obszarach komputera – należy wskazać dokładną ścieżkę), należy je rozdzielać przecinkami, na przykład: **avgscanx /scan=C:\,D:\**

### Parametry skanowania

Aby wyświetlić pełny przegląd dostępnych parametrów, należy wpisać odpowiednie polecenie oraz parametr **/?** lub **/HELP** (np. **avgscanx /?**). Jedynym wymaganym parametrem jest **/SCAN**, który pozwala określić, jakie obszary komputera mają być skanowane. Bardziej szczegółowe informacje na temat opcji zawiera [przeгляд parametrów wiersza poleceń](#).

Aby uruchomić skanowanie, należy nacisnąć klawisz **Enter**. Skanowanie można zatrzymać, naciskając kombinację klawiszy **Ctrl+C** lub **Ctrl+Pause**.

### Skanowanie z poziomu wiersza poleceń uruchamiane za pomocą interfejsu graficznego

Gdy komputer działa w trybie awaryjnym, skanowanie z poziomu wiersza poleceń można również uruchomić za pomocą interfejsu graficznego użytkownika. Skanowanie zostanie uruchomione z wiersza poleceń, a okno dialogowe **Kompozytor wiersza poleceń** umożliwi jedynie określenie większości parametrów skanowania w wygodnym interfejsie graficznym.

Ponieważ okno to jest dostępne tylko w trybie awaryjnym, jego szczegółowy opis można znaleźć w pliku pomocy dostępnym bezpośrednio z tego okna.

#### 12.4.1. Parametry skanowania z wiersza poleceń

Poniżej przedstawiono listę wszystkich parametrów dostępnych dla skanowania z wiersza poleceń:

- **/SCAN** [Skanuj określone pliki lub foldery](#) /SCAN=ścieżka;ścieżka  
(np. /SCAN=C:\;D:\)
- **/COMP** [Skanuj cały komputer](#)
- **/HEUR** Użyj analizy heurystycznej\*\*\*
- **/EXCLUDE** Wyklucz ze skanowania ścieżki lub pliki

- **/@** Plik polecenia /nazwa pliku/
- **/EXT** Skanuj te rozszerzenia /na przykład EXT=EXE,DLL/
- **/NOEXT** Nie skanuj tych rozszerzen /na przykład NOEXT=JPG/
- **/ARC** Skanuj archiwa
- **/CLEAN** Czysc automatycznie
- **/TRASH** Przenies zainfekowane pliki do Przechowalni wirusów\*\*\*
- **/QT** Szybki test
- **/MACROW** Raportuj pliki zawierajace makra
- **/PWDW** Raportuj pliki chronione haslem
- **/IGNLOCKED** Ignoruj pliki zablokowane
- **/REPORT** Raportuj do pliku /nazwa pliku/
- **/REPAPPEND** Dopisz do pliku raportu
- **/REPOK** Raportuj niezainfekowane pliki jako OK
- **/NOBREAK** Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- **/BOOT** Wlacz sprawdzanie MBR/sektora rozruchowego
- **/PROC** Skanuj aktywne procesy
- **/PUP** Raportuj [potencjalnie niechciane programy](#)
- **/REG** Skanuj rejestr
- **/COO** Skanuj pliki cookie
- **/?** Wyszwiatl pomoc na ten temat
- **/HELP** Wyszwiatl pomoc na ten temat
- **/PRIORITY** Ustaw priorytet skanowania /Niski, Automatyczny, Wysoki/ (zobacz [Ustawienia zaawansowane/ Skany](#))

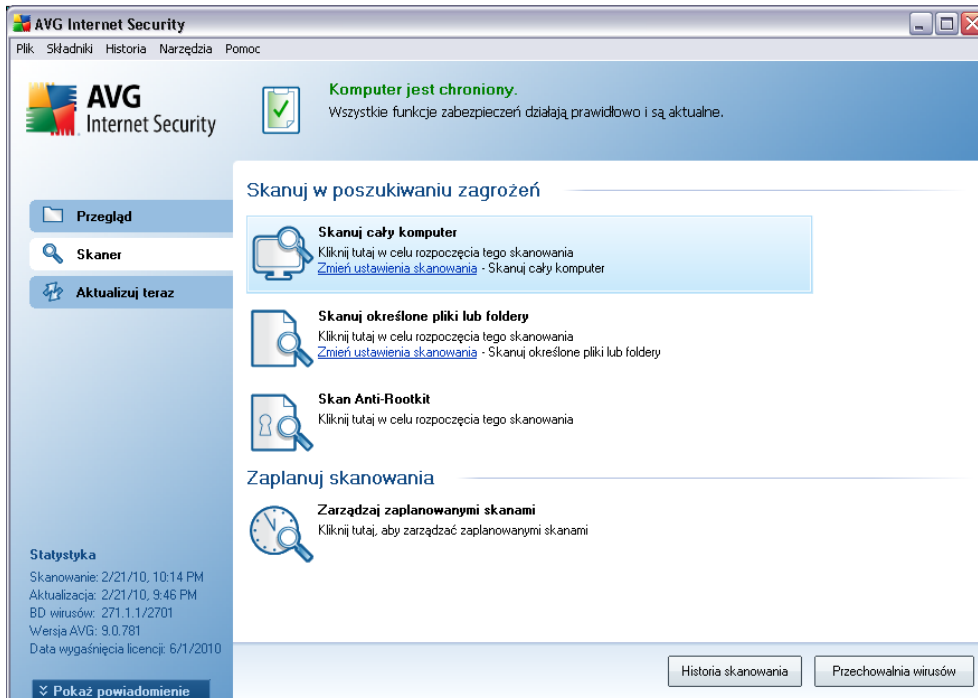
- **/SHUTDOWN** Zamknij komputer po ukończeniu skanowania
- **/FORCESHUTDOWN** Wymus zamknięcie komputera po ukończeniu skanowania
- **/ADS** Skanuj alternatywne strumienie danych (tylko NTFS)

## 12.5. Planowanie skanowania

System **AVG 9 Anti-Virus plus Firewall** pozwala uruchamiać skanowanie na zadanie (na przykład gdy podejrzewa się infekcję komputera) lub zgodnie z założonym harmonogramem. Stanowczo zaleca się korzystać z harmonogramu: ten sposób daje pewność, że komputer jest chroniony przed infekcjami i zwalnia użytkownika z obowiązku pamiętania o regularnych testach.

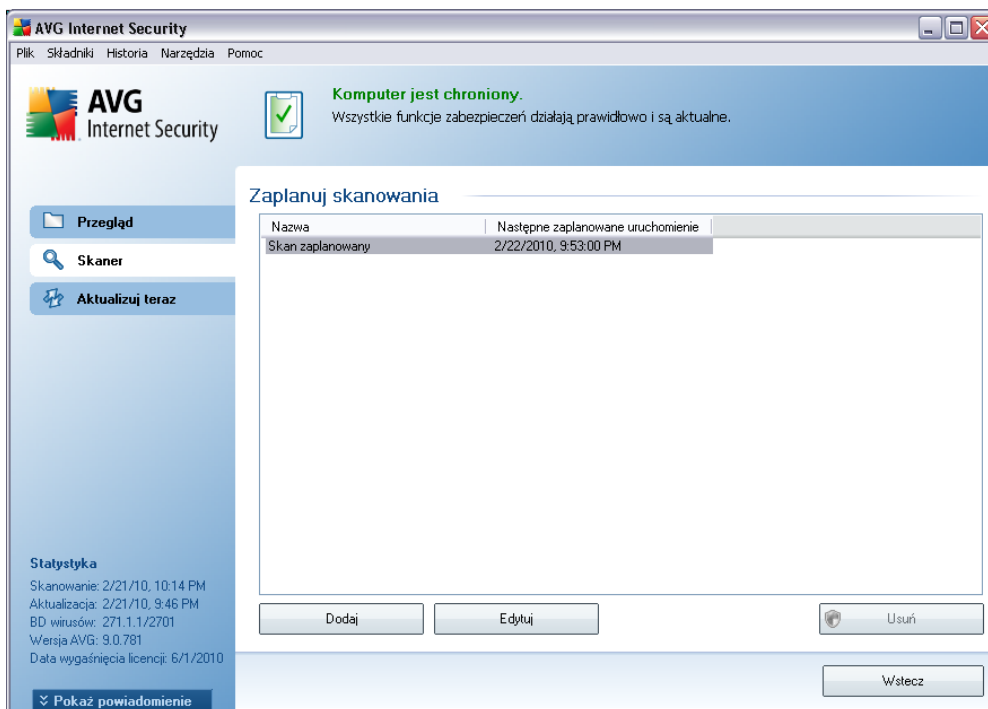
**Skan całego komputera** należy uruchamiać regularnie co najmniej raz na tydzień. Jeśli jest to możliwe, należy skanować komputer codziennie — zgodnie z domyślną konfiguracją harmonogramu skanowania. Jeśli komputer działa 24 godziny na dobę, można zaplanować skanowanie poza czasem pracy. Jeśli komputer jest czasami wyłączany, pominięte z tego powodu skany uruchamiane są [po ponownym włączeniu komputera](#).

Aby utworzyć nowe harmonogramy, skorzystaj z przycisku znajdującego się w dolnej części [interfejsu skanera AVG](#), w sekcji **Zaplanuj skanowania**:



## Zaplanuj skanowania

Kliknij ikone w sekcji **Zaplanuj skanowania**, aby otworzyć nowe okno dialogowe **planowania skanowania**, które zawiera listę wszystkich zaplanowanych testów:

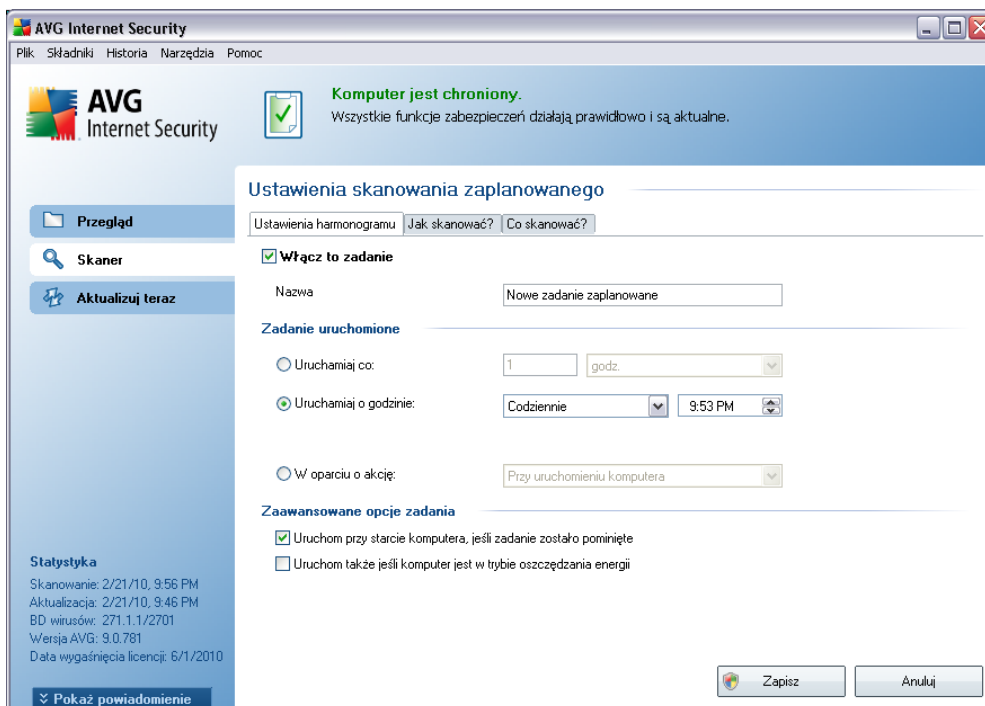


Zawartość okna można edytować, używając następujących przycisków:

- **Dodaj** — otwiera okno **Ustawienia skanowania zaplanowanego**, a w nim kartę **Ustawienia harmonogramu**. W oknie tym można określić parametry definiowanego testu.
- **Edytuj** — jest aktywny tylko, jeśli wybrano istniejący test na liście zaplanowanych testów. W takim przypadku kliknięcie przycisku powoduje przejście do okna dialogowego **Ustawienia skanowania zaplanowanego**, na kartę **Ustawienia harmonogramu**. Parametry wybranego testu są już określone i można je edytować.
- **Usuń** — jest aktywny tylko, jeśli wybrano istniejący test na liście zaplanowanych skanowań. Kliknięcie przycisku spowoduje usunięcie wybranej pozycji z listy. Usunąć można jedynie testy zdefiniowane przez użytkownika; nie da się usunąć domyślnego **Skanu zaplanowanego**.
- **Wstecz** — pozwala wrócić do [interfejsu skanera AVG](#)

### 12.5.1. Ustawienia harmonogramu

Aby zaplanować nowy test i uruchamiać go regularnie, należy przejść do okna dialogowego **Ustawienia zaplanowanego testu** (klikając przycisk **Dodaj harmonogram skanowania** w oknie dialogowym **Planowanie skanowania**). Okno dialogowe jest podzielone na trzy karty: **Ustawienia harmonogramu** – zobacz ilustracja poniżej (karta otwierana domyślnie), [Jak skanować](#) [Co skanować](#).



Na karcie **Ustawienia harmonogramu** można zaznaczyć/odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć zaplanowany test lub włączyć go ponownie, gdy zajdzie taka potrzeba.

Następnie należy nazwać nowo tworzony skan. Nazwę można wpisać w polu tekstowym obok etykiety **Nazwa**. Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości.

**Przykład:** Nazwy takie jak „Nowy skan” lub „Mój skan” nie są odpowiednie, ponieważ nie informują o tym, co jest przedmiotem skanowania. Przykładem dobrej, opisowej nazwy jest „Skan obszarów systemowych”. Ponadto, nie ma potrzeby określenia w nazwie skanowania, czy skanowany jest cały komputer, czy tylko jego wybrane obszary – własne testy użytkownika są zawsze specyficznym [skanowaniem określonych plików lub folderów](#).

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

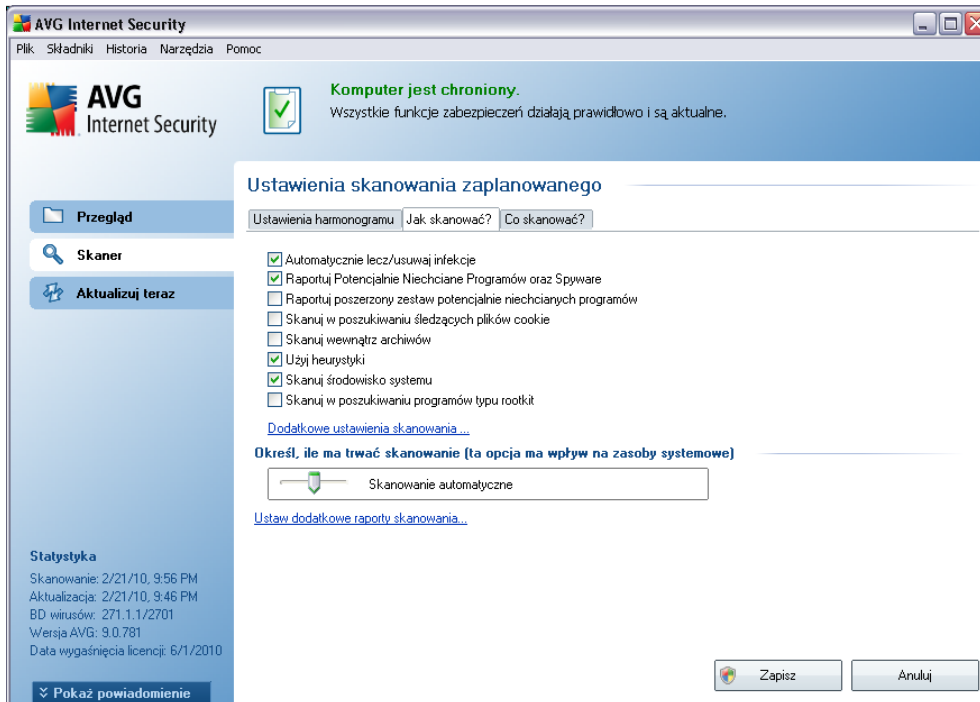
- **Zadanie uruchomione** — należy określić interwał przeprowadzanych testów. Skanowanie może być powtarzane w określonych odstępach czasu (**Uruchamiaj co**) lub o zadanej godzinie (**Uruchamiaj o określonej godzinie**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**W oparciu o akcje, np. uruchomienie komputera**).
- **Zaawansowane opcje zadania** — ta sekcja umożliwia zdefiniowanie warunków skanowania w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony.

### Przyciski kontrolne konfiguracji harmonogramu

Na trzech zakładkach okna dialogowego **Ustawienia zaplanowanego skanowania** dostępne są trzy przyciski sterujące (**Ustawienia harmonogramu**, **Jak skanować** i **Co skanować**). Działanie tych przycisków jest takie samo na każdej zakładce:

- **Zapisz** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [domyślnego okna Interfejsu użytkownika AVG](#). Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
- **Anuluj** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [Interfejsu użytkownika AVG](#).

## 12.5.2. Jak skanować?



Karta **Jak skanować?** zawiera listę parametrów testu, które można włączyć lub wyłączyć. Domyślnie większość funkcji jest włączona, a odpowiadające im ustawienia są stosowane podczas skanowania. Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachowując wstępnie zdefiniowaną konfigurację:

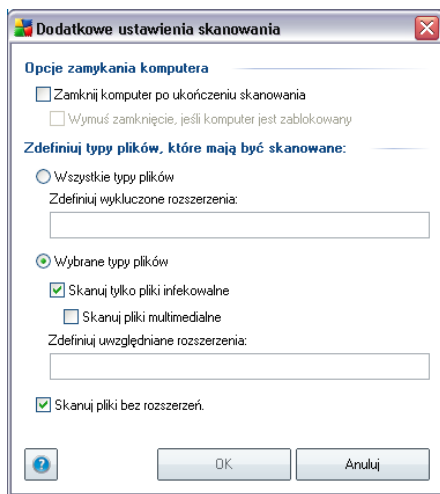
- **Automatycznie lecz/usuwaj infekcje** — (domyślnie włączona) jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowanego pliku nie można wyleczyć, lub jeśli opcja ta zostanie wyłączona, system powiadomi o wykryciu wirusa i zapyta o sposób reakcji na infekcję. Zalecana czynnością jest przeniesienie zainfekowanego pliku do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane programy i spyware** (opcja domyślnie włączona) — zaznaczenie tego pola powoduje włączenie silnika [Anti-Spyware](#) i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). [Oprogramowanie szpiegujące](#) należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji — znacząco zwiększa ona poziom

ochrony komputera

- **Raportuj udoskonalony zestaw potencjalnie niechcianych programów** — jeśli poprzednia opcja jest aktywna, można również zaznaczyć to pole, aby możliwe było wykrywanie większej ilości [oprogramowania szpiegującego](#), czyli programów, które są zupełnie bezpieczne w momencie nabywania ich od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.
- **Skanuj w poszukiwaniu sledzacych plików cookie** — (domyślnie włączone) ten parametr składnika [Anti-Spyware](#) określa, czy wykrywane mają być pliki cookie (używane w protokole HTTP do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach, np. preferencji wyglądu witryny i zawartość koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** — (domyślnie włączona) parametr ten określa, czy skanowanie ma obejmować pliki znajdujące się wewnątrz niektórych typów archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** — (domyślnie włączona) analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny) jest jedną z metod wykrywania wirusów w czasie rzeczywistym.
- **Skanuj środowisko systemu** — (domyślnie włączona) skanowanie obejmuje także obszary systemowe komputera.

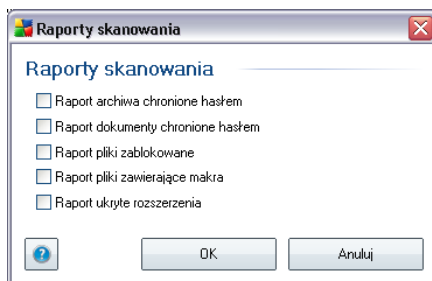
Następnie można zmienić konfigurację skanowania zgodnie z poniższym opisem:

- **Dodatkowe ustawienia skanowania** — link do okna dialogowego **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:



- **Opcje wylaczania komputera** — okreslaja, czy komputer ma zostac automatycznie wylaczony po zakonczeniu skanowania. Wybranie tej opcji (**Zamknij komputer po ukonczeniu skanowania**) powoduje aktywowanie nowej funkcji, która pozwala zamknac komputer nawet, gdy jest zablokowany (**Wymus zamkniecie, jesli komputer jest zablokowany**).
- **Zdefiniuj typy plików do skanowania** — nalezy zdecydowac, które z ponizszych elementow maja byc skanowane:
  - **Wszystkie typy plików** z opcja zdefiniowania wyjatkow skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzen, który nie powinny byc skanowane;
  - **Wybrane typy plików** — skanowane beda tylko pliki infekowalne (*pliki, które nie moga zostac zainfekowane, nie beda skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzglednieniem plików multimedialnych (*plików wideo i audio — jesli to pole pozostanie niezaznaczone, czas skanowanie skróci sie jeszcze bardziej, poniewaz takie pliku czesto sa duze, a nie sa podatne na infekcje*). Za pomoca rozszerzen mozna okreslic, które pliki maja byc zawsze skanowane.
  - Opcjonalnie mozna zdecydowac o **skanowaniu plików bez rozszerzenia** — ta opcja jest domyslnie włączona i zaleca sie niezmiennianie tego stanu bez waznego powodu. Pliki bez rozszerzenia sa podejrzane i powinny byc skanowane za kazdym razem.

- **Priorytet procesu skanowania** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślnie ustawiony jest priorytet średni (*Skanowanie automatyczne*), który optymalizuje zarówno szybkość skanowania, jak i wykorzystanie zasobów systemowych. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).
- **Ustaw dodatkowe raporty skanowania** — link ten pozwala otworzyć nowe okno dialogowe **Raporty skanowania**, w którym można określić elementy lub zdarzenia, które mają być zgłaszane:



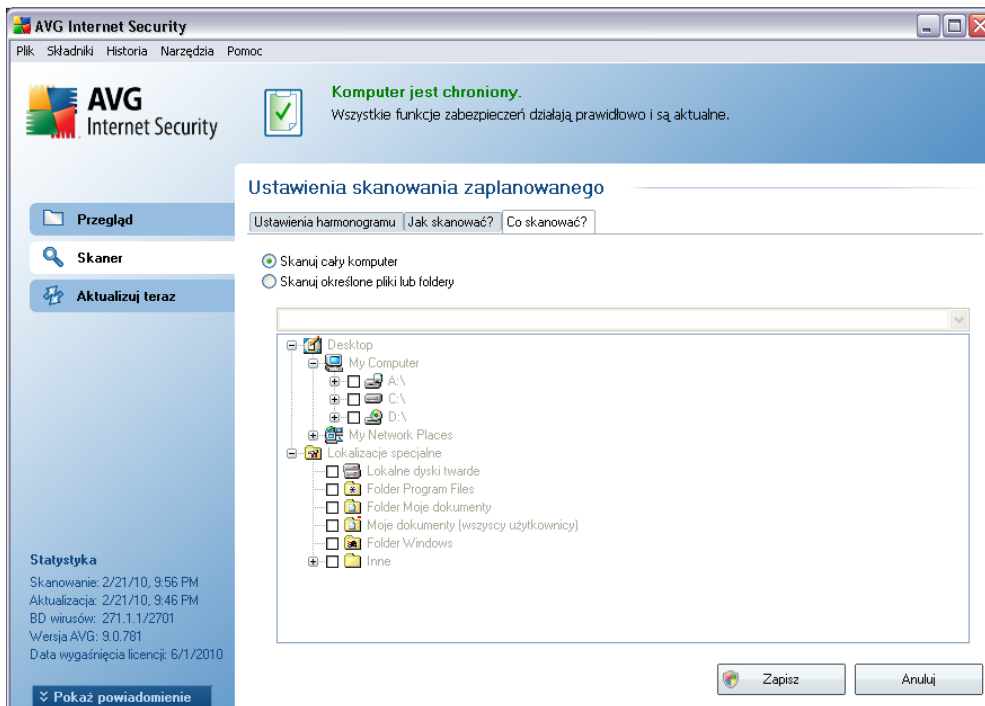
**Uwaga:** Domyślnie konfiguracja jest ustawiona pod kątem optymalnej wydajności. Konfiguracje skanowania należy zmieniać tylko w uzasadnionych sytuacjach. Stanowczo zaleca się stosowanie wstępnie zdefiniowanych ustawień. Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników. Więcej opcji dostępne jest w oknie [Ustawienia zaawansowane](#), (**Menu główne/Plik/Ustawienia zaawansowane**).

## Przyciski kontrolne

Na wszystkich trzech kartach okna z **konfiguracją skanu zaplanowanego** ([Ustawienia harmonogramu](#), [Jak skanować?](#) i [Co skanować?](#)) dostępne są dwa przyciski kontrolne. Ich działanie na każdej karcie jest takie samo:

- **Zapisz** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [domyślnego okna Interfejsu użytkownika AVG](#). Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
- **Anuluj** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [Interfejsu użytkownika AVG](#).

### 12.5.3. Co skanować?



Na karcie **Co skanować?** można określić, czy planowane jest [skanowanie całego komputera](#), czy [skanowanie określonych plików lub folderów](#).

Jeśli zostanie wybrane skanowanie określonych plików lub folderów, w dolnej części tego okna dialogowego zostanie aktywowane okno katalogów, które umożliwi wybranie folderów do skanowania (*rozwijaj pozycje, klikając znak plusa, dopóki nie znajdziesz folderu, który ma zostać przeskanowany*). Zaznaczając więcej pól, można wybrać kilka folderów. Wybrane foldery zostaną wyświetlone w polu tekstowym u góry okna dialogowego, a historia wybranych skanowań będzie przechowywana w rozwijanym menu do późniejszego użytku. Opcjonalnie można wprowadzić ręcznie pełną ścieżkę dostępu wybranego folderu (*w przypadku kilku ścieżek należy je rozdzielić średnikiem bez dodatkowej spacji*).

Drzewo katalogów zawiera również gałęzie **Lokalizacje specjalne**. Poniżej znajduje się lista tych lokalizacji; będa one skanowane, jeśli zostanie obok nich zaznaczone odpowiednie pole wyboru:

- **Lokalne dyski twarde** — wszystkie dyski twarde na tym komputerze
- **Program Files** — C:\:\Folder Program Files\

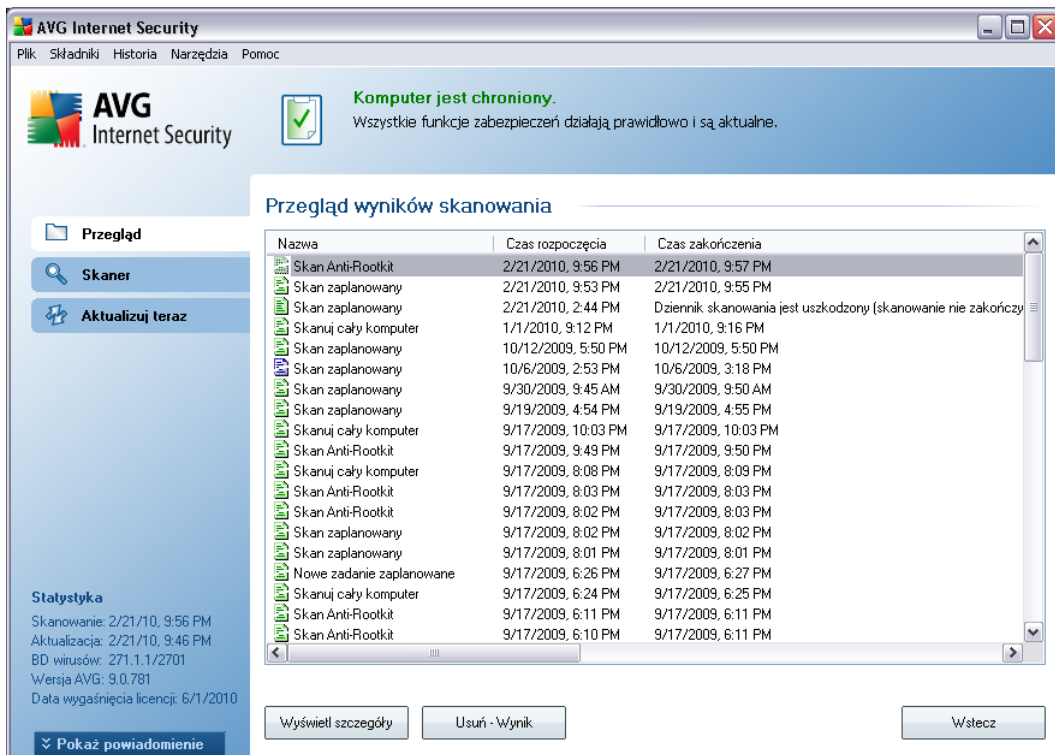
- **Folder Moje dokumenty** — C:\Documents and Settings\User\My Documents\
- **Udostępniane dokumenty** — C:\Documents and Settings\All Users\Documents\
- **Folder Windows** — C:\Windows\
- **Inne**
  - *Dysk systemowy* — dysk twardy, na którym zainstalowany jest system operacyjny (zazwyczaj C:)
  - *Folder systemowy* — Windows/System32
  - *Folder plików tymczasowych* — Documents and Settings/User/Local Settings/Temp
  - *Folder tymczasowych plików internetowych* — Documents and Settings/User/Local Settings/Temporary Internet Files

### **Przyciski kontrolne konfiguracji harmonogramu**

Na trzech zakładkach okna dialogowego **Ustawienia zaplanowanego skanowania** dostępne są trzy przyciski sterujące (**Ustawienia harmonogramu**, **Jak skanować** i **Co skanować**). Działanie tych przycisków jest takie samo na każdej zakładce:

- **Zapisz** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [domyślnego okna Interfejsu użytkownika AVG](#). Oznacza to, że aby zapisać nowe parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
- **Anuluj** — powoduje anulowanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do [Interfejsu użytkownika AVG](#).


## 12.6. Przegląd wyników skanowania



Dostęp do okna **Przegląd wyników skanowania** możliwy jest z poziomu [Interfejsu skanera AVG](#), przez kliknięcie przycisku **Historia skanowania**. Okno to zawiera listę wszystkich wcześniejszych testów oraz informacje o ich wynikach:

- **Nazwa** – oznaczenie skanowania; może to być nazwa jednego ze [wstępnie zdefiniowanych skanów](#) lub nazwa nadana przez użytkownika jego [skanowi zaplanowanemu](#). Każdej nazwie towarzyszy ikona określająca wynik skanowania:

 – zielona oznacza, że nie wykryto żadnych infekcji;

 – niebieska ikona oznacza, że wykryto infekcję, ale zainfekowany obiekt został automatycznie usunięty.

 – czerwona oznacza, że wykryto infekcję i nie udało się jej usunąć.

Każda z ikon może być widoczna w całości lub „przerwana” – jeśli ikona jest cała, skanowanie zostało prawidłowo ukończony; w przeciwnym

razie skanowanie zostało anulowane lub przerwane.

**Uwaga:** Szczegółowe informacje na temat każdego testu zawiera okno [Wyniki skanowania](#) dostępne po kliknięciu przycisku **Wyświetl szczegóły** (w dolnej części okna).

- **Czas rozpoczęcia** — data i godzina uruchomienia testu.
- **Czas zakończenia** — data i godzina zakończenia skanowania.
- **Przetestowano obiektów** — liczba obiektów sprawdzonych podczas skanowania.
- **Infekcje** — liczba [infekcji wirusowych](#), które zostały wykryte/usunięte.
- **Oprogramowanie szpiegujące** — liczba [programów szpiegujących](#), które zostały wykryte/usunięte.
- **Ostrzeżenia** — liczba wykrytych [podejrzanych obiektów](#)
- **Programy typu rootkit** — liczba wykrytych [programów typu rootkit](#)
  - **Informacji w dzienniku skanowania** — informacje dotyczące przebiegu i wyniku skanowania (zwykle o jego zakończeniu lub przerwaniu).

### Przyciski kontrolne

Przyciski kontrolne dostępne w oknie **Przegląd wyników skanowania** to:

- **Wyświetl szczegóły** — kliknięcie tego przycisku powoduje przełączenie się do okna dialogowego [Wyniki skanowania](#), w którym można przejrzeć szczegółowe dane dotyczące wybranego skanowania.
- **Usun wynik** — kliknięcie tego przycisku powoduje usunięcie wybranej pozycji z przeglądu wyników skanowania.
- **Wstecz** — otwiera ponownie domyślne okno [Interfejsu skanera AVG](#).

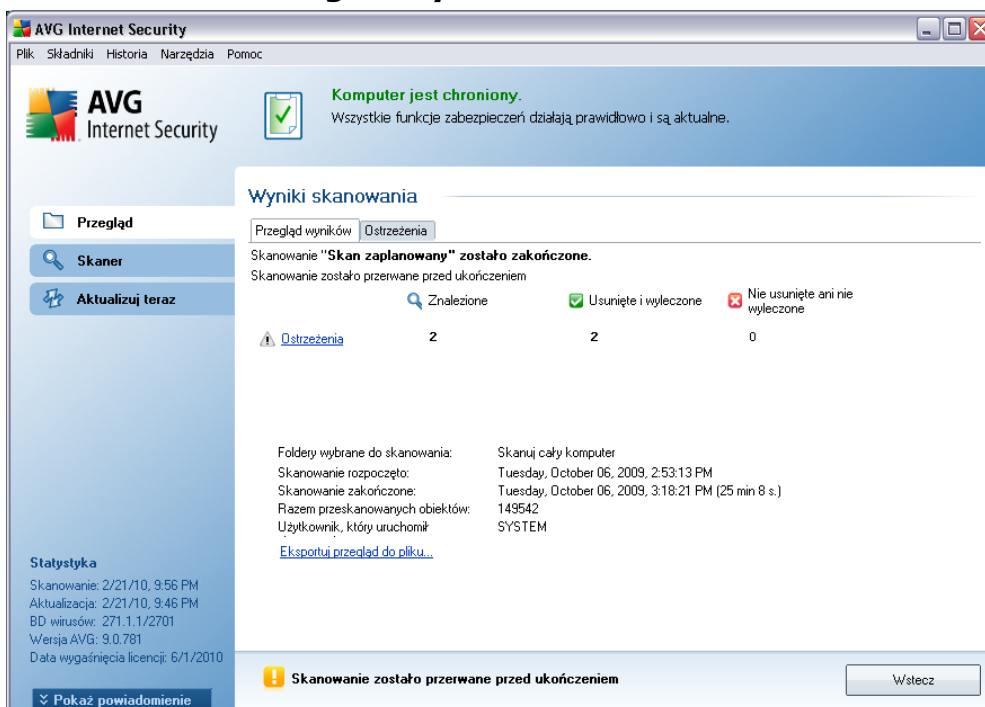
### 12.7. Szczegóły wyników skanowania

Po wybraniu w oknie [Przegląd wyników skanowania](#) któregoś z testów, można kliknąć przycisk **Wyświetl szczegóły**, aby przejść do okna **Wyniki skanowania**, które zawiera dodatkowe informacje o jego przebiegu.

Okno to podzielone jest na kilka kart:


- **[Przegląd wyników](#)** — karta jest zawsze wyświetlana; zawiera statystyki dotyczące przebiegu skanowania.
- **[Infekcje](#)** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto co najmniej jedną [infekcję wirusową](#).
- **[Oprogramowanie szpiegujące](#)** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto [oprogramowanie szpiegujące](#).
- **[Ostrzeżenia](#)** — ta karta jest wyświetlana na przykład, jeśli podczas skanowania wykryto pliki cookie.
- **[Informacje](#)** — karta jest wyświetlana tylko, jeśli w czasie skanowania wykryto potencjalne zagrożenia, których nie można było zakwalifikować do powyższych kategorii; dla każdego znalezionej obiektu wyświetlany jest komunikat ostrzegawczy. Dodatkowo, są tu wyświetlane informacje o obiektach, które nie mogły zostać przeskanowane (np. archiwa chronione hasłem).

### 12.7.1. Karta "Przegląd wyników"



AVG Internet Security


Plik Składniki Historia Narzędzia Pomoc

**AVG Internet Security**  **Komputer jest chroniony.**  
Wszystkie funkcje zabezpieczeń działają prawidłowo i są aktualne.

**Wyniki skanowania**


Przegląd wyników Ostrzeżenia

Skanowanie "**Skan zaplanowany**" zostało zakończone.  
Skanowanie zostało przerwane przed ukończeniem

Znaleziono	Usunięte i wylączone	Nie usunięte ani nie wylączone
 <a href="#">Ostrzeżenia</a> 2	2	0

Foldery wybrane do skanowania: Skanuj cały komputer  
 Skanowanie rozpoczęło: Tuesday, October 06, 2009, 2:53:13 PM  
 Skanowanie zakończone: Tuesday, October 06, 2009, 3:18:21 PM (25 min 8 s.)  
 Razem przeskanowanych obiektów: 149542  
 Użytkownik, który uruchomił: SYSTEM  
[Eksportuj przegląd do pliku...](#)

**Statystyka**  
 Skanowanie: 2/21/10, 9:56 PM  
 Aktualizacja: 2/21/10, 9:46 PM  
 BD wirusów: 271.1.1/2701  
 Wersja AVG: 9.0.781  
 Data wygaśnięcia licencji: 6/1/2010

 **Skanowanie zostało przerwane przed ukończeniem** Wstecz

[Pokaż powiadomienie](#)

Na karcie **Wyniki skanowania** można znaleźć szczegółowe statystyki oraz informacje o:

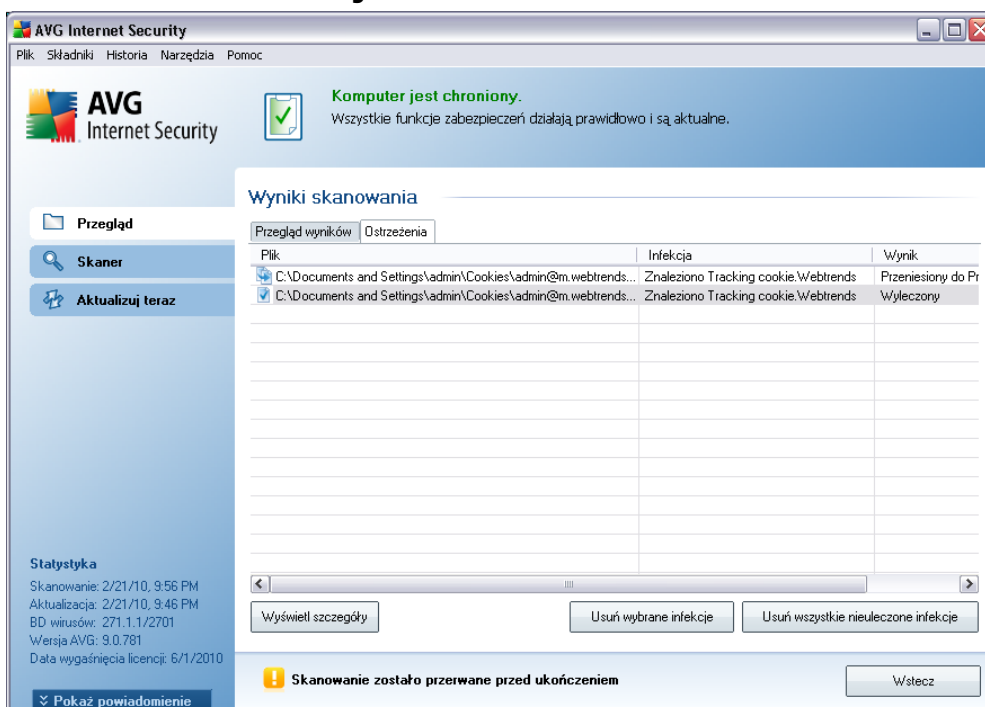
- wykrytych [infekcjach wirusowych/programach szpiegujących](#)
- usuniętych [infekcjach wirusowych/programach szpiegujących](#)
- liczbie [infekcji wirusowych/programów szpiegujących](#), których nie udało się usunąć ani wyleczyć.

Ponadto, znajdują się tu informacje o dacie i dokładnej godzinie uruchomienia testu, łącznej liczbie przeskanowanych obiektów, czasie trwania oraz liczbie napotkanych błędów.

### Przyciski kontrolne

Okno to zawiera tylko jeden przycisk kontrolny. Kliknięcie przycisku **Zamknij wyniki** powoduje powrót do [Przeglądu wyników skanowania](#).

### 12.7.2. Karta "Infekcje"



The screenshot shows the AVG Internet Security interface. At the top, it says "Komputer jest chroniony." (Computer is protected). Below that, the "Wyniki skanowania" (Scan results) section is active. It displays a table with the following data:

Plik	Infekcja	Wynik
C:\Documents and Settings\admin\Cookies\admin@m.webtrends...	Znaleziono Tracking cookie.Webtrends	Przeniesiony do Pr
C:\Documents and Settings\admin\Cookies\admin@m.webtrends...	Znaleziono Tracking cookie.Webtrends	Wyleczony

At the bottom of the window, there is a status bar with a yellow warning icon and the text: "Skanowanie zostało przerwane przed ukończeniem" (Scanning was interrupted before completion). There are also buttons for "Wyświetl szczegóły" (Show details), "Usuń wybrane infekcje" (Remove selected infections), "Usuń wszystkie nieuleczone infekcje" (Remove all unhealed infections), and "Wstecz" (Back).

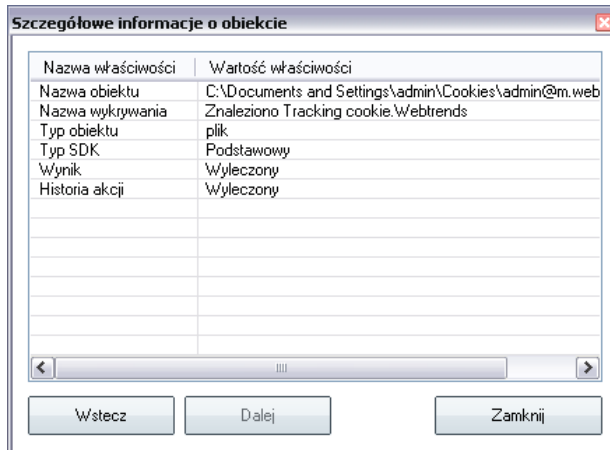
Karta **Infekcje** jest wyświetlana w oknie dialogowym **Wyniki skanowania** tylko, jeśli podczas skanowania wykryto [wirusa](#). Karta jest podzielona na trzy obszary, które zawierają następujące informacje:

- **Plik** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego obiektu.
- **Infekcje** — nazwa wykrytego [wirusa](#) (szczegółowe informacje na temat wirusów zawiera [Encyklopedia Wirusów](#) dostępna online).
- **Wynik** — określa bieżący stan zainfekowanego obiektu, który wykryto podczas skanowania:
  - **Zainfekowany** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (np. jeśli [wylaczono opcje automatycznego leczenia](#) w szczegółowych ustawieniach skanowania).
  - **Wyleczony** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
  - **Przeniesiony do Przechowalni** — zainfekowany obiekt został przeniesiony do [Przechowalni wirusów](#).
  - **Usunięty** — zainfekowany obiekt został usunięty.
  - **Dodany do listy wyjątków PNP** — znaleziony obiekt został uznany za wyjątek i dodany do listy wyjątków PNP (skonfigurowanej w ustawieniach zaawansowanych, w oknie [Wyjątki PNP](#)).
  - **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
  - **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (może na przykład zawierać makra); informacje te należy traktować wyłącznie jako ostrzeżenie.
  - **Wymagany restart systemu** — aby całkowicie usunąć zainfekowany obiekt, należy ponownie uruchomić komputer.

## Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

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



Mozna w nim znaleźć informacje o lokalizacji wykrytego pliku (**Nazwa właściwości**). Za pomocą przycisków **Wstecz / Dalej** można wyświetlać informacje o wybranych znalezionych obiektach. Przycisk **Zamknij** zamyka okno.

- **Usun wybrane infekcje** — pozwala przenieść wybrane obiekty do [Przechowalni wirusów](#).
- **Usun wszystkie niewyleczone pliki** — pozwala usunąć wszystkie znalezione obiekty, których nie można wyleczyć ani przenieść do [Przechowalni wirusów](#).
- **Zamknij wyniki** — powoduje zamknięcie szczegółowych wyników i powrót do okna [Przegląd wyników skanowania](#).

### 12.7.3. Karta "Oprogramowanie szpiegujące"

Karta **Oprogramowanie szpiegujące** jest wyświetlana w oknie dialogowym **Wyniki skanowania** tylko, jeśli podczas skanowania wykryto [oprogramowanie szpiegujące](#). Karta jest podzielona na trzy obszary, które zawierają następujące informacje:

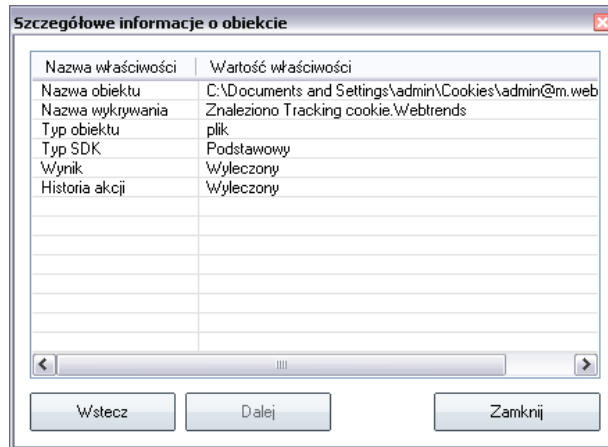
- **Plik** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego obiektu.
- **Infekcje** — nazwa wykrytego [oprogramowania szpiegującego](#) (szczegółowe informacje na temat wirusów zawiera [Encyklopedia Wirusów](#) dostępna online).
- **Wynik** — określa bieżący stan obiektu, który wykryto podczas skanowania:

- **Zainfekowany** — zainfekowany obiekt został wykryty i pozostawiony w oryginalnej lokalizacji (np. jeśli [wylaczono opcje automatycznego leczenia](#) w szczegółowych ustawieniach skanowania).
- **Wyleczony** — zainfekowany obiekt został automatycznie wyleczony i pozostawiony w oryginalnej lokalizacji.
- **Przeniesiony do Przechowalni** — zainfekowany obiekt został przeniesiony do [Przechowalni wirusów](#).
- **Usunięty** — zainfekowany obiekt został usunięty.
- **Dodany do listy wyjątków PNP** — znaleziony obiekt został uznany za wyjątek i dodany do listy wyjątków PNP (*skonfigurowanej w ustawieniach zaawansowanych, w oknie [Wyjątki PNP](#)*).
- **Plik zablokowany - nie testowany** — obiekt jest zablokowany i program AVG nie mógł go przeskanować.
- **Obiekt potencjalnie niebezpieczny** — obiekt został uznany za potencjalnie niebezpieczny, ale nie zainfekowany (może np. zawierać makra); informacja ta jest wyłącznie ostrzeżeniem.
- **Wymagany restart systemu** — aby całkowicie usunąć zainfekowany obiekt, należy ponownie uruchomić komputer.

### Przyciski kontrolne

Okno zawiera trzy przyciski kontrolne:

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

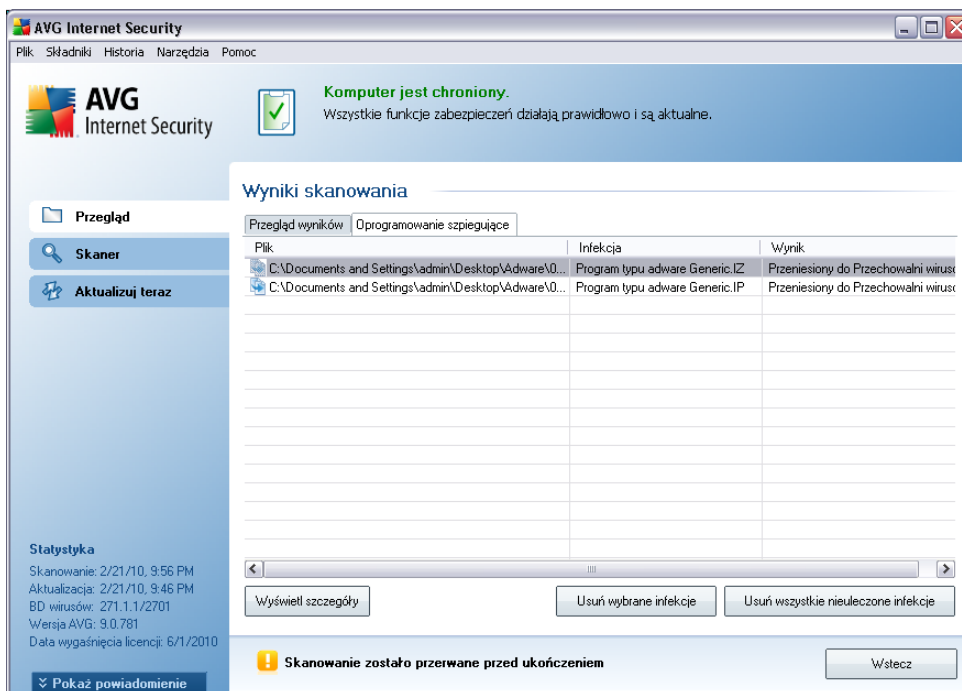


Mozna w nim znaleźć informacje o lokalizacji wykrytego pliku (**Nazwa właściwości**). Za pomocą przycisków **Wstecz** / **Dalej** można wyświetlać informacje o wybranych znalezionych obiektach. Przycisk **Zamknij** zamyka okno.

- **Usun wybrane infekcje** — pozwala przenieść wybrane obiekty do [Przechowalni wirusów](#).
- **Usun wszystkie niewyleczone pliki** — pozwala usunąć wszystkie znalezione obiekty, których nie można wyleczyć ani przenieść do [Przechowalni wirusów](#).
- **Zamknij wyniki** — powoduje zamknięcie szczegółowych wyników i powrót do okna [Przegląd wyników skanowania](#).

#### 12.7.4. Karta "Ostrzeżenia"

Karta **Ostrzeżenia** zawiera informacje o „podejrzanych” obiektach (zwykle *plikach*) wykrytych podczas skanowania. Gdy [Ochrona Rezydentna](#) wykryje takie pliki, zazwyczaj blokuje do nich dostęp. Typowe przykłady obiektów tego typu to: ukryte pliki, cookies, podejrzane klucze rejestru, zabezpieczone hasłem archiwa i dokumenty itp. Pliki te nie stanowią żadnego bezpośredniego zagrożenia dla bezpieczeństwa komputera i użytkownika. Informacje o nich przydatne są jednak w wypadku wykrycia na komputerze oprogramowania reklamowego lub szpiegującego. Jeśli podczas testu AVG pojawiły się tylko ostrzeżenia, nie jest konieczne podejmowanie jakichkolwiek działań.



Oto krótki opis najbardziej popularnych obiektów tego typu:

- **Pliki ukryte** Pliki ukryte są domyślnie niewidoczne dla użytkownika w systemie Windows. Niektóre wirusy mogą próbować uniknąć wykrycia przez wykorzystanie tej właściwości. Jeśli system AVG zgłasza obecność ukrytego pliku, który może być szkodliwy, można przenieść go do [Przechowalni wirusów AVG](#).
- **Pliki cookie** Pliki cookie to pliki tekstowe wykorzystywane przez strony internetowe do przechowywania informacji właściwych dla danego użytkownika. Są one później używane do ładowania witryn internetowych dostosowanych do wymagań użytkownika, itp.
- **Podejrzane klucze rejestru** Niektóre szkodliwe oprogramowanie przechowuje informacje w rejestrze systemu Windows, aby uruchamiać się podczas ładowania systemu lub rozszerzyć zakres swojego działania.

### 12.7.5. Karta "Rootkity"

Karta **Programy typu rootkit** zawiera informacje na temat programów typu rootkit wykrytych podczas skanowania, jeśli uruchomiono **skanowanie składowania Anti-Rootkit** lub dodano te opcje ręcznie do konfiguracji [skanu całego komputera](#) (opcja

jest domyślnie wyłączona).

**Program typu rootkit** to wirus zaprojektowany w celu przejęcia całkowitej kontroli nad systemem komputerowym bez zgody jego właścicieli czy upoważnionych administratorów. Bezpośredni dostęp do sprzętu jest rzadko wymagany, ponieważ programy typu rootkit w pełni zdalnie kontrolują system operacyjny komputera. Zwykle ukrywają one swoją obecność myląc lub unikając standardowych mechanizmów bezpieczeństwa systemu operacyjnego. Wiele z nich jest jednocześnie koniami trojańskimi, które dodatkowo starają się przekonać użytkowników, że ich systemy są bezpieczne. Techniki stosowane przez rootkity to m.in. ukrywanie uruchomionych procesów (przed programami monitorującymi) oraz plików lub danych przed samym systemem operacyjnym.

Struktura tej karty jest w zasadzie taka sama jak kart [Infekcje](#) i [Oprogramowanie szpiegujące](#).

#### 12.7.6. Karta "Informacje"

Karta **Informacje** zawiera dane dotyczące znalezionych obiektów, których nie można zakwalifikować jako infekcje, oprogramowanie szpiegujące itp. Obiektów tych nie można w stu procentach uznać za niebezpieczne, ale często wymagają one uwagi użytkownika. Skaner AVG jest w stanie wykryć pliki, które mogą nie być zainfekowane, ale są podejrzane. Zgłaszane będą one jako **lub** Informacja.

**Informacje** o zagrożeniu mogą być zgłaszane z jednego z następujących powodów:

- **Plik kompresowany w czasie rzeczywistym** - Plik został skompresowany przy użyciu jednego z mniej popularnych programów kompresujących w czasie wykonania, co może wskazywać na próbę uniemożliwienia skanowania takiego pliku. Nie każde zgłoszenie takiego pliku oznacza obecność wirusa.
- **Plik rekurencyjnie kompresowany w czasie rzeczywistym** - Podobny do powyższego, ale rzadziej spotykany wśród zwykłego oprogramowania. Takie pliki są podejrzane i należy rozważyć ich usunięcie lub przesłanie do analizy.
- **Archiwum lub dokument chroniony hasłem** - Pliki chronione hasłem nie mogą być skanowane przez program AVG (*ani generalnie przez żaden inny program chroniący przed szkodliwym oprogramowaniem*).
- **Dokument zawierający makra** — zgłoszone dokumenty zawierają makra, które mogą być szkodliwe.
- **Ukryte rozszerzenie** — pliki z ukrytymi rozszerzeniami mogą udawać np. obrazy, podczas gdy w rzeczywistości są plikami wykonywalnymi (np. "obrazek.jpg.exe"). Drugie rozszerzenie jest w systemie Windows domyślnie niewidoczne.

Program AVG zgłasza takie pliki, aby zapobiec ich przypadkowemu uruchomieniu.

- **Niewłaściwa ścieżka do pliku** — jeżeli jakiś ważny plik systemowy jest uruchamiany z innej ścieżki niż domyślna (np. plik "winlogon.exe" jest uruchamiany z folderu innego niż Windows), system AVG zgłasza tę niezgodność. W niektórych przypadkach wirusy używają nazw standardowych procesów systemowych, aby ich obecność w systemie była trudniejsza do wychwycenia przez użytkownika.
- **Plik zablokowany** — raportowany plik jest zablokowany, dlatego nie może zostać przeskanowany przez system AVG. Oznacza to zazwyczaj, że dany plik jest stale używany przez system (np. plik wymiany).

## 12.8. Przechowywanie wirusów



**Kwarantanna** to bezpieczne środowisko przeznaczone do zarządzania podejrzanymi/zainfekowanymi obiektami, które zostały wykryte podczas testów przeprowadzonych przez AVG. Po wykryciu zainfekowanego obiektu podczas skanowania (w przypadku, gdy AVG nie jest w stanie automatycznie go wyleczyć), użytkownik zostanie poproszony o wybranie reakcji na to zagrożenie. Zalecanym rozwiązaniem jest przeniesienie obiektu do **kwarantanny**, skąd można będzie podjąć dalsze działania związane z analizą, wyleczeniem lub usunięciem pliku. Głównym zadaniem **kwarantanny** jest przechowywanie wszelkich usuniętych plików przez określony czas, aby możliwe było upewnienie się, że plik nie jest wymagany w swojej pierwotnej lokalizacji. Jeśli brak pliku powoduje problemy, można go wysłać wraz z pytaniem do analizy lub przywrócić do pierwotnej lokalizacji.

Interfejs **kwarantanny** jest otwierany w nowym oknie i zawiera przegląd informacji o izolowanych, zainfekowanych obiektach:

- **Zagrożenie** — informacje na temat typu infekcji (zgodnie z ich poziomem zainfekowania — wszystkie obiekty na liście mogą być zainfekowane faktycznie lub potencjalnie).
- **Nazwa wirusa** — nazwa wykrytej infekcji pochodząca z [Encyklopedii wirusów](#) (online).
- **Ścieżka do pliku** — pełna ścieżka do oryginalnej lokalizacji zainfekowanego pliku.

- **Pierwotna nazwa obiektu** — wszystkie wykryte obiekty na liście zostały oznaczone standardowymi nazwami określanymi przez AVG w trakcie skanowania. W przypadku gdy obiekt miał określoną nazwę, która jest znana (np. nazwa załącznika wiadomości e-mail, która nie odpowiada faktycznej zawartości załącznika), jest ona podawana w tej kolumnie.
- **Data zachowania** — data i godzina wykrycia podejrzanego pliku i przeniesienia go do **kwarantanny**.

### Przyciski kontrolne

Interfejs **kwarantanny** zawiera następujące przyciski kontrolne:

- **Przywróć** — przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- **Przywróć jako** — jeśli zainfekowany obiekt ma zostać przeniesiony poza **kwarantannę**, do określonego folderu, ten przycisk pozwala zapisać obiekt z nazwą inną niż pierwotna. Jeśli nazwa pierwotna nie jest znana, użyta zostanie nazwa standardowa.
- **Szczegóły** — ten przycisk może być używany tylko dla zagrożeń wykrytych przez składnik **Identity Protection**. Jego kliknięcie wyświetla porównawczy przegląd szczegółów zagrożeń (*zainfekowane pliki/procesy, charakterystyka procesów itp.*). Należy zwrócić uwagę na fakt, że dla wszystkich pozycji innych niż wykryte przez składnik IDP ten przycisk pozostanie szary i nieaktywny!
- **Usuń** — nieodwracalnie usuwa zainfekowany plik z **kwarantanny**.
- **Opróżnij kwarantannę** — usuwa bezpowrotnie całą zawartość **kwarantanny**. Usunięcie plików z kwarantanny oznacza całkowite i nieodwracalne ich usunięcie z dysku (nie są przenoszone do kosza).

## 13. Aktualizacje AVG

**Zapewnienie aktualności programu AVG jest niezbędne, ponieważ tylko w ten sposób wszystkie nowo pojawiające się wirusy będą wykrywane we właściwym czasie.**

Podczas [procesu instalacji systemu AVG](#) możliwe jest określenie, jak często on ma być aktualizowany. Dostępne opcje to **Co 4 godziny** lub **Codziennie** (zobacz okno dialogowe [Planowanie regularnego skanowania i pobierania aktualizacji](#)). Ponieważ Aktualizacje systemu AVG nie są publikowane zgodnie z jakimkolwiek harmonogramem (powstają jako reakcja na pojawiające się zagrożenia), zalecamy sprawdzanie dostępności aktualizacji przynajmniej raz dziennie. Sprawdzanie co 4 godziny zagwarantuje ciągłą aktualność systemu **AVG 9 Anti-Virus plus Firewall**.

### 13.1. Poziomy aktualizacji

Program AVG oferuje dwa poziomy aktualizacji:

- **Aktualizacja definicji** zawiera uzupełnienia niezbędne do zapewnienia niezawodnej ochrony antywirusowej. Na ogół nie zawiera modyfikacji programu i aktualizuje tylko bazy definicji. Ta aktualizacja powinna zostać zastosowana, gdy tylko będzie dostępna.
- **Aktualizacja programu** zawiera różne zmiany w programie głównym, oraz poprawki i udoskonalenia.

Podczas [planowania aktualizacji](#) można wybrać poziom priorytetu aktualizacji, które mają zostać pobrane i zastosowane.

**Uwaga:** Jeśli zaplanowane skanowanie i zaplanowana aktualizacja nałożą się, proces aktualizacji będzie miał pierwszeństwo i skanowanie zostanie przerwane.

### 13.2. Typy aktualizacji

Mozna wyróżnić dwa typy aktualizacji:

- **Aktualizacja na zadanie** — natychmiastowa aktualizacja oprogramowania AVG, której można dokonać w dowolnym momencie, w razie wystąpienia takiej konieczności.
- **Aktualizacja zaplanowana** — system AVG umożliwia przygotowanie [harmonogramu aktualizacji](#). Aktualizacja zaplanowana jest wykonywana regularnie, zgodnie z ustawioną konfiguracją. Gdy dostępne są nowe pliki aktualizacyjne, AVG pobiera je bezpośrednio z internetu lub katalogu sieciowego. W przypadku braku nowych aktualizacji proces ten kończy się, nie

dokonując żadnych zmian.

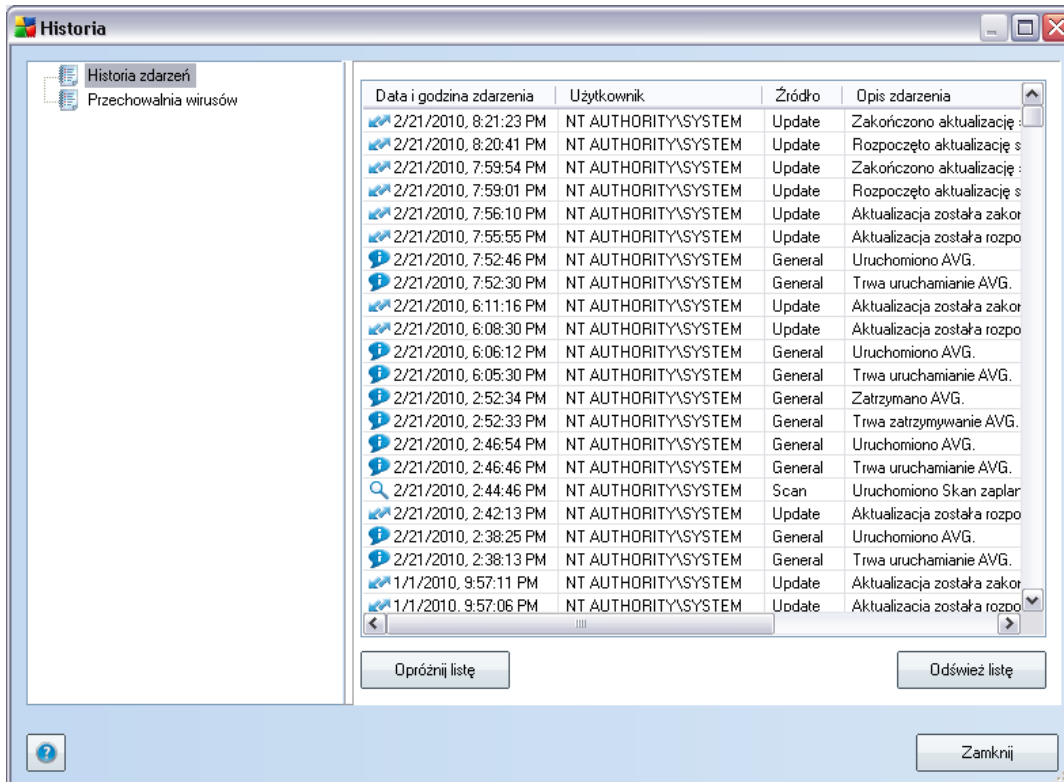
### 13.3. Proces aktualizacji

Proces aktualizacji można uruchomić natychmiast, gdy jest ona potrzebna, klikając szybki link **Aktualizuj teraz\*\*\***. Link ten jest zawsze dostępny w głównym oknie [interfejsu użytkownika AVG](#). Mimo to, zaleca się regularne aktualizowanie systemu, zgodnie z harmonogramem, który można edytować za pomocą [Menedżera aktualizacji](#).

Po uruchomieniu tego procesu program AVG sprawdza, czy dostępne są nowe pliki aktualizacyjne. Jeśli tak, system pobiera je i uruchamia właściwy proces aktualizacji. W tym czasie otwierany jest interfejs **Aktualizacja**, w którym można śledzić przedstawiony graficznie postęp aktualizacji oraz przeglądać szereg parametrów (rozmiar pliku aktualizacji, ilość odebranych danych, szybkość pobierania, czas pobierania itd., ...).

**Uwaga:** Przed zaktualizowaniem programu AVG tworzony jest punkt odtwarzania systemu. Przy jego użyciu możliwe będzie odtworzenie pierwotnego stanu systemu (np. w przypadku niepowodzenia aktualizacji i awarii komputera). Funkcja ta jest dostępna po kolejnym wybraniu opcji: Start / Wszystkie programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoswiadczonej osobom!

## 14. Historia zdarzen



Do interfejsu **Historii zdarzen** można dostać się poprzez [menu główne Historia/ Dziennik historii zdarzen](#). Okno to zawiera podsumowanie najważniejszych wydarzeń, które wystąpiły w czasie pracy systemu **AVG 9 Anti-Virus plus Firewall**. **Dziennik historii zdarzen** zawiera rekordy odpowiadające następującym typom zdarzeń:

- Informacje o aktualizacjach oprogramowania AVG;
- Uruchomienie, zakończenie lub wstrzymanie testu (łącznie z testami wykonywanymi automatycznie);
- Zdarzenia powiązane z wykryciem wirusa (przez [Ochronę Rezydentną](#) lub [podczas zwykłego skanowania](#)), wraz ze wskazaniem lokalizacji zainfekowanego pliku;
- Inne ważne zdarzenia.

### **Przyciski kontrolne**

- **Opróżnij listę** — powoduje usunięcie wszystkich wpisów z listy zdarzeń.
- **Odswież listę** — powoduje odświeżenie zawartości listy zdarzeń.



## 15. FAQ i pomoc techniczna

W przypadku jakichkolwiek problemów z oprogramowaniem AVG (w kwestiach handlowych lub technicznych) należy skorzystać z sekcji **FAQ** witryny systemu AVG (<http://www.avg.com/>).

Jesli pomoc ta okaze sie niewystarczajaca, zalecamy kontakt z dzialem pomocy technicznej za posrednictwem poczty e-mail. Zachecamy do skorzystania z formularza kontaktowego, dostepnego po wybraniu polecenia menu systemowego **Pomoc/ Uzyskaj pomoc online**.