



AVG Internet Security

Podręcznik użytkownika

Wersja dokumentu AVG.05 (17/06/2016)

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



Spis treści

1. Wprowadzenie	3
2. Wymagania instalacyjne systemu AVG	4
2.1 Obsługiwane systemy operacyjne	4
2.2 Minimalne i zalecane wymagania sprzętowe	4
3. Proces instalacji systemu AVG	5
3.1 Witamy!	5
3.2 Wprowadź swój numer licencji	6
3.3 Dostosuj instalację	8
3.4 Instalowanie systemu AVG	9
3.5 Instalacja ukończona	10
4. Po instalacji	11
4.1 Aktualizacja bazy danych wirusów	11
4.2 Rejestracja produktu	11
4.3 Dostęp do interfejsu użytkownika	11
4.4 Skanowanie całego komputera	11
4.5 Test EICAR	11
4.6 Konfiguracja domyślna systemu AVG	12
5. Interfejs użytkownika AVG	13
5.1 Górna sekcja nawigacyjna	14
5.2 Informacje o stanie bezpieczeństwa	17
5.3 Przegląd składników	18
5.4 Moje aplikacje	19
5.5 Szybkie linki Skanuj/Aktualizuj	19
5.6 Ikona w zasobniku systemowym	20
5.7 Doradca AVG	21
5.8 AVG Accelerator	22
6. Składniki AVG	23
6.1 Ochrona komputera	23
6.2 Ochrona przeglądania sieci	26
6.3 Identity Protection	28
6.4 Ochrona poczty email	30
6.5 Zapora	31
6.6 PC Analyser	34
7. Ustawienia zaawansowane AVG	36
7.1 Wygląd	36
7.2 Dźwięki	38
7.3 Tymczasowe wyłączanie ochrony AVG	39
7.4 Ochrona komputera	40



7.5 Skaner poczty e-mail	46
7.6 Ochrona przeglądania sieci	59
7.7 Identity Protection	62
7.8 Skany	63
7.9 Zaplanowane zadania	69
7.10 Aktualizacja	77
7.11 Wyjątki	81
7.12 Przechowalnia wirusów	83
7.13 Ochrona własna AVG	84
7.14 Ustawienia prywatności	84
7.15 Ignoruj błędny stan	86
7.16 Doradca AVG — znane sieci	87
8. Ustawienia Zapory	88
8.1 Ogólne	88
8.2 Aplikacje	90
8.3 Udostępnianie plików i drukarek	91
8.4 Ustawienia zaawansowane	92
8.5 Zdefiniowane sieci	93
8.6 Usługi systemowe	94
8.7 Dzienniki	96
9. Skanowanie AVG	98
9.1 Wstępnie zdefiniowane skany	100
9.2 Skanowanie w Eksploratorze Windows	109
9.3 Skanowanie z wiersza polecenia	109
9.4 Planowanie skanowania	113
9.5 Wyniki skanowania	120
9.6 Szczegóły wyników skanowania	121
10. AVG File Shredder	122
11. Przechowalnia wirusów	123
12. Historia	125
12.1 Wyniki skanowania	125
12.2 Wyniki narzędzia Ochrona rezydentna	126
12.3 Wyniki narzędzia Identity Protection	129
12.4 Wyniki narzędzia Ochrona poczty email	130
12.5 Wyniki narzędzia Ochrona Sieci	131
12.6 Historia zdarzeń	133
12.7 Dziennik Zapory	134
13. Aktualizacje systemu AVG	135
14. Często zadawane pytania i pomoc techniczna	136



1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację użytkownika systemu oprogramowania **AVG Internet Security**.

AVG Internet Security zapewnia wielowarstwową ochronę w każdej sytuacji, co oznacza, że nie musisz się martwić wirusami, kradzieżą danych osobowych ani niebezpiecznymi stronami internetowymi. Otrzymujesz również dostęp do technologii AVG Protective Cloud i Sieci AVG Community Protection Network. Dzięki tym funkcjom zbieramy informacje o najnowszych zagrożeniach i dzielimy się nimi z członkami naszej społeczności, aby każdemu zapewnić jak najlepszą ochronę. Możesz bezpiecznie dokonywać zakupów i korzystać z bankowości online, cieszyć się wycieczkami na portalach społecznościowych, a także przeglądać i przeszukiwać sieć, wiedząc, że masz zapewnioną ochronę w czasie rzeczywistym.

Możesz skorzystać również z innych źródeł informacji:

- **Plik pomocy.** Sekcja *Rozwiązywanie problemów* dostępna jest bezpośrednio w plikach pomocy **AVG Internet Security** (aby otworzyć pomoc, naciśnij klawisz **F1** w dowolnym oknie aplikacji). Zawiera ona listę najczęściej występujących sytuacji, w których użytkownik może potrzebować pomocy. Wybierz sytuację, która najlepiej opisuje Twój problem, aby otworzyć okno ze szczegółowymi instrukcjami jego rozwiązania.
- **Centrum pomocy technicznej na stronie internetowej AVG:** Możesz również poszukać rozwiązania problemu na stronie AVG (<http://www.avg.com/>). W sekcji **Pomoc techniczna** znajduje się tematyczny spis problemów technicznych i handlowych, uporządkowana sekcja z często zadawanymi pytaniami oraz wszystkie dostępne dane kontaktowe.
- **AVG ThreatLabs.** Specjalna strona AVG (<http://www.avg.com/about-viruses>) poświęcona problemom z wirusami i dostępująca uporządkowany przegląd informacji związanych z zagrożeniami w sieci. Znajdziesz tam również instrukcje dotyczące usuwania wirusów i oprogramowania szpiegującego, a także porady dotyczące bezpieczeństwa.
- **Forum dyskusyjne:** Możesz także skorzystać z forum użytkowników oprogramowania AVG, znajdując tego się pod adresem <http://community.avg.com/>.



2. Wymagania instalacyjne systemu AVG

2.1. Obsługiwane systemy operacyjne

Program **AVG Internet Security** jest przeznaczony do ochrony stacji roboczych z następującymi systemami operacyjnymi:

- Windows XP Home Edition z dodatkiem SP3
- Windows XP Professional z dodatkiem SP3
- Windows Vista (wszystkie wersje)
- Windows 7 (wszystkie wersje)
- Windows 8 (wszystkie wersje)
- Windows 10 (wszystkie wersje)

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

2.2. Minimalne i zalecane wymagania sprzętowe

Minimalne wymagania sprzętowe dotyczące oprogramowania **AVG Internet Security**:

- Procesor Intel Pentium 1,5 GHz lub szybszy
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) pamięci RAM
- 1,3 GB wolnego miejsca na dysku *(na potrzeby instalacji)*

Zalecane wymagania sprzętowe dotyczące oprogramowania **AVG Internet Security**:

- Procesor Intel Pentium 1,8 GHz lub szybszy
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) pamięci RAM
- 1,6 GB wolnego miejsca na dysku *(na potrzeby instalacji)*

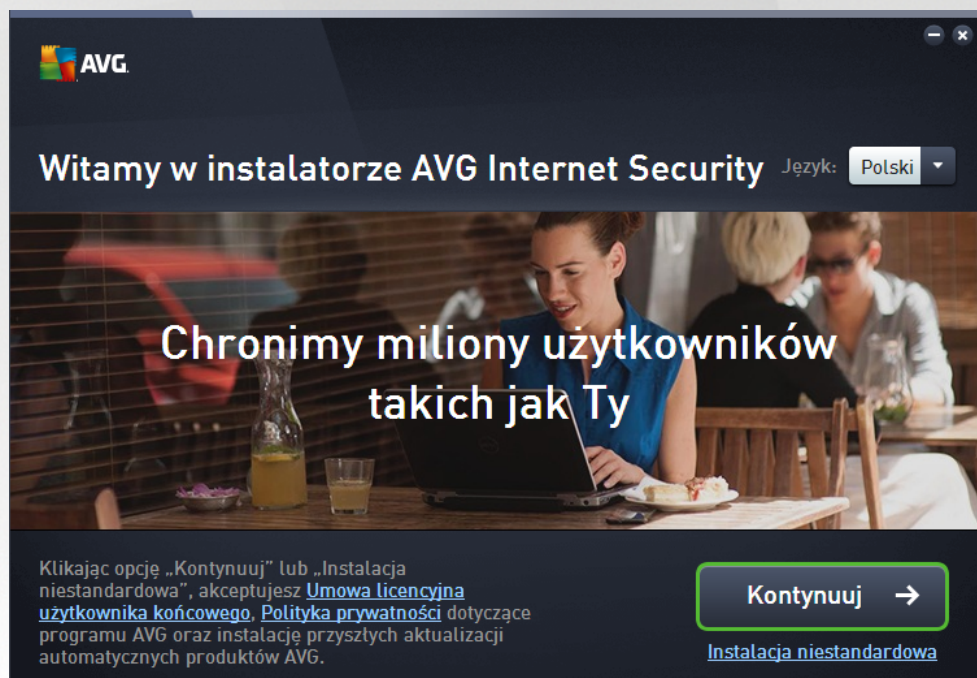


3. Proces instalacji systemu AVG

Do zainstalowania systemu **AVG Internet Security** na komputerze konieczny jest najnowszy plik instalacyjny. Aby upewnić się, że instalujesz najnowszą dostępną wersję **AVG Internet Security**, zalecamy pobranie pliku instalacyjnego bezpośrednio z witryny AVG (<http://www.avg.com/>). Sekcja **Pomoc techniczna** zawiera uporządkowaną listę plików instalacyjnych wszystkich wersji oprogramowania AVG. Po pobraniu i zapisaniu instalatora na dysku można uruchomić proces instalacji. Instalacja składa się z kilku łatwych w zrozumieniu ekranów. Każde z nich opisuje krótko, czego dotyczy. Poniżej znajdziesz szczegółowe opisy poszczególnych okien:

3.1. Witamy!

Proces instalacji rozpoczyna okno **Witamy w programie AVG Internet Security**.



Wybór języka

W tym oknie można wybrać język, który ma być używany podczas instalacji. Kliknij menu rozwijane obok opcji **Język**, aby wyświetlić dostępne języki. Wybierz odpowiedni język, a proces instalacji będzie kontynuowany w tym języku. Również interfejs aplikacji będzie wyświetlany w wybranym języku, z możliwością przełączenia na język angielski, który jest zawsze instalowany domyślnie.

Umowa licencyjna użytkownika końcowego i Polityka prywatności

Przed przejściem do dalszej części procesu instalacji zalecamy zapoznanie się z dokumentami **Umowa licencyjna użytkownika końcowego** i **Polityka prywatności**. Oba dokumenty można otworzyć, korzystając z linków w dolnej części okna dialogowego. Kliknij link, aby wyświetlić nowe okno dialogowe lub nowe okno przeglądarki z pełną treścią wybranego dokumentu. Prosimy o uważne zapoznanie się z tymi prawnymi dokumentami. Klikając przycisk **Kontynuuj**, akceptujesz postanowienia obu dokumentów.



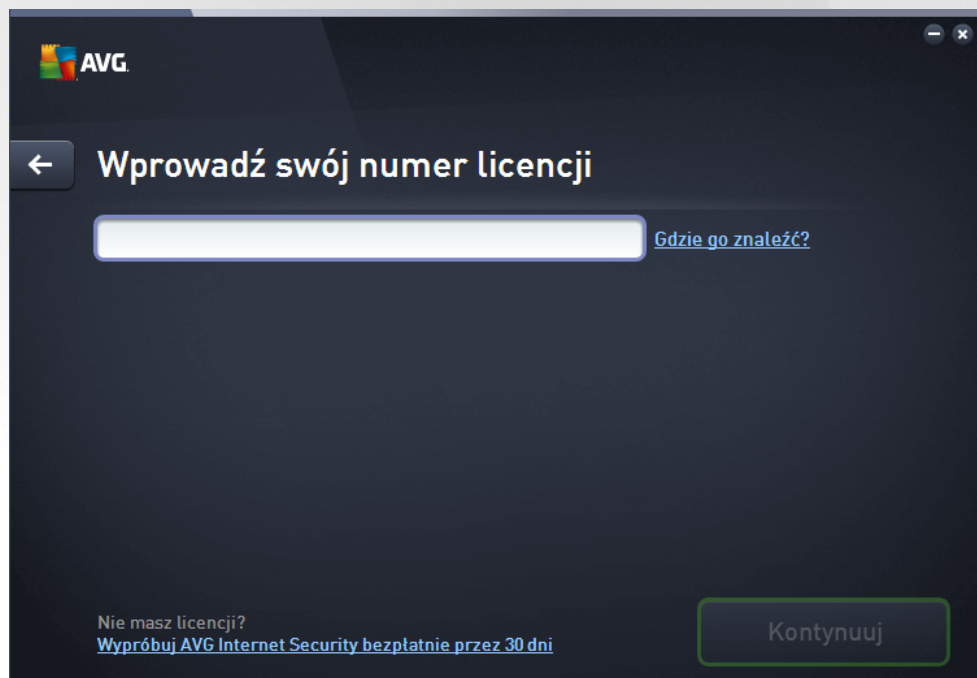
Kontynuowanie instalacji

Aby kontynuować instalację, wystarczy kliknąć przycisk **Kontynuuj**. Zostanie wyświetlona prośba o podanie numeru licencji, po czym proces instalacyjny będzie kontynuowany w trybie automatycznym. W przypadku wątpliwości użytkowników zaleca się skorzystanie z tej standardowej metody instalowania produktu **AVG Internet Security** z ustawieniami określonymi przez dostawcę programu. Taka konfiguracja zapewnia maksymalne bezpieczeństwo oraz optymalne wykorzystanie zasobów. Jeżeli w przyszłości zajdzie potrzeba zmiany konfiguracji, można będzie to zrobić bezpośrednio z poziomu aplikacji.

Istnieje również możliwość przeprowadzenia **Instalacji niestandardowej** poprzez kliknięcie hiperłącza pod przyciskiem **Kontynuuj**. Opcję instalacji niestandardowej powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować systemu z ustawieniami domyślnymi (np. po to, aby dostosować go do specyficznych wymagań systemowych). W przypadku wybrania tej opcji po podaniu numeru licencji zostanie wyświetlone okno dialogowe **Dostosuj instalację**, w którym można określić odpowiednie ustawienia.

3.2. Wprowadź swój numer licencji

W oknie dialogowym **Wprowadź swój numer licencji** możesz aktywować swoją licencję, wpisując jej numer (czyli raczej skopiuj i wklej go) w dostępnym polu tekstowym:



Gdzie znaleźć mój numer licencji?

Numer sprzedaży znajduje się na opakowaniu dysku CD w pudełku z oprogramowaniem **AVG Internet Security**. Numer licencji jest wysyłany pocztą e-mail po zakupieniu oprogramowania **AVG Internet Security** online. Ważne jest dokładne wprowadzenie tego numeru. Jeżeli numer jest dostępny w formie cyfrowej (w wiadomości e-mail), zaleca się skopiowanie go i wklejenie w odpowiednim polu.



Jak użyć metody Kopiuj/wklej

Użycie metody **Kopiuj/wklej** przy wprowadzaniu numeru licencji **AVG Internet Security** pozwala zapewnić poprawne wprowadzenie numeru. Wykonaj następujące kroki:

- Otwórz wiadomość e-mail zawierającą numer licencji.
- Trzymając wciśnięty lewy przycisk myszy, przeciągnij wskaźnik myszy od początku do końca numeru licencji, po czym zwolnij przycisk. Numer powinien teraz być zaznaczony.
- Przytrzymaj klawisz **Ctrl** i naciśnij klawisz **C**. Spowoduje to skopiowanie numeru.
- Wskaż i kliknij miejsce, w którym chcesz wkleić skopiowany numer, czyli pole tekstowe w oknie dialogowym **Wprowadź swój numer licencji**.
- Przytrzymaj klawisz **Ctrl** i naciśnij klawisz **V**. Spowoduje to wklejenie numeru we wskazanym miejscu.

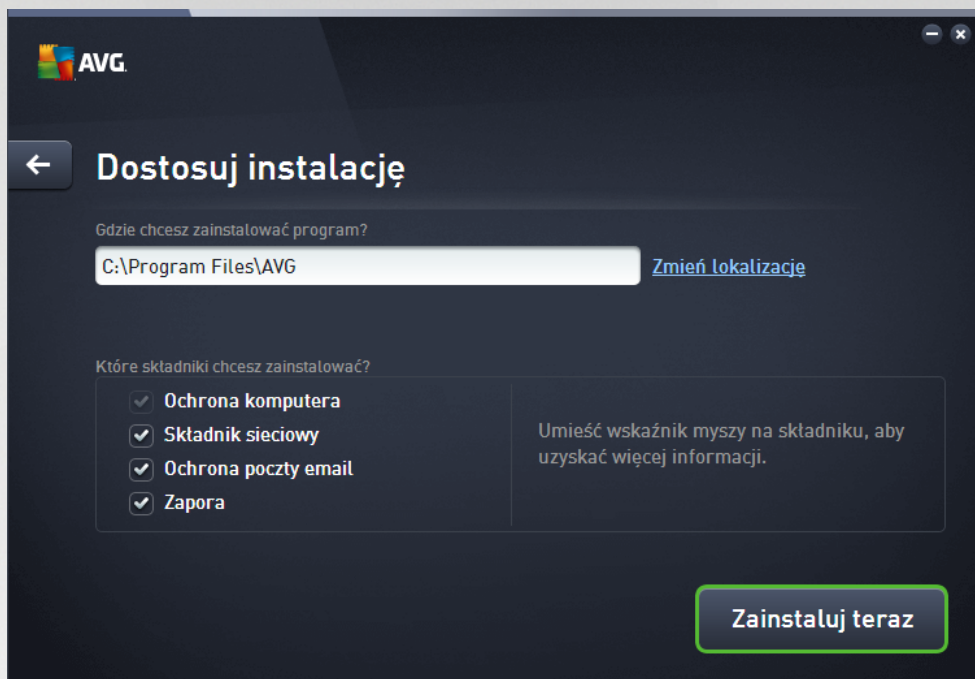
Kontynuowanie instalacji

W dolnej części okna dialogowego znajduje się przycisk **Zainstaluj teraz**. Przycisk zostaje uaktywniony po wprowadzeniu numeru licencji. Po wykonaniu aktywacji kliknij przycisk, aby uruchomić instalację. Jeśli nie masz własnego numeru licencji, możesz zainstalować aplikację **AVG AntiVirus Free Edition**. Niestety wersje bezpłatne nie zawierają wszystkich funkcji dostępnych w pełnej wersji profesjonalnej. Dlatego warto rozważyć odwiedzenie strony internetowej AVG (<http://www.avg.com/>) w celu uzyskania szczegółowych informacji dotyczących zakupu i uaktualnienia oprogramowania AVG.



3.3. Dostosuj instalację

Okno dialogowe *Dostosuj instalację* umożliwia skonfigurowanie szczegółowych parametrów instalacji:



Gdzie chcesz zainstalować aplikację ?

Tutaj możesz wskazać miejsce, w którym chcesz zainstalować aplikację. Adres w polu tekstowym to sugerowana lokalizacja w folderze Program Files. Jeśli wybierzesz inną lokalizację, kliknij link **Zmień lokalizację**, co spowoduje otwarcie nowego okna przedstawiającego strukturę drzewa dysku. Przejdź do odpowiedniej lokalizacji i potwierdź.

Które składniki chcesz zainstalować ?

Ta sekcja udostępnia przegląd wszystkich składników możliwych do zainstalowania. Jeśli ustawienia domyślne nie są odpowiednie dla użytkownika, można usunąć odpowiednie składniki. Wybiera się jednak tylko składniki należące do oprogramowania AVG Internet Security. Jedynym wyjątkiem stanowi składnik **Ochrona komputera** — nie można go wyłączyć z instalacji. Po wybraniu dowolnej pozycji w tej sekcji po prawej stronie zostanie wyświetlony krótki opis odpowiedniego składnika. Szczegółowe informacje o funkcjach poszczególnych składników zawiera rozdział [Przejdź do składników](#) w tej dokumentacji.

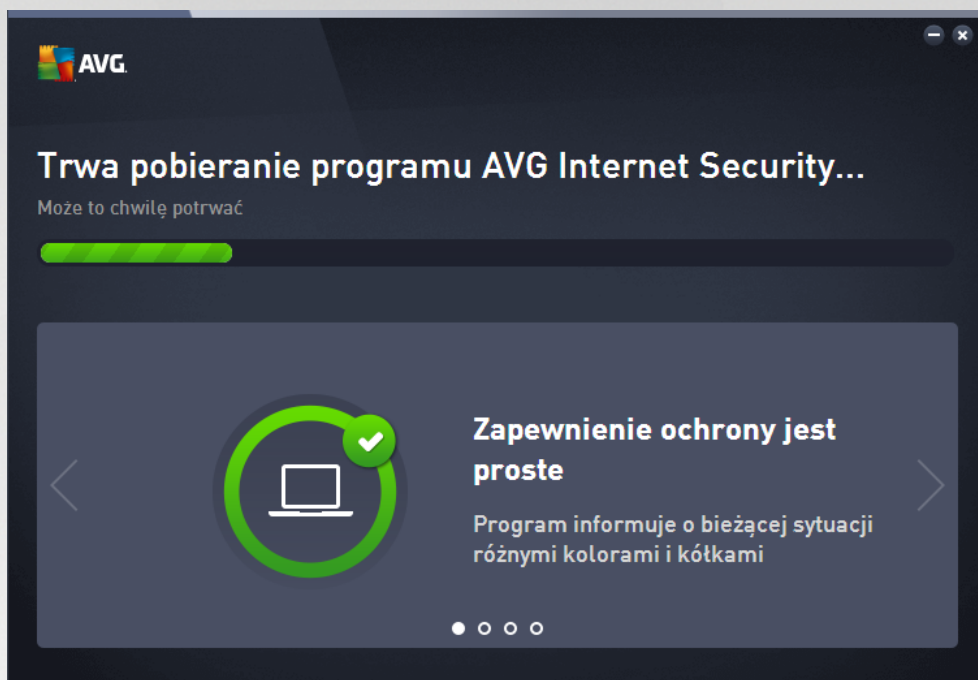
Kontynuowanie instalacji

Aby kontynuować instalację, wystarczy kliknąć przycisk **Zainstaluj teraz**. Alternatywnie, jeśli trzeba zmienić lub zweryfikować ustawienia, można cofnąć się do poprzedniego okna dialogowego za pomocą przycisku strzałki w lewo dostępnego w górnej części tego okna dialogowego.



3.4. Instalowanie systemu AVG

W przypadku potwierdzenia chci uruchomienia instalacji (w poprzednim oknie dialogowym) proces instalacji zostaje uruchomiony automatycznie i nie wymaga działań ze strony użytkownika:

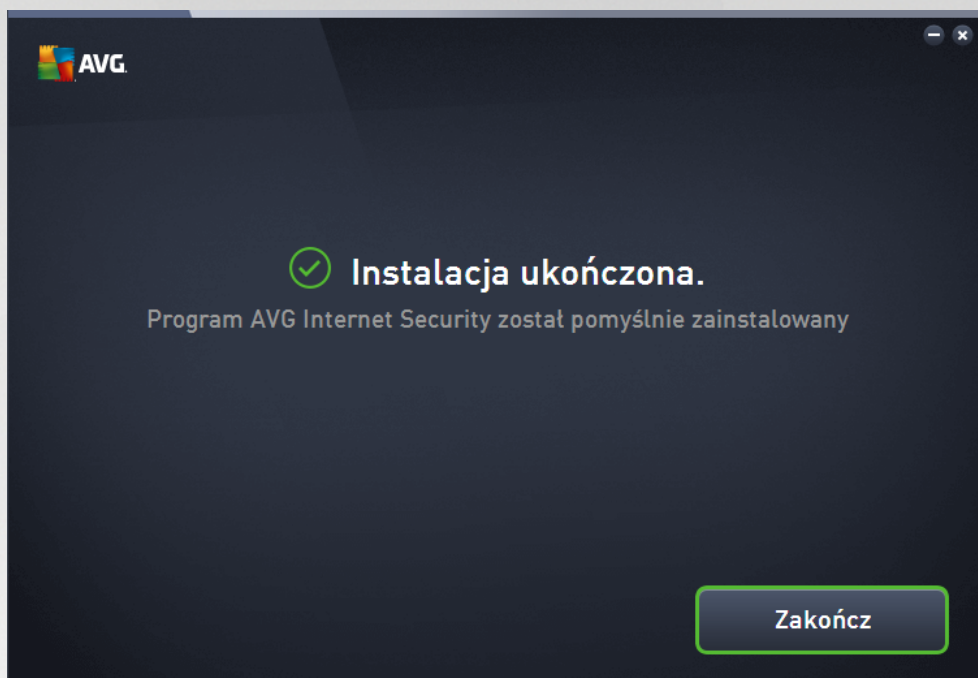


Kiedy proces instalacji zostanie ukończony, nastąpi automatyczne przekierowanie do następnego okna dialogowego.



3.5. Instalacja ukończona

Okno **Instalacja ukończona** potwierdza, że produkt AVG Internet Security został w pełni zainstalowany i skonfigurowany:



Kliknij przycisk **Zakończ**, aby sfinalizować instalację.



4. Po instalacji

4.1. Aktualizacja bazy danych wirusów

Pamiętaj, że po zainstalowaniu (po ponownym uruchomieniu komputera, jeżeli było wymagane) program **AVG Internet Security** automatycznie aktualizuje bazę wirusów i wszystkie składniki, aby przygotować je do pracy, co może potrwać kilka minut. O uruchomieniu procesu aktualizacji poinformuje Cię komunikat wyświetlony w głównym oknie dialogowym. Zaczekaj chwilę na zakończenie procesu aktualizacji, po czym możesz korzystać z ochrony programu **AVG Internet Security**.

4.2. Rejestracja produktu

Po ukończeniu instalacji **AVG Internet Security** zalecamy rejestrację naszego produktu na stronie internetowej AVG (<http://www.avg.com/>). Rejestracja umożliwia pełny dostęp do konta użytkownika AVG, biuletynu aktualizacji AVG i innych usług oferowanych wyłącznie zarejestrowanym klientom. Na stronie rejestracji najprościej jest przejść z poziomu interfejsu użytkownika systemu **AVG Internet Security**. Wybierz z górnej nawigacji pozycję [Opcje / Zarejestruj teraz](#). Zostaniesz wówczas przeniesiony na stronę [Rejestracja](http://www.avg.com/) (<http://www.avg.com/>). Tam znajdziesz dalsze wskazówki.

4.3. Dostęp do interfejsu użytkownika

Dostęp do interfejsu użytkownika AVG możesz uzyskać na kilka sposobów:

- dwukrotnie kliknij ikonę programu AVG Internet Security w zasobniku systemowym
- dwukrotnie kliknij ikonę AVG Protection na pulpicie
- z menu: *Start/Wszystkie programy/AVG/AVG Protection*.

4.4. Skanowanie całego komputera

Istnieje pewne ryzyko, że wirus dostał się do komputera przed zainstalowaniem programu **AVG Internet Security**. Z tego powodu należy uruchomić test [Skan całego komputera](#), aby upewnić się, że jest on w pełni bezpieczny. Pierwsze skanowanie może chwilę potrwać (około godziny), lecz zalecamy uruchomienie go, by uzyskać pewność, że komputer nie jest zainfekowany przez wirusy. Instrukcje dotyczące uruchamiania testu [Skan całego komputera](#) zawiera rozdział [Skanowanie AVG](#).

4.5. Test EICAR

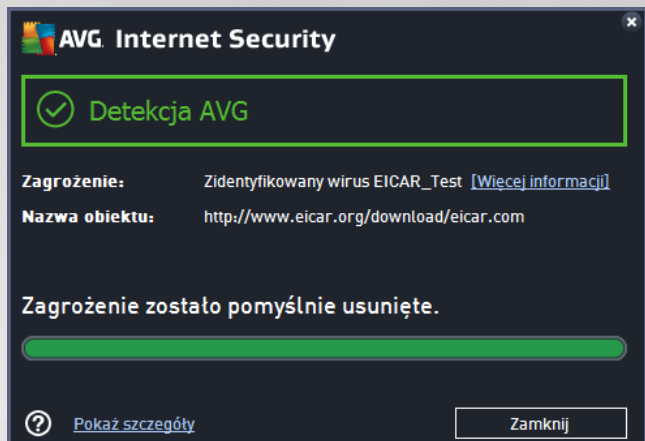
W celu potwierdzenia poprawności instalacji systemu **AVG Internet Security**, możesz wykonać test EICAR.

Test EICAR jest standardową i całkowicie bezpieczną metodą służącą do sprawdzania prawidłowego działania systemu antywirusowego. Można go bezpiecznie rozpowszechniać, ponieważ nie jest prawdziwym wirusem i nie zawiera żadnych fragmentów wirusowego kodu źródłowego. Wirusy rozpoznają go jako wirusa (choć zwykle zgłasza go pod jednoznacznie nazwą, np. „EICAR-AV-Test”). Wirusa EICAR można pobrać z witryny stowarzyszenia EICAR, dostępnej pod adresem www.eicar.com. Można tam również znaleźć wszystkie niezbędne informacje na temat testu EICAR.

Spróbuj pobrać plik [eicar.com](http://www.eicar.com) i zapisać go na dysku twardym komputera. Zaraz po tym, jak potwierdzisz pobranie pliku testowego, oprogramowanie **AVG Internet Security** powinno zareagować, wyświetlając ostrzeżenie. Pojawienie się komunikatu potwierdza, że oprogramowanie AVG jest prawidłowo zainstalowane.



na komputerze.



Je li system AVG nie rozpozna pliku testowego EICAR jako wirusa, nale y ponownie sprawdzi jego konfiguracj !

4.6. Konfiguracja domyślna systemu AVG

Konfiguracja domyślna (ustawienia stosowane zaraz po instalacji) systemu **AVG Internet Security** jest wstępnie definiowana przez producenta i ma na celu zapewnienie optymalnej wydajności wszystkich składników oraz funkcji. **Konfigurację systemu AVG nale y zmienia tylko w uzasadnionych przypadkach! Wszelkie zmiany powinny by wprowadzane wyłącznie przez do wiadczonego u ytkowników.** Je li chcesz precyzyjnie dopasować konfigurację systemu AVG do swoich potrzeb, u yj [Ustawie zaawansowanych AVG](#), wybieraj c z menu głównego *Ustawienia zaawansowane* i edytuj c opcje w nowo otwartym oknie [Ustawienia zaawansowane AVG](#).



5. Interfejs użytkownika AVG

AVG Internet Security zaraz po otwarciu wyświetla główne okno:



Okno główne jest podzielone na kilka sekcji:

- **Górna nawigacja** składa się z czterech linków umieszczonych w górnej sekcji okna głównego (*Więcej od AVG, Raporty, Pomoc, Opcje*). [Szczegóły >>](#)
- **Informacje o stanie bezpieczeństwa** to podstawowe informacje o obecnym stanie Twojego systemu AVG Internet Security. [Szczegóły >>](#)
- **Przebieg zainstalowanych składników** znajduje się na poziomym pasku bloków w środkowej części okna głównego. Składniki widoczne są pod postacią jasnozielonych bloków, oznaczonych ikonami odpowiednich składników i zawierających informacje o ich stanie. [Szczegóły >>](#)
- **Moje aplikacje** przedstawione są na pasku widocznym w dolnej części okna głównego i prezentują przegląd dodatkowych aplikacji AVG Internet Security, które już zostały zainstalowane lub których instalację zalecamy. [Szczegóły >>](#)
- **Szybkie linki Skanuj / Napraw / Aktualizuj** umieszczone są w dolnej linii bloków na głównym ekranie. Przyciski te dają natychmiastowy dostęp do najważniejszych i najczęściej używanych funkcji oprogramowania AVG. [Szczegóły >>](#)

Poza głównym oknem AVG Internet Security istnieje jeszcze jeden element, którego możesz użyć, aby uzyskać dostęp do aplikacji:

- **Ikona w zasobniku systemowym** znajduje się w prawym dolnym rogu ekranu (w zasobniku systemowym) i wskazuje obecny stan programu AVG Internet Security. [Szczegóły >>](#)



5.1. Górna sekcja nawigacyjna

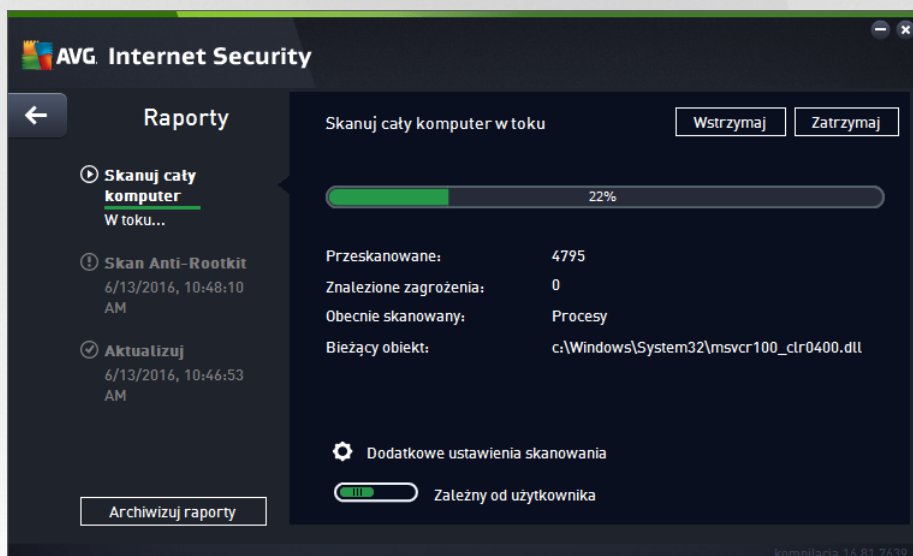
Górna sekcja nawigacyjna składa się z kilku aktywnych linków ułożonych w linii w górnej sekcji głównego okna. Nawigacja możliwa jest dzięki następującym przyciskom:

5.1.1. Więcej od AVG

Kliknij link, aby przejść do witryny AVG i mieć dostęp do wszystkich informacji dotyczących ochrony AVG w zakresie bezpieczeństwa w internecie.

5.1.2. Raporty

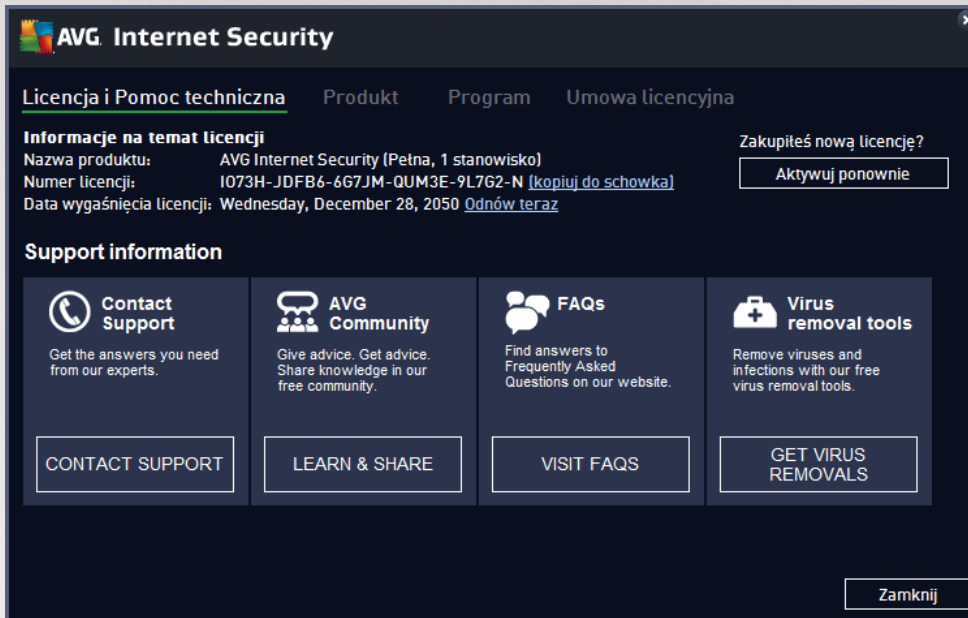
Otwiera nowe okno dialogowe **Raporty** zawierające przegląd wszystkich raportów dotyczących poprzednio uruchomionych procesów skanowania i aktualizacji. Jeżeli skanowanie lub aktualizacja jest w toku, obok tekstu **Raporty** w górnej części nawigacyjnej [głównego interfejsu użytkownika](#) wyświetlona będzie ikona obracającego się kółka. Kliknij ją, aby przejść do okna obrazującego postać uruchomionego procesu:





5.1.3. Pomoc techniczna

Otwiera nowe okno podzielone na cztery karty, w którym można znaleźć wszystkie potrzebne informacje o programie **AVG Internet Security**:



- **Licencja i Pomoc techniczna** — ta karta zawiera informacje o nazwie produktu, numerze licencji i dacie jej wygaśnięcia. W dolnej części okna znajduje się przegląd wszystkich dostępnych sposobów kontaktu z działem obsługi klienta. Na tej karcie dostępne są następujące linki i przyciski:
 - **Aktywuj (ponownie)** — kliknij, aby otworzyć nowe okno **Aktywuj oprogramowanie AVG**. Wprowadzenie w nim nowego numeru licencji umożliwia zastąpienie numeru sprzedanej (używanego podczas instalacji **AVG Internet Security**) lub zmianę numeru licencji na inny (np. przy uaktualnieniu do wyzszej wersji systemu **AVG**).
 - **Kopiuj do schowka** — użyj tego linku, aby skopiować numer licencji, a następnie wkleić go w danym miejscu. W ten sposób będziesz mieć pewność, że numer licencji został wpisany poprawnie.
 - **Odnów teraz** — zalecamy odnowienie licencji programu **AVG Internet Security** z wyprzedzeniem, co najmniej na miesiąc przed wygaśnięciem aktualnej. Użytkownik zostanie powiadomiony o zbliżającym się dacie wygaśnięcia licencji. Kliknij ten link, aby przejść do witryny **AVG** (<http://www.avg.com/>), w której znajdziesz szczegółowe informacje o stanie swojej licencji, jej dacie wygaśnięcia i ofercie odnowienia/uaktualnienia.
- **Produkt** — ta karta zawiera przegląd najważniejszych informacji technicznych **AVG Internet Security** o produkcie AV, zainstalowanych składnikach i zainstalowanej ochronie poczty e-mail.
- **Program** — ta karta zawiera szczegółowe informacje techniczne dotyczące zainstalowanego oprogramowania **AVG Internet Security**, takie jak numer głównej wersji produktu oraz listy numerów wersji wszystkich produktów pokrewnych (np. *Zen*, *PC TuneUp*). Na karcie tej znajduje się także przegląd wszystkich zainstalowanych składników oraz określone informacje dotyczące zabezpieczeń (numer wersji bazy danych wirusów, narzędzi *Link Scanner* i *Anti-Spam*).



- **Umowa licencyjna** — ta karta zawiera pełną treść umowy licencyjnej zawartej z firmą AVG Technologies.

5.1.4. Opcje

Funkcje obsługi systemu **AVG Internet Security** dostępne są w sekcji **Opcje**. Kliknij strzałkę, by otworzyć menu rozwijane:

- Opcja **[Skanuj komputer](#)** uruchamia skanowanie całego komputera.
- **[Skanuj wybrany folder](#)** — przełącza do interfejsu skanowania AVG i umożliwia wskazanie plików oraz folderów, które mają zostać przeskanowane.
- **[Skanuj plik](#)** — pozwala przetestować na danie pojedynczy plik. Wybranie tej opcji powoduje otwarcie nowego okna przedstawiającego strukturę dysku w postaci drzewa. Wskaźnik dany plik i potwierdź rozpoczęcie skanowania.
- **[Aktualizuj](#)** — automatycznie uruchamia proces aktualizacji oprogramowania **AVG Internet Security**.
- **[Aktualizuj z katalogu](#)** — uruchamia proces aktualizacji, korzystając z pliku zlokalizowanego w określonym folderze na dysku lokalnym. Jednak ta opcja jest zalecana do użycia 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 wskaźnik folder, w którym został wcześniej zapisany plik aktualizacji, a następnie uruchom proces aktualizacji.
- **[Przechowalnia wirusów](#)** — otwiera interfejs obszaru kwarantanny (Przechowalni wirusów), do którego trafiają wszystkie zainfekowane obiekty wykryte i usunięte przez oprogramowanie AVG. W czasie tej kwarantanny zainfekowane pliki są izolowane i nie zagrażają bezpieczeństwu komputera, a jednocześnie nie istnieje możliwość ich naprawy w przyszłości.
- **[Historia](#)** — udostępnia dalsze opcje podmenu:
 - **[Wyniki skanowania](#)** — otwiera okno dialogowe zawierające przegląd wyników skanowania.
 - **[Wyniki narzędzia Ochrona rezydentna](#)** — otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez Ochronę rezydentną.
 - **[Wyniki narzędzia Identity Protection](#)** — otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez składnik **[To samo](#)**.
 - **[Wyniki narzędzia Ochrona poczty e-mail](#)** — otwiera okno dialogowe zawierające przegląd zagrożeń z czynnikiem uznanych przez Ochronę poczty e-mail za niebezpieczne.
 - **[Wyniki narzędzia Ochrona Sieci](#)** — otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez Ochronę Sieci.
 - **[Dziennik historii zdarzeń](#)** — otwiera interfejs dziennika historii z przeglądem wszystkich zarejestrowanych akcji **AVG Internet Security**.
 - **[Dziennik Zapory](#)** — otwiera okno zawierające szczegółowy przegląd wszystkich akcji Zapory.



- **Ustawienia zaawansowane** — otwiera okno dialogowe Ustawienia zaawansowane AVG, w którym można edytować konfigurację **AVG Internet Security**. Na ogół zaleca się zachowanie domyślnych ustawień aplikacji zdefiniowanych przez producenta oprogramowania.
- **Ustawienia Zapory** — otwiera okno zaawansowanej konfiguracji składnika Zapora.
- **Spis treści** — otwiera pliki pomocy AVG.
- **Uzyskaj pomoc techniczną** — otwiera [okno dialogowe pomocy technicznej](#) zawierające wszystkie dostępne informacje kontaktowe i dane dotyczące pomocy technicznej.
- **AVG — Twoje WWW** — otwiera stronę internetową AVG (<http://www.avg.com/>).
- **Informacje o wirusach i zagrożeniach** — otwiera internetową encyklopedię wirusów na stronie AVG (<http://www.avg.com/>), gdzie znaleźć można szczegółowe informacje o znanych wirusach.
- **Aktywuj (ponownie)** — otwiera okno dialogowe aktywacji z numerem licencji podanym podczas procesu instalacji. W oknie tym można edytować numer licencji w celu zastąpienia numeru sprzedawcy (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*). W przypadku korzystania z próbnej wersji oprogramowania **AVG Internet Security** ostatnie dwie pozycje to **Kup teraz** i **Aktywuj**. Umożliwiają one kupienie programu w pełnej wersji. W przypadku oprogramowania **AVG Internet Security** zainstalowanego z numerem sprzedawcy, te pozycje to **Zarejestruj** i **Aktywuj**.
- **Zarejestruj teraz/MyAccount** — powoduje przejście do strony rejestracyjnej oprogramowania AVG (<http://www.avg.com/>). Należy tam podać swoje dane rejestracyjne. Tylko klienci, którzy zarejestrowali swój produkt AVG, mogą korzystać z bezpłatnej pomocy technicznej.
- **Informacje o AVG** — otwiera nowe okno dialogowe zawierające cztery karty z informacjami o kupionej licencji i dostępnej pomocy, produkcie oraz programie, a także pełny tekst umowy licencyjnej. (*To samo okno dialogowe można otworzyć, klikając w przycisk Pomoc techniczna w głównym panelu nawigacji*).

5.2. Informacje o stanie bezpieczeństwa

Sekcja **Informacje o stanie bezpieczeństwa** znajduje się w górnej części głównego okna programu **AVG Internet Security**. Znajdziesz tam informacje o bieżącym stanie bezpieczeństwa systemu **AVG Internet Security**. W obszarze tym mogą być wyświetlane następujące ikony:



— zielona ikona wskazuje, że system **AVG Internet Security** jest w pełni funkcjonalny. Komputer jest całkowicie chroniony, bazy danych są aktualne, a wszystkie zainstalowane składniki działają prawidłowo.



— żółta ikona oznacza, że **co najmniej jeden składnik jest nieprawidłowo skonfigurowany**; należy sprawdzić jego właściwości i ustawienia. W systemie **AVG Internet Security** nie wystąpił jednak żaden problem krytyczny, a użytkownik prawdopodobnie wyłączył z jakiegoś powodu jeden lub więcej składników. Komputer nadal jest chroniony. Należy jednak sprawdzić ustawienia składnika, który zgłasza problem. Błędnie skonfigurowany składnik będzie oznaczony pomarańczowym paskiem w [głównym interfejsie użytkownika](#).

Żółta ikona jest wyświetlana również wtedy, gdy z jakiegoś powodu zignorujesz błądny stan dowolnego



ze składników. Opcja **Ignoruj bł dny stan** jest dostępna w gałęzi [Ustawienia zaawansowane / Ignoruj bł dny stan](#). Masz możliwość potwierdzenia, że zdajesz sobie sprawę z błędnego stanu składnika, ale z pewnych powodów chcesz pozostawić system **AVG Internet Security** w tym stanie i nie chcesz już otrzymywać więcej ostrzeżeń na ten temat. W pewnych sytuacjach użycie tej opcji może być pomocne, jednak zalecamy wyłączenie opcji **Ignorowania błędnego stanu** tak szybko, jak to będzie możliwe.

Oprócz tego również ikona będzie wyświetlana, gdy Twój system **AVG Internet Security** wymaga ponownego uruchomienia komputera (**Wymagane ponowne uruchomienie**). Warto zwrócić uwagę na to ostrzeżenie i ponownie uruchomić komputer.



— pomarańczowa ikona wskazuje na krytyczny stan systemu **AVG Internet Security**. Co najmniej jeden składnik nie działa i system **AVG Internet Security** nie może chronić komputera. Należy natychmiast rozwiązać zgłoszony problem. Jeśli nie jest to możliwe, należy skontaktować się z zespołem [Pomocy technicznej AVG](#).

Jeśli system **AVG Internet Security** wykryje, że nie działa z optymalną wydajnością, obok informacji o stanie zostanie wyświetlony przycisk **Kliknij, aby naprawić problem** (lub **Kliknij, aby naprawić wszystko, jeśli problem dotyczy kilku składników**). Kliknij ten przycisk, aby rozpocząć automatyczny proces sprawdzenia i konfigurowania programu. Jest to prosty sposób na osiągnięcie optymalnej wydajności systemu **AVG Internet Security** oraz maksymalnego poziomu bezpieczeństwa.

Stanowczo zaleca się reagowanie na zmiany **Stanu bezpieczeństwa** i natychmiastowe rozwiązanie ewentualnych problemów. Brak reakcji narazi komputer na poważne zagrożenia.

Uwaga: Informacje o stanie systemu **AVG Internet Security** można również uzyskać w dowolnym momencie z poziomu [ikony na pasku zadań](#).

5.3. Przegląd składników

Przegląd zainstalowanych składników znajduje się na poziomym pasku bloków w rodkowej części [okna głównego](#). Składniki wyświetlane są pod postacią jasnozielonych bloków oznaczonych ikonami odpowiednich składników. Każdy blok zawiera również informacje o bieżącym stanie ochrony. Jeśli składnik jest skonfigurowany poprawnie i w pełni działa, informacja będzie miała kolor zielony. Jeśli składnik jest zatrzymany, jego funkcjonalność jest ograniczona lub znajduje się w stanie błędny, zostanie wyświetlone ostrzeżenie: tekst w kolorze pomarańczowym. **Zalecamy wówczas zwrócenie szczególnej uwagi na ustawienia danego składnika.**

Umieść kursor myszy nad składnikiem, aby wyświetlić krótki tekst w dolnej części [okna głównego](#). Tekst ten stanowi wprowadzenie do funkcjonalności danego składnika. Informuje również o bieżącym stanie składnika, a także wskazuje, która usługa składnika nie jest poprawnie skonfigurowana.

Lista zainstalowanych składników

W systemie **AVG Internet Security** sekcja **Przegląd składników** zawiera informacje o następujących składnikach:

- **Komputer** — ten składnik obejmuje dwie usługi: **Ochrona antywirusowa** wykrywa wirusy, oprogramowanie szpiegujące, robaki, konie trojańskie, niepożądane pliki wykonywalne lub biblioteki i chroni przed szkodliwym oprogramowaniem reklamowym, natomiast **Anti-Rootkit** skanuje aplikacje, sterowniki i biblioteki w poszukiwaniu rootkitów. [Szczegóły >>](#)



- **Przeł danie sieci** — chroni przed zagrożeniami internetowymi, kiedy surfujesz po internecie. [Szczegóły >>](#)
- **To samo** — ten składnik uruchamia usługę **Identity Shield**, która stale chroni Twoje cyfrowe zasoby przed nowymi, nieznanymi zagrożeniami z internetu. [Szczegóły >>](#)
- **E-mail** — sprawdza przychodzące wiadomości e-mail w poszukiwaniu spamu, blokuje wirusy, próby phishingu i inne zagrożenia. [Szczegóły >>](#)
- **Zapora** — kontroluje całą komunikację na wszystkich portach sieciowych, chroni komputer przed atakami oraz blokuje wszelkich intruzów. [Szczegóły >>](#)

Dostępne akcje

- **Umieść kursor nad ikoną dowolnego składnika**, aby ją zaznaczyć w ramach przeglądu tego składnika. Jednocześnie u dołu [interfejsu użytkownika](#) zostanie wyświetlony opis funkcji wybranego składnika.
- **Pojedyncze kliknięcie ikony składnika** pozwala otworzyć jego interfejs użytkownika, który zawiera informacje o jego bieżącym stanie i daje dostęp do konfiguracji oraz statystyk.

5.4. Moje aplikacje

W obszarze **Moje aplikacje** (pasek zielonych bloków pod zbiorom składników) znajduje się przegląd dodatkowych aplikacji AVG, które są już zainstalowane lub których instalacja jest zalecana. Bloki te są wyświetlane zależnie od systemu i mogą reprezentować następujące aplikacje:

- **Ochrona mobilna** to aplikacja chroniąca Twój telefon komórkowy przed wirusami i złośliwym oprogramowaniem. Daje również możliwość zdalnego sterowania swoim telefonem, jeżeli kiedykolwiek go utracisz.
- Aplikacja **PC TuneUp** jest zaawansowanym narzędziem analizującym stan systemu i umożliwia ci zwiększenie szybkości i wydajności komputera.

Szczegółowe informacje na temat każdej aplikacji z sekcji **Moje aplikacje** są dostępne po kliknięciu odpowiedniego bloku. Następnie wówczas przejdziesz do dedykowanej strony AVG, na której będzie również możliwe natychmiastowe pobranie danego składnika.

5.5. Szybkie linki Skanuj/Aktualizuj

Szybkie linki znajdują się w dolnej części [interfejsu użytkownika programu AVG Internet Security](#).

Pozwalają one uzyskać natychmiastowy dostęp do najważniejszych i najczęściej używanych funkcji aplikacji, czyli skanowania i aktualizacji. Szybkie linki dostępne są z poziomu dowolnego okna interfejsu:

- **Skanuj teraz** — przycisk ten jest graficznie podzielony na dwie części. Użyj linku **Skanuj teraz**, aby natychmiast uruchomić [skanowanie całego komputera](#) i obserwować jego postęp oraz wyniki w otwartym oknie [Raporty](#). Przycisk **Opcje** służy do otwierania okna **Opcje skanowania**, które pozwala [zarządzić zaplanowanymi skanami](#) oraz edytować parametry [Skanu całego komputera / Skanu określonych plików lub folderów](#). (Szczegóły można znaleźć w rozdziale [Skanowanie AVG](#))
- **Popraw wydajność** — ten przycisk umożliwia dostęp do usługi [PC Analyzer](#), zaawansowanego







narzędzia przeznaczonego do szczegółowej analizy i modyfikacji ustawień systemu w celu zwiększenia szybkości i efektywności działania komputera.

- **Aktualizuj teraz** — użycie tego przycisku, aby natychmiast uruchomić aktualizację produktu. Informacje o wynikach aktualizacji zostaną wyświetlone w wysuwanym oknie nad ikoną AVG w zasobniku systemowym. (Szczegóły można znaleźć w rozdziale [Aktualizacje AVG](#))

5.6. Ikona w zasobniku systemowym

Ikona AVG w zasobniku systemowym (na pasku systemu Windows, w prawym dolnym rogu ekranu) wyświetla bieżący stan oprogramowania **AVG Internet Security**. Ikona ta jest zawsze widoczna, niezależnie od tego, czy [interfejs użytkownika AVG Internet Security](#) jest otwarty, czy zamknięty:

Ikona AVG w zasobniku systemowym

-  Jeśli ikona jest kolorowa i nie zawiera żadnych dodatków, oznacza to, że wszystkie składniki systemu **AVG Internet Security** są aktywne i w pełni funkcjonalne. Może ona być kolorowa także wtedy, gdy system AVG zasignalizował błąd, ale użytkownik akceptuje je i celowo [ignoruje stan składników](#). (Korzystając z opcji ignorowania stanu składników, potwierdzasz, że wiesz o [nieprawidłowym stanie składnika](#), ale z pewnych powodów nie chcesz przywrócić go do normalnego działania).
-  Ikona z wykrzyknikiem oznacza, że jeden składnik (lub więcej składników) jest w [stanie błędny](#). Zawsze bacznie obserwuj takie sytuacje i spróbuj przywrócić poprawną konfigurację odpowiednich składników. W tym celu wystarczy kliknąć dwukrotnie ikonę w zasobniku systemowym, co spowoduje otwarcie [interfejsu użytkownika aplikacji](#) i umożliwi wprowadzenie zmian. Szczegóły na temat składników, których dotyczy [stan błędny](#) systemu można znaleźć w sekcji [Informacje o stanie bezpieczeństwa](#).
-  Kolorowej ikonie na pasku zadań może towarzyszyć wirujący promień światła. Taki wygląd ikony oznacza, że właśnie uruchomiono proces aktualizacji.
-  Kolorowa ikona z białą strzałką oznacza, że przeprowadzany jest jeden ze skanów programu **AVG Internet Security**.

Informacje ikony w zasobniku systemowym

Ikona AVG w zasobniku systemowym informuje także o bieżących działaniach w programie **AVG Internet Security** oraz możliwych zmianach stanu programu (np. *automatycznym uruchomieniu zaplanowanego skanowania lub aktualizacji, przełączeniu profilu Zapory, zmianie stanu składnika, wystąpieniu stanu błędny*) przy użyciu wyskakującego okienka otwieranego z poziomu ikony w zasobniku systemowym.

Akcje dostępne z poziomu ikony w zasobniku systemowym

Ikona AVG w zasobniku systemowym może być używana do szybkiego uruchomienia [interfejsu użytkownika programu AVG Internet Security](#) (wystarczy dwukrotnie kliknąć w nią). Kliknięcie ikony prawym przyciskiem myszy powoduje otwarcie menu kontekstowego zawierającego następujące opcje:



- **Otwórz program AVG** — kliknij, aby otworzyć [interfejs użytkownika](#) programu **AVG Internet Security**.
- **Tymczasowo wyłóż ochronę AVG** — ta opcja pozwala natychmiast wyłączyć wszelką ochronę zapewnianą przez system **AVG Internet Security**. Pamiętaj, że tej opcji nie powinno się używać, chyba że jest to absolutnie konieczne. W większości przypadków nie jest konieczne wyłączenie oprogramowania **AVG Internet Security** przed zainstalowaniem nowego oprogramowania lub sterowników, nawet jeśli instalator lub kreator sugeruje uprzednie zamknięcie działających programów i aplikacji, aby proces instalacji przebiegał bez zakłóceń. Jeśli jednak tymczasowe wyłączenie oprogramowania **AVG Internet Security** jest konieczne, należy je włączyć ponownie, gdy tylko będzie to możliwe. Jeśli oprogramowanie antywirusowe jest wyłączone, komputer podłączony do Internetu jest narażony na ataki, przed którymi nie będzie chroniony.
- **Skanuj** — kliknięcie tej opcji powoduje otwarcie menu kontekstowego zawierającego [predefiniowane skany](#) ([Skan całego komputera](#) i [Skan wybranych plików/folderów](#)) i umożliwia natychmiastowe uruchomienie dowolnego z nich.
- **Zapora** — kliknięcie powoduje otwarcie menu kontekstowego umożliwiającego szybki dostęp do wszystkich [dostępnych trybów Zapory](#). Zmiana obecnie ustawionego trybu Zapory nastąpi po wybraniu go z menu i potwierdzeniu kliknięciem.
- **Uruchomione skany** — ten element jest wyświetlany tylko w przypadku, gdy na komputerze jest aktualnie uruchomione skanowanie. Istnieje możliwość ustawienia priorytetu uruchomionego skanu, zatrzymania skanowania lub wstrzymania go. Dostępne są również następujące akcje: *Ustaw priorytet dla wszystkich skanowań*, *Wstrzymaj wszystkie skanowania* lub *Zatrzymaj wszystkie skanowania*.
- **Popraw wydajność** — kliknij, aby uruchomić składnik [PC Analyzer](#).
- **Zaloguj się do konta AVG MyAccount** — otwiera stronę główną AVG MyAccount umożliwiającą zarządzanie subskrypcjami produktów, zakup dodatkowej ochrony, pobranie plików instalacyjnych, sprawdzenie złożonych zamówień i faktur, a także zarządzanie danymi osobowymi.
- **Aktualizuj teraz** — uruchamia natychmiastowo [aktualizację](#).
- **Pomoc** — otwiera plik pomocy na stronie startowej.

5.7. Doradca AVG

Doradca AVG został opracowany po to, aby wykrywać problemy (które mogą stwarzać zagrożenie dla komputera) oraz proponować ich rozwiązania. **Doradca AVG** widoczny jest w postaci powiadomienia wysuwanego nad zasobnikiem systemowym. Usługa ta wykrywa **nieznane sieci o znanej nazwie**. Dotyczy to zazwyczaj jedynie użytkowników, którzy korzystają z różnych sieci na swoich komputerach przenośnych: Jeśli nowa, nieznaną sieć będzie miała podobną nazwę do dobrze znanej (np. *Dom lub MojeWiFi*), może przez przypadek połączyć się z potencjalnie niebezpieczną siecią. **Doradca AVG** może Cię przed tym uchronić, ostrzegając, że pod zaufaną nazwą kryje się nieznaną sieć. Jeśli stwierdzisz, że nowa sieć jest bezpieczna, oczywiście możesz zachować ją na prowadzonej przez **Doradcę AVG** liście znanych sieci, aby w przyszłości ci nie była już ona zgłaszana.

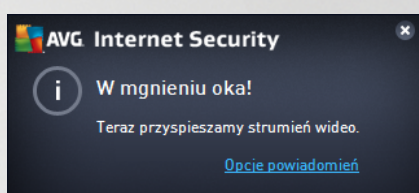


Obsługiwane przeglądarki internetowe

Ta funkcja współpracuje z następującymi przeglądarkami: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

Usługa **AVG Accelerator** pozwala na płynniejsze odtwarzanie filmów online i łatwiejsze pobieranie dodatkowych plików. W czasie działania składnika AVG Accelerator będzie wyświetlane odpowiednie powiadomienie nad ikoną AVG na pasku zadań.





6. Składniki AVG

6.1. Ochrona komputera


Składnik **Komputer** obejmuje dwie podstawowe usługi dotyczące bezpieczeństwa: **AntiVirus** i **Sejf danych**:

- **AntiVirus** składa się z silnika skanującego, który chroni wszystkie pliki, obszary komputera oraz urządzenia wymienne (*dyski flash itd.*) oraz skanuje w poszukiwaniu znanych wirusów. Wszelkie wykryte infekcje zostaną zablokowane, a następnie wyleczone lub przeniesione do [Przechowalni wirusów](#). Zazwyczaj użytkownik nie będzie w stanie zauważyć tego procesu, ponieważ odbywa się on "w tle". AntiVirus używa także analizy heurystycznej, która pozwala skanować pliki w poszukiwaniu typowych charakterystyk wirusów. Oznacza to, że składnik AntiVirus może wykryć nowy, nieznaną wirus, jeżeli zawiera on pewne cechy znane z istniejących wirusów. **AVG Internet Security** może również analizować i wykrywać wykonywalne aplikacje i biblioteki DLL, które mogą być potencjalnie niepożądane w systemie (*różne rodzaje oprogramowania szpiegującego, reklamowego itp.*). Ponadto AntiVirus skanuje rejestr systemu w poszukiwaniu podejrzanych wpisów, a także monitoruje tymczasowe pliki internetowe. Umożliwia to traktowanie wszystkich potencjalnie szkodliwych obiektów tak jak infekcji.
- **Sejf danych** umożliwia tworzenie bezpiecznych wirtualnych przechowalni cennych lub poufnych danych. Zawartość Sejfu danych jest szyfrowana wybranym przez użytkownika hasłem, aby nikt nie mógł jej zobaczyć bez autoryzacji.




Elementy okna


Aby przełączyć się między dwiema sekcjami okna, wystarczy kliknąć w dowolnym obszarze odpowiedniego panelu. Panel zostanie wówczas podświetlony jasnoniebieskim kolorem. W obu sekcjach okna znajdują się poniżej przyciski kontrolne. Ich działanie jest takie samo, niezależnie od funkcji, do której należą (*AntiVirus lub Sejf danych*):

 **Włączone/Wyłączone** — ten przycisk może przypominać sygnalizację świetlną, zarówno wyglądem, jak i funkcjonalnością. Pojedyncze kliknięcie powoduje przełączenie między dwoma



stanami. Kolor zielony reprezentuje stan **Włączony**, co oznacza, że usługa AntiVirus jest aktywna i w pełni funkcjonalna. Kolor czerwony reprezentuje stan **Wyłączony**, co oznacza, że usługa nie jest aktywna. Jeśli nie masz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli zechcesz wyłączyć usługę, zostanie wyświetlone ostrzeżenie o możliwym ryzyku: czerwony znak **Ostrzeżenie** oraz informacje o braku pełnej ochrony. **Pamiętaj o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!**

 **Ustawienia** — kliknij ten przycisk, aby przejść do interfejsu [ustawień zaawansowanych](#). Zostanie otwarte odpowiednie okno, w którym będzie można skonfigurować wybrane usługi ([AntiVirus](#)). W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład programu **AVG Internet Security**, ale zalecamy to jedynie do wiadczonego użytkownikom.

 **Strzałka** — użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do [głównego interfejsu użytkownika](#) z przeglądem składników.

Tworzenie własnego sejfów danych

W sekcji **Sejf danych** okna **Ochrona komputera** jest dostępny przycisk **Utwórz swój sejf**. Kliknij ten przycisk, aby otworzyć nowe okno dialogowe z tą samą nazwą, gdzie określić można parametry zakładanego sejfów. Uzupełnij wszystkie wymagane informacje, a następnie postępuj zgodnie z instrukcjami z aplikacji:



Po pierwsze określ nazwę sejfów i utwórz silne hasło:

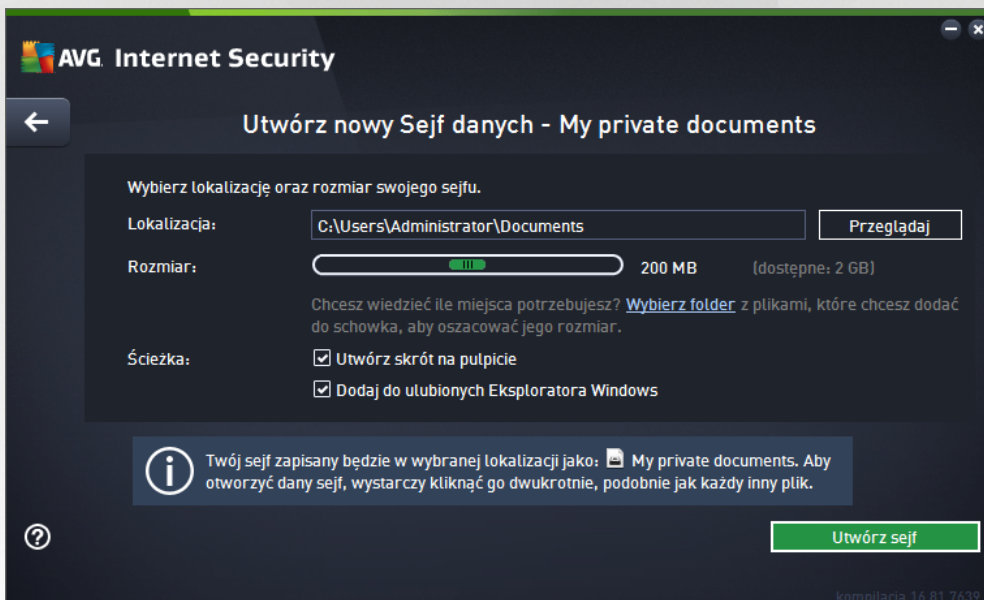
- **Nazwa sejfów** — aby utworzyć nowy sejf danych, najpierw wybierz odpowiednią nazwę sejfów, aby móc go później rozpoznać. Jeśli korzystasz z tego samego komputera co reszta członków rodziny, możesz podać zarówno swoje imię, jak również wskazówkę dotyczącą zawartości sejfów, na przykład *Wiadomo ci e-mail taty*.
- **Utwórz hasło/Powtórz hasło** — wymyśl hasło dla swojego sejfów danych i wpisz je w odpowiednie



pola tekstowe. Wskaźnik graficzny znajdujący się po prawej stronie informuje, czy hasło jest słabe (stosunkowo łatwe do odgadnięcia za pomocą specjalnych narzędzi), czy też silne. Zalecamy stosowanie haseł o przynajmniej średnim stopniu bezpieczeństwa. Siła hasła może być zwiększona, stosując w nim wielkie litery, cyfry i inne znaki, takie jak kropki, myślniki itp. Jeżeli chcesz mieć pewność, że wprowadzasz prawidłowe hasło, możesz zaznaczyć pole **Pokaż hasło** (oczywiście, jeżeli nikt inny nie patrzy wtedy na Twój monitor).

- **Wskazówka do hasła** — zalecamy także utworzenie pomocnej wskazówki do hasła, która pozwoli Ci je sobie przypomnieć. Sejf danych chroni Twoje pliki i umożliwia im dostęp wyłącznie za pomocą hasła. Nie możesz na tego obejść, więc jeżeli zapomnisz, jakie masz hasło, nie będziesz mieć dostępu do sejfu danych.

Po określeniu wszystkich wymaganych danych w polach tekstowych, kliknij przycisk **Dalej**, aby przejść do następnego kroku:



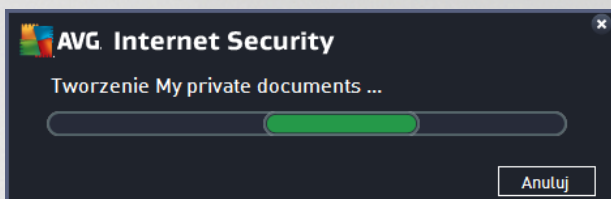
Okno to pozwala na następujące opcje konfiguracji:

- **Lokalizacja** określa, gdzie dany sejf zostanie umieszczony. Wybierz odpowiednie miejsce na dysku twardym lub pozostaw lokalizację domyślną, czyli folder *Dokumenty*. Po utworzeniu sejfu danych jego lokalizacja nie może zostać zmieniona.
- **Rozmiar** — istnieje możliwość zdefiniowania rozmiaru sejfu danych, aby przydzielić do niego potrzebne miejsce na dysku. Wartość ta nie powinna być zbyt mała (*niewystarczająca dla Twoich potrzeb*) ani zbyt duża (*zabierająca niepotrzebnie za dużo miejsca na dysku*). Jeżeli wiesz już, co będzie znajdować się w sejfie, możesz umieścić te pliki w jednym folderze, a następnie użyć polecenia **Wybierz folder**, aby automatycznie obliczyć całkowity rozmiar sejfu. Jednak rozmiar ten może zostać później zmieniony w zależności od potrzeb użytkownika.
- **Dostęp** — pola wyboru w tej sekcji umożliwiają tworzenie wygodnych skrótów do sejfu danych.



Korzystanie z Sejfu danych

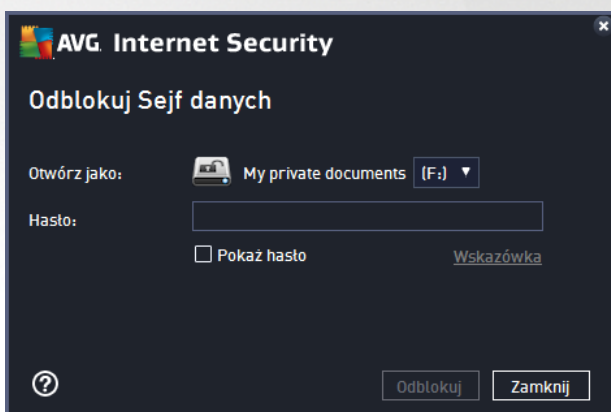
Gdy zakończysz konfigurację ustawień, kliknij przycisk **Utwórz sejf**. Zostanie otwarte nowe okno dialogowe **Twój Sejf danych jest już gotowy** informujące o tym, że w sejfie można już przechowywać dane. Sejf jest otwarty i możesz z niego od razu skorzystać. Przy kolejnych próbach uzyskania dostępu do sejfu zostanie wyświetlona prośba o jego odblokowanie za pomocą zdefiniowanego wcześniej hasła:



Aby skorzystać ze swojego nowego Sejfu danych, musisz go najpierw otworzyć — kliknij przycisk **Otwórz teraz**. Sejf po otwarciu będzie widoczny w Twoim komputerze jako nowy dysk wirtualny. Przypisz do niego dowolny liter z menu rozwijanego (do wyboru będą tylko aktualnie nieużywane dyski). Zazwyczaj niedozwolone są litery takie jak: C (przypisana do dysku twardego), A (stacja dyskietek) lub D (napęd DVD). Pamiętaj, że za każdym razem, gdy odblokowujesz sejf danych, możliwy jest wybór innej litery dysku.

Odblokowywanie sejfu danych

Przy kolejnej próbie uzyskania dostępu do Sejfu danych zostanie wyświetlona prośba o jego odblokowanie za pomocą zdefiniowanego wcześniej hasła:



Wpisz hasło w polu tekstowym, aby dokonać autoryzacji, a następnie kliknij przycisk **Odblokuj**. Jeśli potrzebujesz pomocy w przypomnieniu sobie hasła, kliknij opcję **Wskazówka**, aby wyświetlić podpowiedź dotyczącą hasła utworzonego podczas tworzenia sejfu danych. Nowy sejf danych będzie widoczny w przeglądzie Twoich sejfów danych jako ODBLOKOWANY i można będzie dodawać do niego pliki oraz je usuwać.

6.2. Ochrona przeglądania sieci

Ochrona przeglądania sieci składa się z dwóch usług: **LinkScanner Surf-Shield** i **Ochrona Sieci**:

- **LinkScanner Surf-Shield** to funkcja zapewniająca ochronę przed rosnącą liczbą zagrożeń




internetowych. Zagrozenia te moglyby ukryte na stronie internetowej jakiego typu (od stron rzadowych przez witryny duzych i znanych marek, po strony malych firm). Rzadko kiedy pozostaj tam dluzej ni 24 godziny. Skladnik LinkScanner zapewnia nadzwyczaj skuteczn ochron , skanuj c wszystkie linki znajduj ce si na ka dej przegl danej stronie. Robi to dokladnie wtedy, gdy ma to najwi ksze znaczenie — zanim zdecydujesz si je klikn . **Funkcja LinkScanner Surf-Shield nie jest przeznaczona dla platform serwerowych!**

- **Ochrona Sieci** to rodzaj programu rezydentnego zapewniaj cego ochron w czasie rzeczywistym. Skladnik ten skanuje zawarto odwiedzanych stron internetowych (oraz znajduj cych si na nich plikow), jeszcze zanim zostan zaladowane przez przegl dark lub pobrane na dysk twardy. Ochrona Sieci wykrywa strony zawieraj ce niebezpieczny kod javascript i blokuje ich ladowanie. Ponadto, identyfikuje szkodliwe oprogramowanie zawarte na stronach WWW i w razie podejrze zatrzymuje pobieranie, aby nie dopu ci do infekcji komputera. Ta zaawansowana funkcja ochrony blokuje szkodliw zawarto dowolnej otwieranej witryny internetowej, zapobiegaj c pobraniu jej na komputer. Gdy jest ona wlczona, kliknie cie jakiegokolwiek linku lub wpisanie adresu URL prowadz cego do niebezpiecznej witryny spowoduje automatyczne zablokowanie strony, dzi ki czemu komputer nie zostanie nie wiadomie zainfekowany. Warto pamitac , e infekcja mo e przedosta si na komputer z zainfekowanej witryny nawet podczas zwyklych odwiedzin strony internetowej. **Ochrona Sieci nie jest przeznaczona dla platform serwerowych!**




Elementy okna


Aby przeł czy si mi dzy dwiema sekcjami okna, mo esz klikn w dowolnym obszarze odpowiedniego panelu. Panel zostanie wówczas pod wietlony jasnyniebieskim kolorem. W obu sekcjach okna znajduj si poni sze przyciski kontrolne. Ich funkcjonalno jest identyczna, niezale nie od uslugi, ktorej dotycz (*LinkScanner Surf-Shield lub Ochrona Sieci*):

 **Wl czone/Wyl czone** — ten przycisk mo e przypomina sygnalizacj wietln , zarowno wygl dem, jak i funkcjonalno ci . Pojedyncze kliknie cie powoduje przeł czenie go mi dzy dwoma stanami. Kolor zielony reprezentuje stan **Wl czony**, co oznacza, e uslug LinkScanner Surf-Shield / Ochrona Sieci jest aktywna i w pelni funkcjonalna. Kolor czerwony reprezentuje stan **Wyl czony**, co oznacza, e uslug nie jest aktywna. Je li nie masz powa nego powodu do wyl czenia uslugi,



stanowczo zalecamy pozostawienie domylnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli chcesz wyłączyć usługę, zostanie wyświetlone ostrzeżenie o możliwym ryzyku: czerwony znak **Ostrzeżenie** oraz informacje o braku pełnej ochrony. **Pamiętaj o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!**

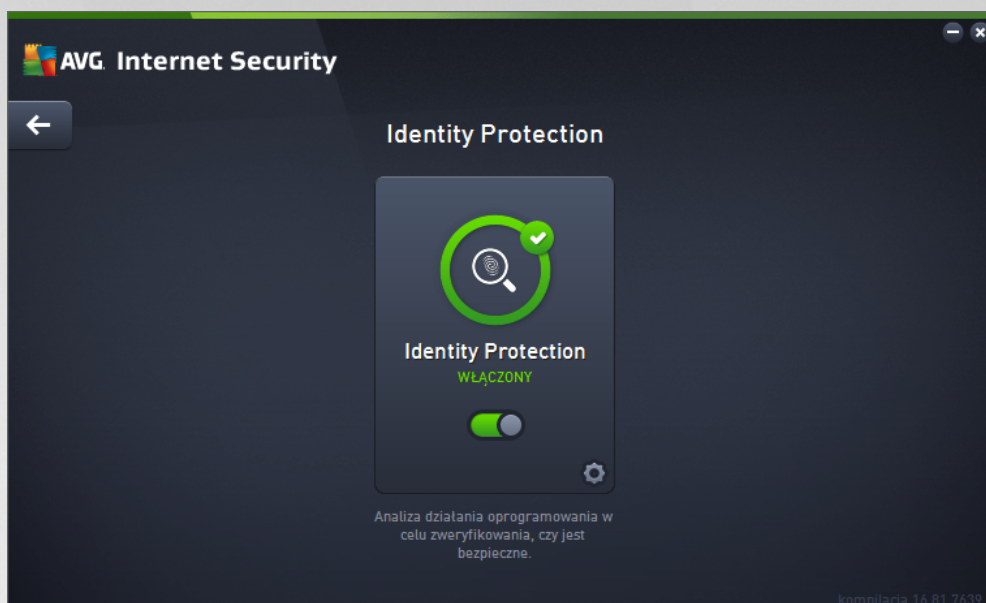
 **Ustawienia** — kliknij ten przycisk, aby przejść do interfejsu [ustawień zaawansowanych](#). Dokładniej, zostanie otworzone odpowiednie okno, w którym można skonfigurować wybrane usługi, tj. [LinkScanner Surf-Shield](#) lub [Ochrona Sieci](#). W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład programu **AVG Internet Security**, ale zalecamy to jedynie do wiadczonych użytkownikom.

 **Strzałka** — użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do [głównego interfejsu użytkownika](#) z przegladaniem składników.

6.3. Identity Protection


Składnik **Identity Protection** uruchamia usługę **Identity Shield**, która stale chroni Twoje cyfrowe zasoby przed nowymi, nieznanymi zagrożeniami z Internetu:


- Usługa **Identity Protection** służy do ochrony przed szkodliwym oprogramowaniem, zabezpieczając przed wszystkimi jego rodzajami (np. programami szpiegującymi, botami, kradzieżą Twoich danych) przy użyciu technologii behawioralnych zdolnych wykrywać również najnowsze wirusy. Identity Protection to usługa, której głównym zadaniem jest zapobieganie kradzieżom Twoich danych (w wyniku kradzieży haseł, rachunków bankowych, numerów kart kredytowych i innych cennych danych) przez szkodliwe oprogramowanie (ang. *malware*). Zapewnia poprawne działanie wszystkich programów uruchomionych na Twoim komputerze i w sieci lokalnej. Usługa Identity Protection dzięki zapewnianiu stałego nadzoru wykrywa i blokuje podejrzaną zachowanie, a także chroni komputer przed nowym szkodliwym oprogramowaniem. Usługa Identity Protection zapewnia komputerowi ochronę w czasie rzeczywistym przed nowymi, a nawet nieznanymi zagrożeniami. Monitoruje ona wszystkie procesy (w tym ukryte) i rozpoznaje ponad 285 różnych wzorców zachowań, dzięki czemu może ustalić, czy w systemie dzieje się coś szkodliwego. Z tego względu może wykrywać zagrożenia, które nie zostały jeszcze opisane w bazie danych wirusów. Gdy na komputerze pojawi się nieznaną kod programu, jest on natychmiast obserwowany i monitorowany pod kątem szkodliwego zachowania. Jeśli dany plik zostanie uznany za szkodliwy, usługa Identity Protection przekaże jego kod do [Przechowalni wirusów](#) i cofnie wszelkie zmiany wprowadzone w systemie (ingerencje w kod, zmiany w rejestrze, operacje otwarcia portów itd.). Nie ma potrzeby przeprowadzania skanów w celu zapewnienia ochrony. Technologia ma charakter wysoce proaktywny, wymaga rzadkich aktualizacji i zapewnia stałą ochronę.




Elementy okna

W oknie dialogowym znajdują się następujące elementy sterujące:

 **Włączone/Wyłączone** — ten przycisk może przypominać sygnalizację świetlną, zarówno wyglądem, jak i funkcjonalnością. Pojedyncze kliknięcie powoduje przełączenie go między dwoma stanami. Kolor zielony reprezentuje stan **Włączony**, co oznacza, że usługa Identity Protection jest aktywna i w pełni funkcjonalna. Kolor czerwony reprezentuje stan **Wyłączony**, co oznacza, że usługa nie jest aktywna. Jeśli nie masz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli zdecydujesz się wyłączyć usługę, zostanie wyświetlone ostrzeżenie o możliwym ryzyku: czerwony znak **Ostrzeżenie** oraz informacje o braku pełnej ochrony. **Pamiętaj o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!**

 **Ustawienia** — kliknij ten przycisk, aby przejść do interfejsu [ustawień zaawansowanych](#). Zostanie otwarte odpowiednie okno, w którym można skonfigurować wybraną usługę ([Identity Protection](#)). W interfejsie ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład programu **AVG Internet Security**, ale zalecamy to jedynie do włączonych usług.

 **Strzałka** — użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do [głównego interfejsu użytkownika](#) z przeglądem składników.

Niestety, produkt **AVG Internet Security** nie zawiera usługi Identity Alert. Jeśli interesuje Cię ochrona tego typu, kliknij przycisk **Uaktualnij, aby aktywować**. Następnie przejdź do specjalnej strony umożliwiającej zakup licencji Identity Alert.

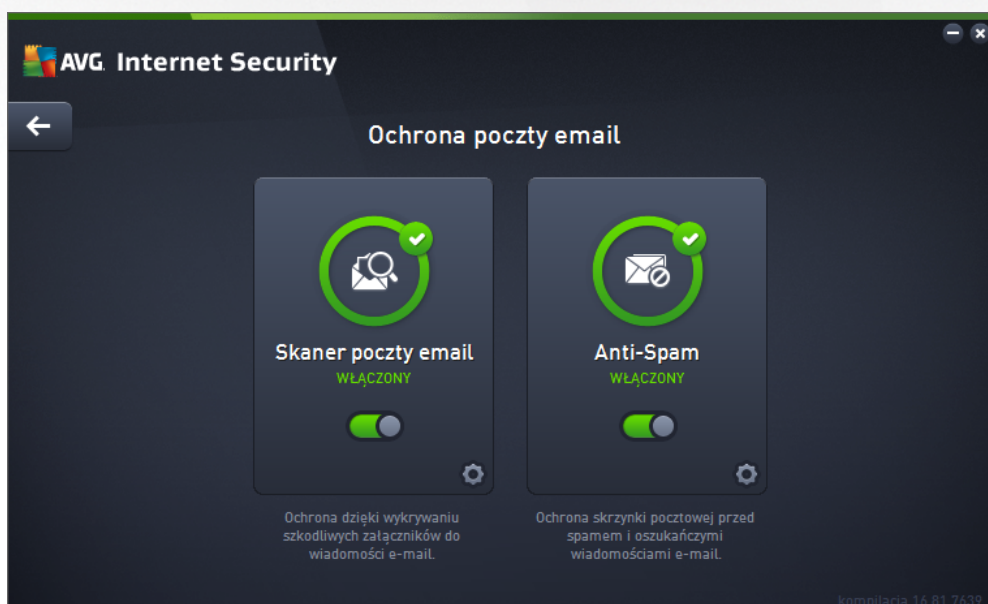
Nawet w przypadku edycji AVG Premium Security usługa Identity Alert jest obecnie dostępna jedynie w wybranych obszarach: w Stanach Zjednoczonych, Wielkiej Brytanii, Kanadzie i Irlandii.



6.4. Ochrona poczty email

Składnik **Ochrona poczty e-mail** obejmuje dwie podstawowe usługi dotyczące bezpieczeństwa: **Skaner poczty e-mail** i **Anti-Spam** (usługa Anti-Spam jest dostępna tylko w wersjach Internet i Premium Security).


- **Skaner poczty e-mail:** Poczta e-mail często jest źródłem wirusów i koni trojańskich. Wyłudzenia danych i spam powodują, że stała się ona jeszcze w większym zagrożeniem. Darmowe konta pocztowe są szczególnie narażone na otrzymywanie szkodliwych wiadomości e-mail, *ponieważ rzadko korzystają z technologii antyspamowych*, a użytkownicy domowi najczęściej używają właśnie takich kont. Dodatkowo odwiedzają one 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. Składnik Ochrona poczty e-mail jest odpowiedzialny za skanowanie wszystkich wiadomości e-mail (zarówno wysyłanych, jak i otrzymywanych). Każdy wirus wykryty w wiadomości jest natychmiast przenoszony do [Przechowalni wirusów](#). Skaner poczty może odfiltrowywać określone typy załączników i dodawać do wiadomości tekst certyfikujący brak infekcji. **Skaner poczty e-mail nie jest przeznaczony dla platform serwerowych!**
- **Anti-Spam** sprawdza wszystkie przychodzące wiadomości e-mail i zaznacza te niepożądane jako spam. (*Spam to nieadresowane wiadomości e-mail — najczęściej reklamujące produkt lub usługę — które są masowo rozsyłane jednocześnie nie do wielu skrzynek pocztowych, zamykając je. Spamem nie jest korespondencja seryjna rozsyłana do odbiorców po wyrażeniu przez nich zgody*). Składnik Anti-Spam może modyfikować temat wiadomości e-mail (*zidentyfikowanej jako spam*), dodając do niego specjalny ciąg tekstowy. Dzięki temu można łatwo filtrować wiadomości e-mail w programie pocztowym. Składnik Anti-Spam podczas przetwarzania każdej wiadomości wykorzystuje kilka metod analizy, oferując maksymalnie skuteczną ochronę przeciwko niepożądanym wiadomościom e-mail. Składnik Anti-Spam wykrywa spam, korzystając z regularnie aktualizowanej bazy danych. Można także użyć [serwerów RBL](#) (*publicznych baz adresów znanych nadawców spamu*) lub ręcznie dodać adresy do [białej listy](#) (*wiadomości pochodzące z tych adresów nie są nigdy oznaczane jako spam*) lub [czarnej listy](#) (*wiadomości pochodzące z tych adresów są zawsze oznaczane jako spam*).







Elementy okna

Aby przełączyć się między dwiema sekcjami okna, wystarczy kliknąć w dowolnym obszarze odpowiedniego panelu. Panel zostanie wówczas podświetlony jasnoniebieskim kolorem. W obu sekcjach okna znajdują się poniżej przyciski kontrolne. Ich funkcjonalność jest taka sama, niezależnie od tego, do której usługi się odnoszą (*Skaner poczty email lub Anti-Spam*):

 **Włączony/Wyłączony** — ten przycisk może przypominać sygnalizację świetlną, zarówno wyglądem, jak i funkcjonalnością. Pojedyncze kliknięcie powoduje przełączenie go między dwoma stanami. Kolor zielony reprezentuje stan **Włączony**, co oznacza, że usługa jest aktywna i w pełni funkcjonalna. Kolor czerwony reprezentuje stan **Wyłączony**, co oznacza, że usługa nie jest aktywna. Jeśli nie masz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli zechcesz wyłączyć usługę, zostanie wyświetlone ostrzeżenie o możliwym ryzyku: czerwony znak **Ostrzeżenie** oraz informacje o braku pełnej ochrony. **Pamiętaj o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!**

 **Ustawienia** — kliknij ten przycisk, aby przejść do interfejsu [ustawień zaawansowanych](#). Dokładniej, zostanie otworzone odpowiednie okno, w którym można skonfigurować wybraną usługę, tj. [Skaner poczty e-mail](#) lub [Anti-Spam](#). W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład programu **AVG Internet Security**, ale zalecamy to jedynie do wiadczonym użytkownikom.

 **Strzałka** — użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do [głównego interfejsu użytkownika](#) z przeglądem składników.

6.5. Zapora

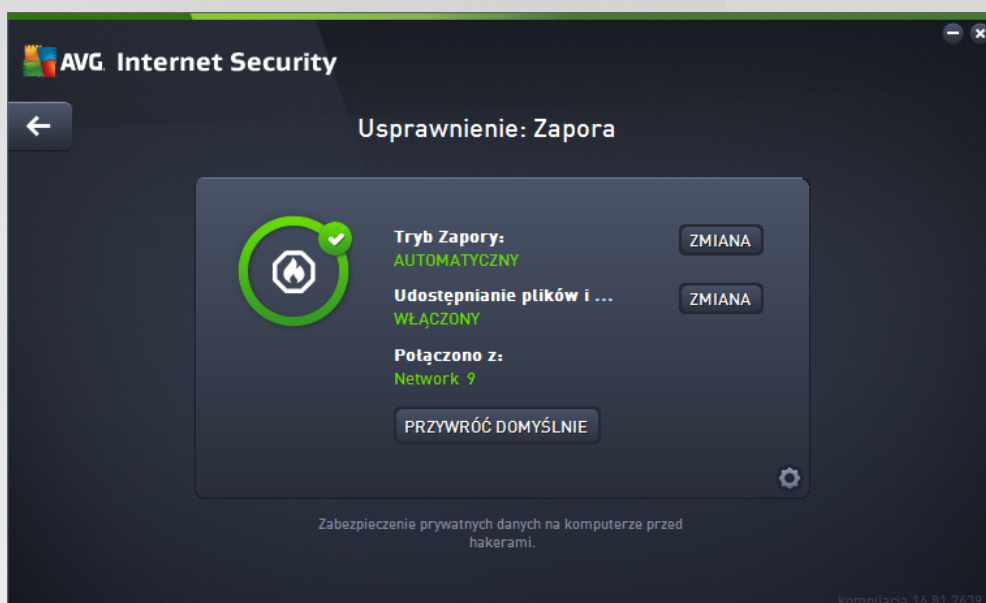
Zapora internetowa to system, który wymusza stosowanie zasad kontroli dostępu między dwiema sieciami lub ich większą liczbą, blokując lub umożliwiając przepływ danych. Zapora składa się z zestawu reguł, które sterują komunikacją na każdym indywidualnym porcie sieciowym, chroniąc w ten sposób sieć lokalną przed atakami, których źródło znajduje się *na zewnątrz (zazwyczaj w internecie)*. Komunikacja jest oceniana w oparciu o zdefiniowane reguły, a następnie jest umożliwiana lub blokowana. Jeśli Zapora wykryje próbę ataku, blokuje ją i nie pozwala intruzowi przejść 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 internetowy, który odbywa się za pośrednictwem programu Microsoft Internet Explorer. Próba transmisji danych WWW przez jakkolwiek inny przeglądarkę będzie w takim przypadku blokowana. Zapora chroni również dane osobowe — nikt nie uzyska ich bez Twojej zgody. Decyduje też o tym, jak komputer wymienia dane z innymi komputerami w sieci internetowej lub w sieci lokalnej. Zapora w środowisku komercyjnym chroni również pojedyncze komputery przed atakami przeprowadzonymi z wnętrza tej samej sieci.

W systemie **AVG Internet Security Zapora** kontroluje cały ruch na każdym porcie sieciowym komputera. Na podstawie zdefiniowanych reguł Zapora *ocenia uruchomione aplikacje (chcąc je nawet za pośrednictwem sieci lokalnej lub internetowej) oraz programy usiłujące z zewnątrz połączyć się z Twoim komputerem*. Zapora umożliwia lub blokuje komunikację tych aplikacji na określonych portach sieciowych. Domyślnie, jeśli aplikacja jest nieznaną (tj. *nie ma zdefiniowanych reguł Zapory*), składnik Zapora wyświetli pytanie, czy próba komunikacji ma zostać odblokowana czy zablokowana.

Zapora AVG nie jest przeznaczona do współpracy z serwerami!



Zalecenie: Generalnie nie zaleca się używania więcej niż jednej zapory internetowej na danym komputerze. Zainstalowanie dodatkowych zapór nie zwiększy bezpieczeństwa komputera. Zwiększy się natomiast prawdopodobieństwo wystąpienia konfliktów 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.



Uwaga: Po zainstalowaniu programu AVG Internet Security składnik Zapora może wymagać ponownego uruchomienia komputera. W takim przypadku zostanie wyświetlone okno dialogowe składnika z informacją o konieczności ponownego uruchomienia komputera. W wyświetlonym oknie dialogowym znajduje się przycisk **Uruchom ponownie teraz**. Do czasu ponownego uruchomienia składnik Zapora nie będzie w pełni aktywowany. Ponadto w oknie dialogowym wszystkie opcje edycji będą nieaktywne. Zwróć uwagę na ostrzeżenie i jak najszybciej uruchom ponownie komputer!

Dostępne tryby Zapory

Zapora umożliwia definiowanie określonych reguł bezpieczeństwa na podstawie środowiska i trybu pracy komputera. Każda opcja wymaga innego poziomu zabezpieczenia, a dostosowywanie poziomów odbywa się za pomocą odpowiednich trybów. Krótko mówiąc, tryb Zapory to określona konfiguracja tego składnika. Dostępna jest pewna liczba wstępnie zdefiniowanych konfiguracji.

- **Automatyczny** — w tym trybie Zapora obsługuje cały ruch sieciowy automatycznie. Nie musisz podejmować żadnych decyzji. Zapora zezwoli na połączenia wszystkich znanych aplikacji, tworząc jednocześnie reguły umożliwiające im nadal używanie połączeń w przyszłości. W przypadku innych aplikacji Zapora zdecyduje, czy pozwoli na komunikację, czy ją zablokuje, na podstawie analizy działania aplikacji. W takich sytuacjach nie utworzy ona jednak reguły, więc aplikacja będzie sprawdzana przy każdej dorazowej próbie połączenia. Tryb automatyczny działa dyskretnie i jest polecany zwłaszcza użytkownikom.
- **Interaktywny** — tryb ten może być przydatny, jeśli chcesz w pełni kontrolować ruch przychodzący i wychodzący z Twojego komputera. Zapora będzie monitorowała ruch i przy każdej próbie połączenia lub transferu danych pozwoli Ci zdecydować, czy chcesz na to zezwolić. Ten tryb jest zalecany tylko w przypadku użytkowników zaawansowanych.



- **Blokuj dost p do internetu** — poł czenie z internetem b dzie całkowicie zablokowane, uniemo liwiaj c Ci dost p do internetu, a ka demu z zewn trz — do Twojego komputera. Ten tryb jest przeznaczony tylko do stosowania tymczasowo i w szczególnych sytuacjach.
- **Wył cz Zapor (niezalecane)** — wył czenie Zapory zezwoli na cały ruch przychodz cy do komputera i wychodz cy z niego. W rezultacie stanie si on podatny na ataki hakerów. T opcj nale y stosowa z rozrag .

Nale y zwróci uwag na specyficzny automatyczny tryb pracy Zapory. Tryb ten jest aktywowany w tle za ka dym razem, gdy składnik [Komputer](#) lub [Identity Protection](#) zostanie wył czony, co nara a komputer na zwi kszone niebezpiecze stwo. W takim przypadku Zapor zezwoli automatycznie na ruch sieciowy dotycz cy tylko znanych i całkowicie bezpiecznych aplikacji. We wszystkich pozostałych przypadkach b dzie wy wietlany monit o podj cie decyzji. Słu y to zrównowa eniu ryzyka spowodowanego wył czonymi składnikami i jest sposobem na zachowanie bezpiecze stwa Twojego komputera.

Zdecydowanie nie zalecamy wył czania Zapory. Je li jednak wyst puje konieczno zdezaktywowania składnika Zapora, mo na to zrobi , zaznaczaj c tryb Wył cz Zapor na powy szej li cie dost pnych trybów Zapory.

Elementy okna

W tym oknie dialogowym jest wy wietlany przegl d informacji o bie cym stanie składnika Zapora:

- **Tryb Zapory** — informuje o obecnie wybranym trybie Zapory. U yj przycisku **Zmie** znajduj cego si obok podanej informacji, aby przej do interfejsu [Ustawienia Zapory](#) i zmieni bie cy tryb na inny (*opis i zalecenia dotycz ce profili Zapory znajduj si w poprzednim akapicie*).
- **Udost pnianie plików i drukarek** — informuje, czy udost pnianie plików i drukarek (*w obu kierunkach*) jest obecnie dozwolone. Udost pnianie plików i drukarek oznacza w praktyce udost pnianie wszystkich plików i folderów, które oznaczysz jako udost pnione w systemie Windows, popularnych jednostkach dyskowych, drukarkach, skanerach i podobnych urz dzeniach. Udost pnianie tego typu elementów jest po dane jedynie w sieciach uwa anych za bezpieczne (*np. w domu, w pracy lub w szkole*). Je li jednak masz poł czenie z sieci publicznej (*np. sieci Wi-Fi na lotnisku lub w kawiarence internetowej*), lepiej niczego nie udost pnia .
- **Poł czony z** — podaje nazw sieci, z któr masz obecnie poł czenie. W systemie Windows XP nazwa sieci odpowiada nazwie wybranej dla danej sieci podczas pierwszego poł czenia z ni . W systemie Windows Vista i nowszych nazwa sieci pobierana jest automatycznie z Centrum sieci i udost pnienia.
- **Przywró domy lne** — ten przycisk umo liwia nadpisanie bie cej konfiguracji Zapory i przywrócenie konfiguracji domy lnej (na podstawie automatycznego wykrywania).

To okno zawiera nast puj ce graficzne elementy steruj ce:



Ustawienia — kliknij ten przycisk, aby otworzy menu podr czne zawieraj ce dwie opcje:

- **Ustawienia zaawansowane** — ta opcja powoduje przeniesienie do interfejsu [Ustawienia Zapory](#), który umo liwia edycj pełnej konfiguracji Zapory. Wszelkie zmiany konfiguracji powinny by wprowadzane wył cznie przez do wiadczonych u ytkowników!



- o **Usu ochron za pomoc skłladnika Zapora** — zaznaczenie tej opcji umożliwia odinstalowanie skłladnika Zapora, co mo e osłabi ochron Twojego komputera. Je li mimo to chcesz usun skłladnik Zapora, potwierd swoj decyzj , co spowoduje całkowite odinstalowanie tego skłladnika.

← **Strzałka** — u yj zielonej strzałki w prawym górnym rogu okna, aby powróci do [głównego interfejsu u ytkownika](#) z przegl dem skłladników.

6.6. PC Analyzer

Skłladnik **PC Analyzer** stanowi zaawansowane narz dzie przeznaczone do szczegółowej analizy i modyfikacji ustawie systemu w celu zwi kszenia szybko ci i efektywno ci działania komputera. Mo na go otworzy za pomoc przycisku **Popraw wydajno** znajdu cego si w [głównym oknie dialogowym interfejsu u ytkownika](#) lub przy u yciu tej samej opcji dost pnej w menu kontekstowym [ikony AVG w zasobniku systemowym](#). Post p analizie oraz jej wyniki b dzie mo na obserwowa bezpo rednio w tabeli:



Przeanalizowane mog zosta problemy z nast puj cych kategorii: bł dy rejestru, pliki wiadomo ci- mieci, fragmentacja i bł dne skróty:

- **Bł dy rejestru** — okre la liczb bł dów rejestru systemu Windows, które mog powodowa wolniejsze działanie komputera lub wy wietlanie komunikatów o bł dach.
- **Pliki- mieci** — okre la liczb zb dnych plików, które zajmuj miejsce na dysku i prawdopodobnie mo na je usun . Zazwyczaj s to ró nego rodzaju pliki tymczasowe oraz pliki znajduj ce si w Koszu.
- **Fragmentacja** — umo liwia obliczenie procentowego stopnia fragmentacji danych na dysku twardym (po upływie dłu szego czasu wiele plików mo e ulec rozproszeniu po ró nych sektorach dysku fizycznego).
- **Przerwane skróty** — wykrywa nie działaj ce skróty prowadz ce do nieistniej cych lokalizacji itd.

Podgl d wyników zawiera liczb wykrytych problemów systemowych sklasyfikowanych według odpowiednich



kategori. Wyniki analizy b d rónie wy wietlane w postaci graficznej na osi w kolumnie **Poziom zagro enia**.

Przyciski kontrolne

- **Zatrzymaj analiz** (*wy wietlany podczas trwania analizy*) — klikni cie tego przycisku umo liwia przerwanie analizy komputera.
- **Napraw teraz** (*wy wietlany po zako czeniu analizy*) — niestety funkcje programu PC Analityzer w ramach oprogramowania **AVG Internet Security** s ograniczone do analizy aktualnego stanu komputera. Firma AVG udost pnia jednak zaawansowane narz dzie przeznaczone do szczegóowej analizy i modyfikacji ustawie systemu w celu zwi kszenia szybko ci i efektywno ci dziaania komputera. Kliknij przycisk, aby nast piło przekierowanie do specjalnej witryny internetowej zawieraj cej wi cej informacji.

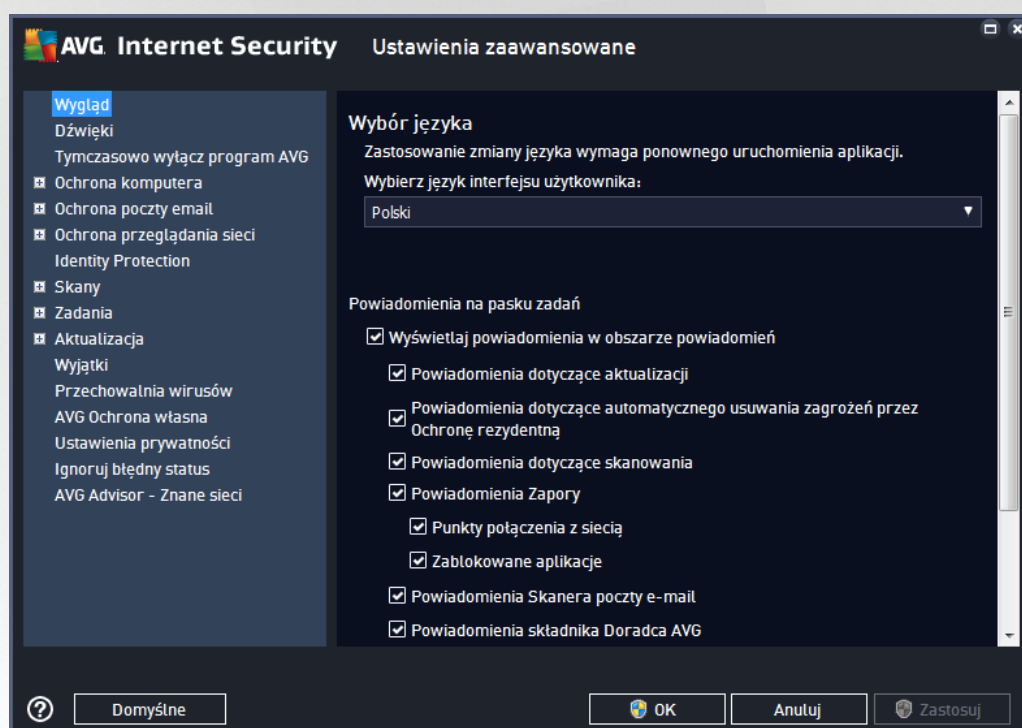


7. Ustawienia zaawansowane AVG

Opcje zaawansowanej konfiguracji systemu **AVG Internet Security** zostają otwarte w nowym oknie o nazwie **AVG — Ustawienia zaawansowane**. Okno to podzielone jest na dwa obszary: lewy zawiera drzewo nawigacyjne, a prawy – opcje konfiguracji programu. Wybranie składnika, którego (*lub cz ci którego*) konfiguracja ma zostać zmieniona, powoduje przejście do odpowiedniego okna z prawej strony.

7.1. Wygląd

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



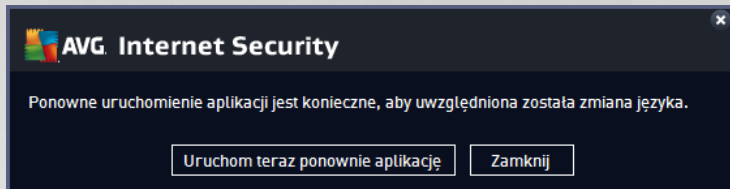
Wybór języka

W sekcji **Wybór języka** z menu rozwijanego można wybrać język aplikacji. Wybrany język będzie używany w całym [interfejsie użytkownika programu AVG Internet Security](#). Menu rozwijane zawiera tylko języki wybrane podczas instalacji i język angielski (*instalowany domyślnie*). Przełączenie aplikacji **AVG Internet Security** na inny język wymaga ponownego uruchomienia aplikacji. Wykonaj następujące kroki:

- Wybierz dany język aplikacji z menu rozwijanego
- Potwierdź wybór, klikając przycisk **Zastosuj** (*prawy dolny róg okna dialogowego*)
- Kliknij przycisk **OK**, aby potwierdzić
- Zostanie wówczas wyświetlony komunikat informujący o konieczności ponownego uruchomienia aplikacji **AVG Internet Security**



- Kliknij przycisk **Uruchom AVG ponownie**, aby zgodzi si na ponowne uruchomienie programu, i poczekaj kilka sekund na zastosowanie zmian:



Powiadomienia nad zasobnikiem systemowym

W tym obszarze mo na wyl czy wy wietlane w dymkach powiadomienia dotycz ce stanu aplikacji **AVG Internet Security**. Domy lnie powiadomienia systemowe s wy wietlane. Stanowczo nie zaleca si zmiany tego ustawienia bez uzasadnionej przyczyny. Powiadomienia zawieraj m.in. informacje o rozpocz ciu skanowania lub aktualizacji b d o zmianie stanu któregokolwiek ze składników aplikacji **AVG Internet Security**. Warto zwraca na nie uwag .

Je li jednak z jakiego powodu zdecydujesz, e nie chcesz otrzymywa tych informacji, lub e interesuj Ci tylko niektóre powiadomienia (*zwi zane z konkretnym składnikiem programu AVG Internet Security*), mo esz zdefiniowa swoje preferencje przez zaznaczenie odpowiednich pól:

- **Wy wietlaj powiadomienia w obszarze powiadomie** (*domy lnie wlczone*) — b d wy wietlane wszystkie powiadomienia. Odznaczenie tej opcji powoduje całkowite wyl czenie wszystkich powiadomie . Po wyl czeniu tej opcji mo na bardziej szczegółowo okre li , jakie powiadomienia maj by wy wietlane:
 - **Powiadomienia dotycz ce aktualizacji** (*domy lnie wlczone*) — zdecyduj, czy powinny by wy wietlane informacje dotycz ce uruchamiania, post pu i wyników aktualizacji **AVG Internet Security**.
 - **Powiadomienia dotycz ce automatycznego usuwania zagro e przez Ochron rezydentn** (*domy lnie wlczone*) — zdecyduj, czy maj by wy wietlane informacje dotycz ce zapisywania, kopiowania i otwierania plików (*ta konfiguracja jest dost pna tylko wtedy, gdy jest wlczona opcja automatycznego leczenia Ochrony rezydentnej*).
 - **Powiadomienia dotycz ce skanowania** (*domy lnie wlczone*) — wy wietlane b d informacje dotycz ce automatycznego rozpocz cia, post pu i wyników zaplanowanego skanowania.
 - **Powiadomienia dotycz ce Zapory** (*domy lnie wlczone*) — wy wietlane b d informacje dotycz ce stanu i działa Zapory, np. ostrze enia o wyl czeniu/wyl czeniu składnika, mo liwym blokowaniu poł cze itd. Ta opcja ma dwa kolejne pola wyboru (*szczególony opis zwi zanych z nimi funkcji mo na znale w rozdziale Zapora niniejszego dokumentu*):
 - **Punkty poł czenia z sieci** (*domy lnie wyl czone*) — przy ł czeniu z sieci Zapora poinformuje Ci , czy zna sie i czy wlczone jest udost pnienie plików i drukarek.
 - **Zablokowane aplikacje** (*domy lnie wlczone*) — gdy nieznan lub podejrzana aplikacja próbuje poł czy si z sieci , Zapora zablokuje prób poł czenia i wy wietli powiadomienie. Jest to przydatna funkcja, dzi ki której u ytkownik jest zawsze poinformowany, wi c nie zalecamy wyl czenia jej.



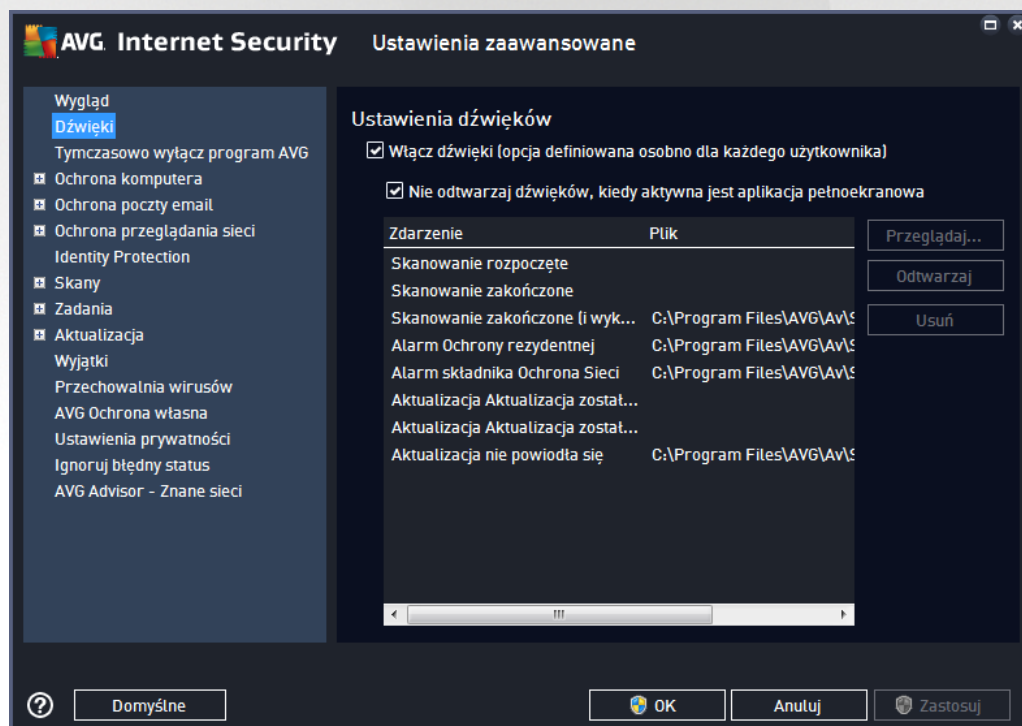
- o **Powiadomienia Skanera poczty email** (domyślnie włączone) — wyświetlane będą informacje o skanowaniu wszystkich wiadomości przychodzących i wychodzących.
- o **Powiadomienia dotyczące statystyk** (domyślnie włączone) — pozostaw to pole zaznaczone, aby otrzymywać regularne powiadomienia o dotychczasowych statystykach bezpieczeństwa.
- o **Powiadomienia Doradcy AVG** (domyślnie włączone) — zdecyduj, czy chcesz wyświetlać informacje o aktywności **Doradcy AVG** w rozwijanym panelu nad zasobnikiem systemowym.

Tryb gry

Ta funkcja jest przeznaczona dla aplikacji pełnoekranowych, w działaniu których mogłyby przeszkadzać (np. minimalizowana aplikacja 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).

7.2. Dźwięki

W oknie dialogowym **Ustawienia dźwięków** można określić, czy oprogramowanie **AVG Internet Security** ma informować o określonych czynnościach za pomocą dźwięków:



W każdym z tych ustawień jest włączony tylko kontekst aktualnego konta użytkownika. To znaczy, że każdy użytkownik komputera może mieć własne ustawienia dźwięków. Jeśli zgadzasz się na powiadomienie dźwiękowe, pozostaw pole **Włącz dźwięki** zaznaczone (domyślnie ta opcja jest aktywna). Możesz również zaznaczyć pole **Nie odtwarzaj dźwięków w trakcie działania aplikacji pełnoekranowej**, aby wyłączyć dźwięki wtedy, gdy mogłyby one przeszkadzać (więcej informacji znajduje się w sekcji **Tryb Gry**, w rozdziale [Ustawienia zaawansowane / Wygląd](#) niniejszej dokumentacji).



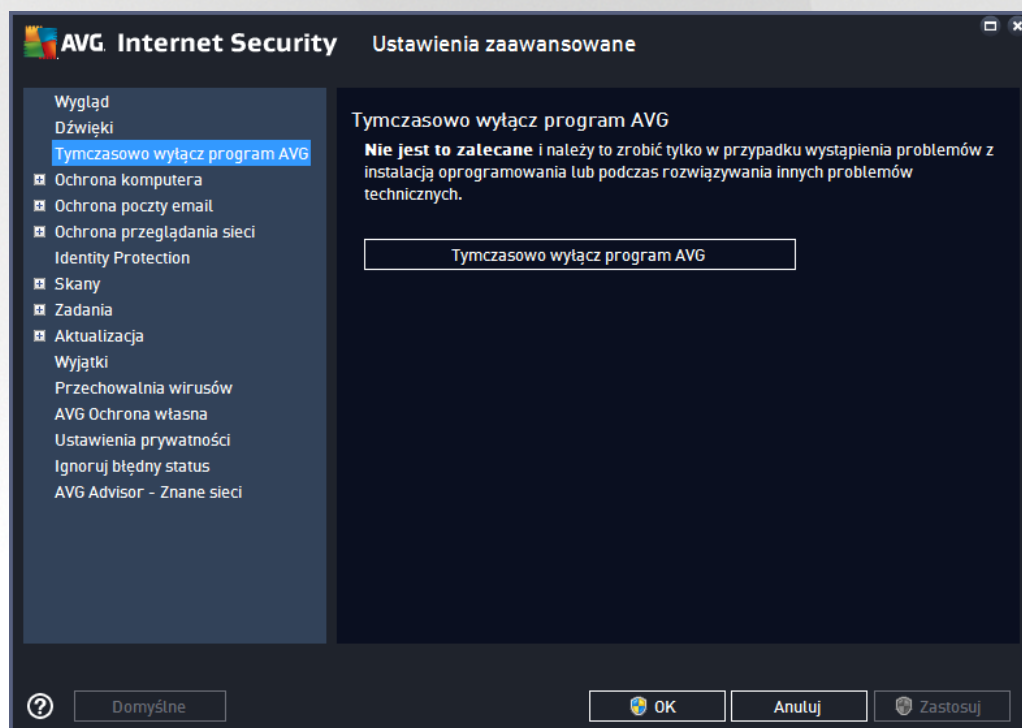
Przyciski kontrolne

- **Przełóż** — po wybraniu konkretnego zdarzenia z listy u yj przycisku **Przełóż**, aby wskaza plik d wi kowy, który chcesz przypisa temu zdarzeniu. (*Przypominamy, e obecnie obsługiwane s tylko pliki *.wav!*)
- **Odtwórz** — aby odsłucha wybrany d wi k, wska na li cie dane zdarzenie i kliknij przycisk **Odtwórz**.
- **Usu** — u yj przycisku **Usu**, aby usun d wi k przypisany do danego zdarzenia.

7.3. Tymczasowe wyłączenie ochrony AVG

W oknie dialogowym **Tymczasowo wył czy ochron AVG** mo na wył czy cał ochron zapewnian przez oprogramowanie **AVG Internet Security**.

Pami taj, e tej opcji nie powinno si u ywa, chyba e jest to absolutnie konieczne.

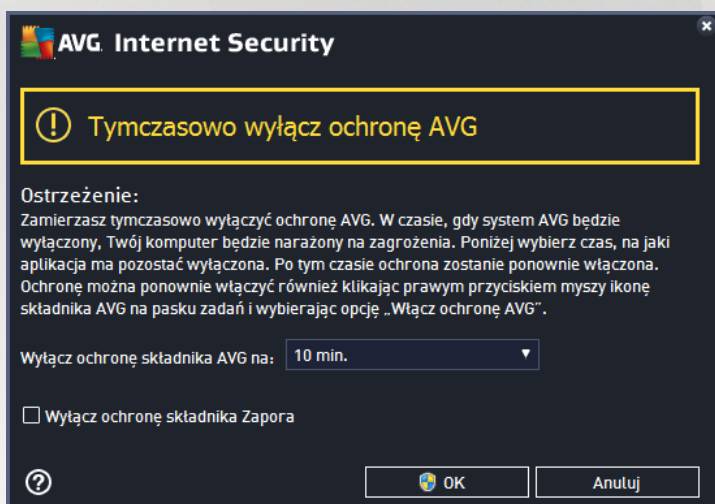


W wi kszo ci przypadków **nie jest konieczne** wył czanie oprogramowania **AVG Internet Security** przed zainstalowaniem nowego oprogramowania lub sterowników, nawet je li instalator lub kreator sugeruje uprzednie zamkni cie działaj cych programów i aplikacji, aby proces instalacji przebiegał bez zakłóce . W przypadku wyst pienia problemów podczas instalacji nale y najpierw spróbowa [wył czy ochron rezydentn](#) (w powi zanym oknie dialogowym usun zaznaczenie opcji **Wł czy Ochron rezydentn**). Je li jednak tymczasowe wył czanie oprogramowania **AVG Internet Security** jest konieczne, nale y je wł czy ponownie, gdy tylko b dzie to mo liwe. Je li oprogramowanie antywirusowe jest wył czone, komputer podł czony do internetu jest nara ony na ataki, przed którymi nie b dzie chroniony.



Jak wyłączyć ochronę AVG

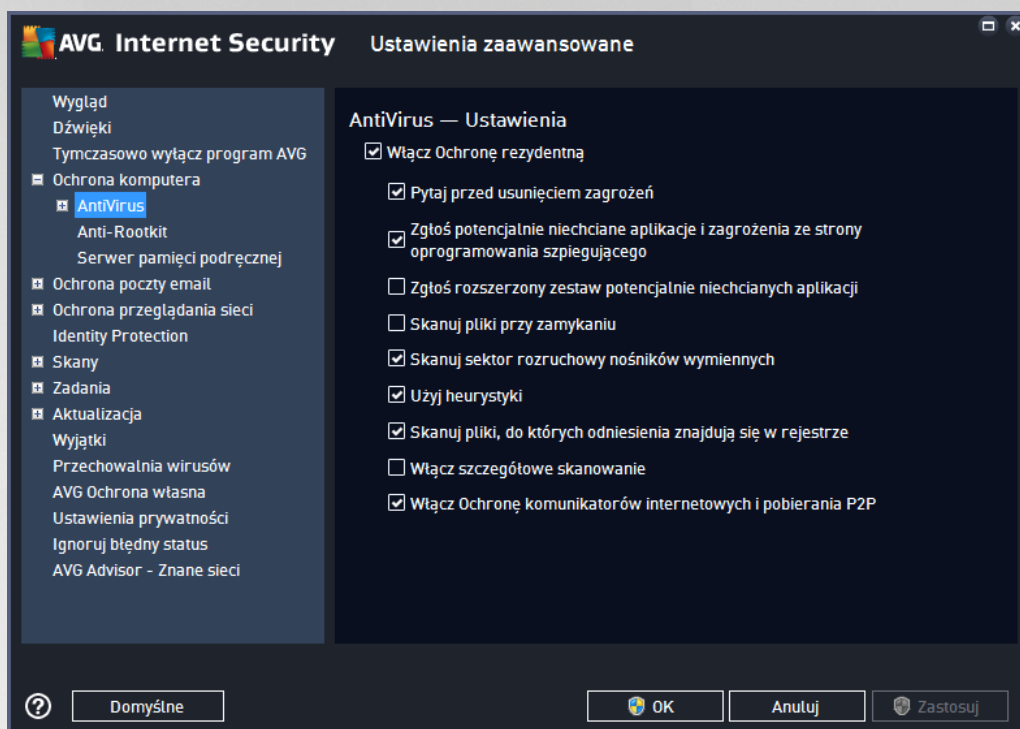
Zaznacz pole wyboru **Tymczasowo wyłącz ochronę AVG**, a następnie potwierdź swoją decyzję, klikając przycisk **Zastosuj**. W nowo otwartym oknie **Tymczasowo wyłącz ochronę AVG** określ, na jak długo chcesz wyłączyć oprogramowanie **AVG Internet Security**. Domyślnie ochrona pozostanie nieaktywna przez 10 minut, co powinno wystarczyć na wykonanie typowego zadania (np. instalacji nowego oprogramowania). Możesz ustawić dłuższy czas, ale nie jest to zalecane, jeżeli nie ma takiej konieczności. Po upływie cię danego czasu wszystkie wyłączone składniki zostaną automatycznie aktywowane ponownie. Możesz wyłączyć ochronę AVG a następnie przesto restartu komputera. Osobną opcję umożliwiająca wyłączenie **Zapory** dostępna jest w oknie **Tymczasowo wyłącz ochronę AVG**. Aby to zrobić, zaznacz pole **Wyłącz ochronę Zapora**.



7.4. Ochrona komputera

7.4.1. AntiVirus

AntiVirus oraz **Ochrona rezydentna** stale chroni Twój komputer przed wszystkimi znanymi typami wirusów, oprogramowania szpiegującego i złośliwego oprogramowania (*wł czaj c w to tak zwane u pionie i nieaktywne zagrożenia, które zostały pobrane, lecz jeszcze nie aktywowane*).



W oknie **Ustawienia Ochrony rezydentnej** można całkowicie włączyć lub wyłączyć Ochronę rezydentną, zaznaczając lub odznaczając pole **Włącz Ochronę rezydentną** (opcja ta jest domyślnie włączona). Można też aktywować tylko wybrane funkcje składnika Ochrona rezydentna:

- **Pytaj przed usunięciem zagrożenia** (domyślnie włączona) — zaznacz to pole, aby uzyskać pewność, że Ochrona rezydentna nie podejmie żadnych działań w sposób automatyczny; każdorazowo zostanie wyświetlone okno z opisem wykrytego zagrożenia i monitorem o podjęciu decyzji. Jeśli pozostawisz to pole niezaznaczone, program **AVG Internet Security** automatycznie wyleczy infekcję, a jeśli to niebędzie możliwe — przeniesie obiekt do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane programy oraz oprogramowanie szpiegujące** (domyślnie włączona) — zaznacz to pole, aby włączyć skanowanie w poszukiwaniu oprogramowania szpiegującego oprócz 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 zniższa ona poziom ochrony komputera.
- **Zgłoś rozszerzony zestaw potencjalnie niechcianych aplikacji** (domyślnie wyłączona) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego domyślnie jest wyłączona.
- **Skanuj pliki przy zamykaniu** (opcja domyślnie wyłączona) — system AVG będzie skanował 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) — zaznaczenie tego pola



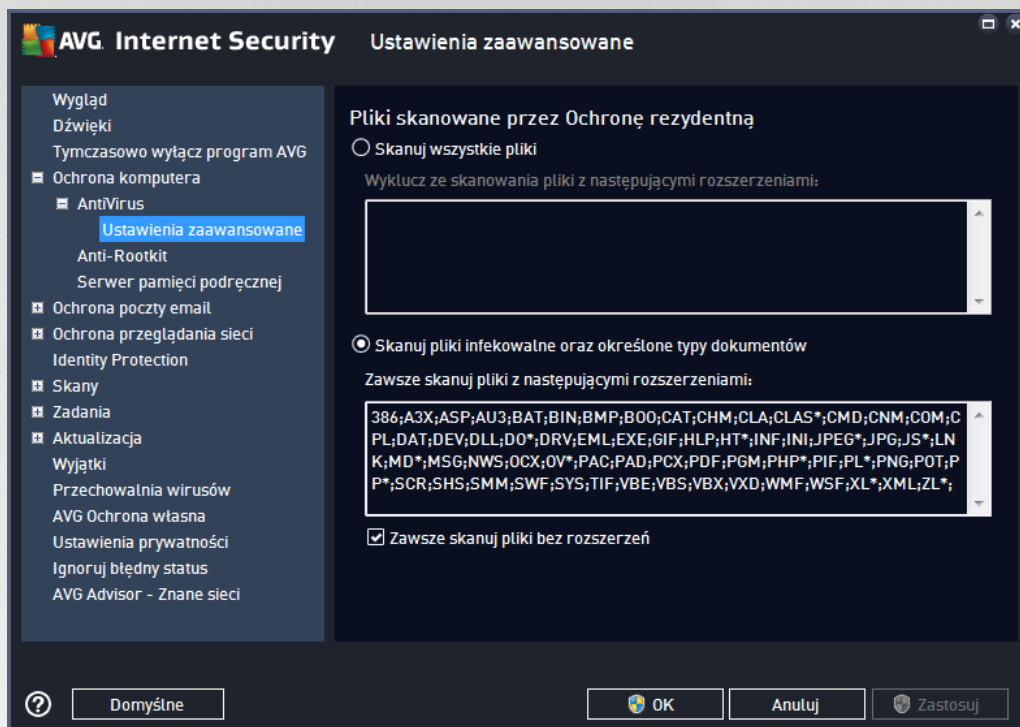
aktywuje skanowanie sektorów rozruchowych wszystkich podłączonych do komputera nośników pamięci USB, dysków zewnętrznych i innych nośników wymiennych.

- **Użyj heurystyki** (domyślnie włączone) — przy skanowaniu będzie używana analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej).
- **Skanuj pliki, do których odniesienia znajdują się w rejestrze** (domyślnie włączone) — ten parametr określa, czy system AVG będzie skanował wszystkie pliki wykonywalne dodane do rejestru w sekcji autostartu.
- **Włącz szczegółowe skanowanie** (opcja domyślnie wyłączona) — w określonych sytuacjach (w stanie wyjątkowej konieczności) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej szczegółowego skanowania, które bardziej dogłębnie sprawdzą wszystkie obiekty mogące stwarzać zagrożenie. Należy pamiętać, że ta metoda skanowania jest dość czasochłonna.
- **Włącz Ochronę komunikatorów internetowych i pobierania P2P** (domyślnie włączone) — zaznacz to pole, aby zapewnić ochronę komunikatorów internetowych (takich jak AIM, Yahoo!, ICQ, Skype, MSN Messenger itp.) i danych pobranych z sieci peer-to-peer (sieci umożliwiających nawzajemne bezpośrednich połączenia między klientami, bez udziału serwera, co może być potencjalnie niebezpieczne; takie sieci zazwyczaj służą do wymiany muzyki).

Uwaga: Jeśli program AVG jest zainstalowany w systemie Windows 10, na liście jest widoczna jeszcze jedna pozycja: **Włącz interfejs Windows Antimalware Scan Interface (AMSI) na użytek głównego skanowania oprogramowania**. Ta funkcja zwiększa ochronę antywirusową, zapewniając bardziej ściśle współdziałanie systemu Windows i oprogramowania AVG w zakresie wykrywania złośliwego kodu, dzięki czemu ochrona jest skuteczniejsza, a liczba fałszywych detekcji — mniejsza.



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



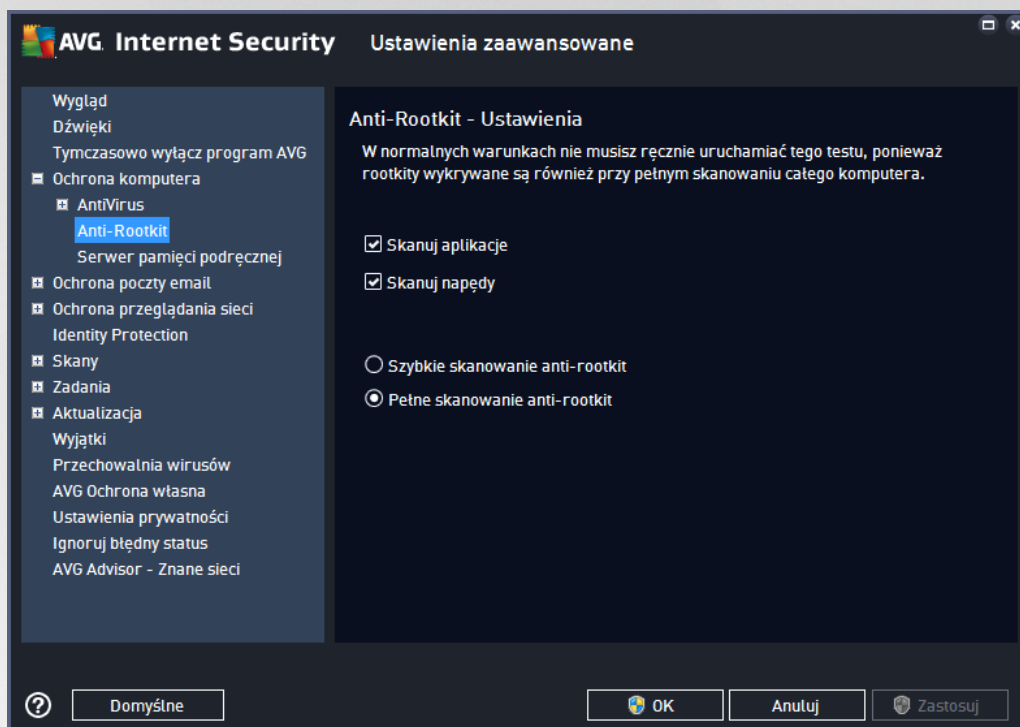
Zaznacz odpowiednie pole, w zależności od tego, czy chcesz skanować **wszystkie pliki** czy **tylko pliki infekowalne i niektóre typy dokumentów**. Aby przyspieszyć skanowanie, a jednocześnie nie zapewnić maksymalnej ochrony, zalecamy zachowanie ustawień domyślnych. Dzięki temu skanowane będą tylko pliki infekowalne. W odpowiedniej sekcji tego samego okna znajduje się także lista rozszerzeń plików, które mają być skanowane.

Zaznaczenie opcji **Zawsze skanuj pliki bez rozszerzeń** (domyślnie włączona) gwarantuje, że Ochrona rezydentna będzie skanowała także pliki bez rozszerzenia i pliki nieznanymi formatami. Nie zaleca się wyłączenia tej opcji, ponieważ pliki bez rozszerzenia są podejrzane.



7.4.2. Anti-Rootkit

W oknie **Ustawienia Anti-Rootkit** możesz edytować konfigurację funkcji **Anti-Rootkit** oraz parametry skanowania w poszukiwaniu rootkitów. Test Anti-Rootkit jest domyślnie włączony. Zobacz [Skanuj całego komputera](#):



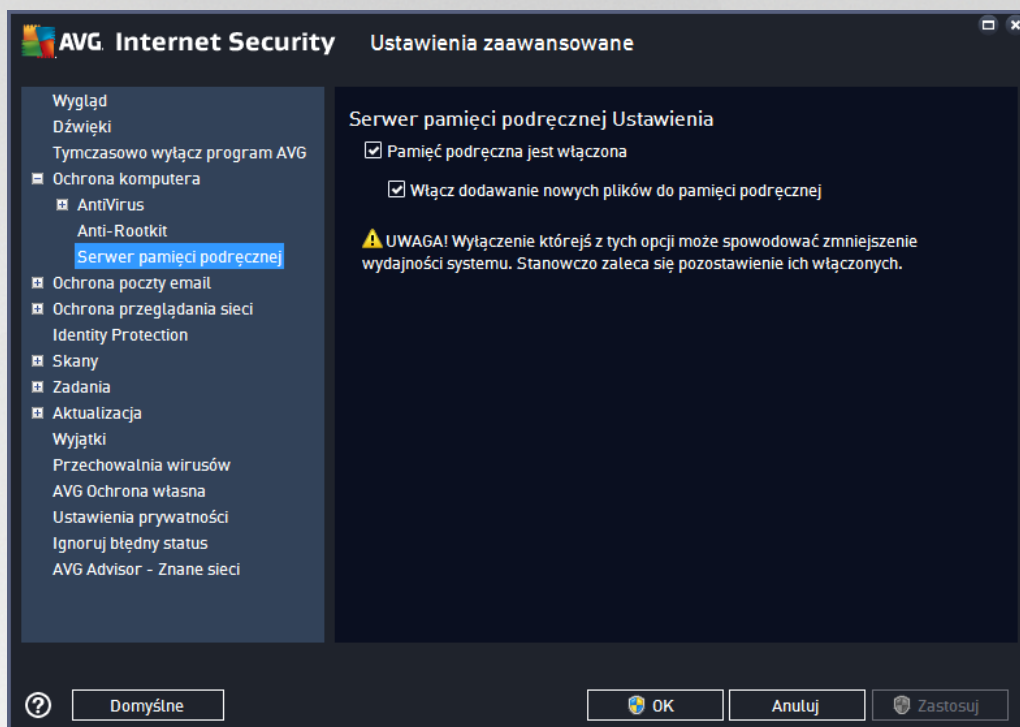
Opcje **Skanuj aplikacje** i **Skanuj napędy** pozwalają szczegółowo określić zakres skanowania Anti-Rootkit. Ustawienia te są przeznaczone dla użytkowników zaawansowanych. Zaleca się pozostawienie wszystkich opcji włączonych. Można również wybrać tryb skanowania w poszukiwaniu rootkitów:

- **Szybkie skanowanie anti-rootkit** — skanuje wszystkie uruchomione procesy, załadowane sterowniki i folder systemowy (zazwyczaj `c:\Windows`)
- **Pełne skanowanie anti-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/płyty CD)



7.4.3. Serwer pamięci podręcznej

Okno **Ustawienia serwera pamięci podręcznej** odnosi się do procesu serwera pamięci podręcznej, który ma za zadanie przyspieszenie wszystkich typów skanowania w programie **AVG Internet Security**:



Serwer pamięci podręcznej zbiera i przechowuje informacje o zaufanych plikach (*tych, które zostały podpisane cyfrowo przez zaufane źródło*). Pliki takie są automatycznie uznawane za bezpieczne, więc nie muszą być powtórnie skanowane i mogą zostać pominięte.

Okno **Ustawienia serwera pamięci podręcznej** zawiera następujące 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 używany plik będzie skanowany w poszukiwaniu wirusów i oprogramowania szpiegującego.
- **Włącz dodawanie nowych plików do pamięci podręcznej** (opcja domyślnie włączona) — usunięcie zaznaczenia tego pola powoduje 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 wirusów.

Jeśli nie masz ważnego powodu, aby wyłączyć serwer pamięci podręcznej, stanowczo zalecamy zachowanie ustawień domyślnych i zostawienie włączonych obu opcji! Uniknij dzięki temu znacznego obniżenia wydajności systemu.

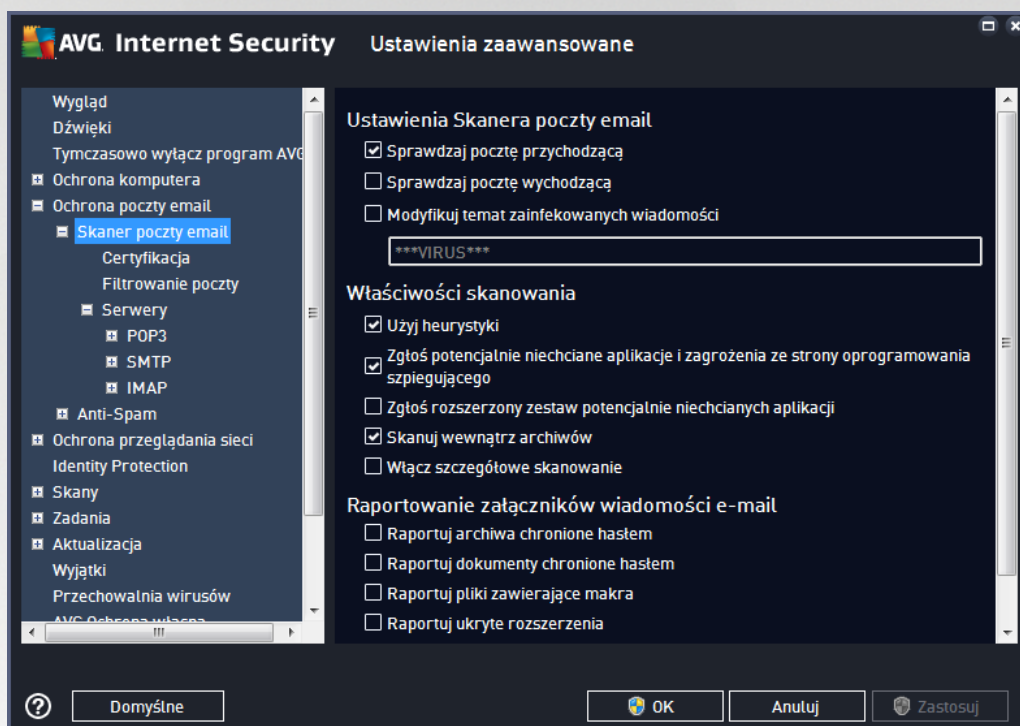


7.5. Skaner poczty e-mail

W tej sekcji można edytować konfigurację składników [Skaner poczty Email](#) oraz [Anti-Spam](#):

7.5.1. Skaner poczty e-mail

Okno dialogowe **Skaner poczty Email** jest podzielone na trzy obszary:



Skanowanie poczty email

W tej sekcji można określić następujące, podstawowe ustawienia dla przychodzących i wychodzących wiadomości e-mail:

- **Sprawdzaj pocztę przychodzącą** (domyślnie włączona) — zaznacz lub odznacz to pole, aby włączyć lub wyłączyć opcję skanowania wszystkich wiadomości e-mail dostarczanych do klienta poczty e-mail.
- **Sprawdzaj pocztę wychodzącą** (domyślnie wyłączona) — zaznacz lub odznacz to pole, aby włączyć lub wyłączyć opcję skanowania wszystkich wiadomości e-mail wysyłanych z klienta poczty e-mail.
- **Modyfikuj temat zainfekowanych wiadomości** (domyślnie wyłączona) — jeżeli chcesz otrzymywać ostrzeżenia o tym, że przeskanowana wiadomość e-mail została zaklasyfikowana jako zainfekowana, zaznacz to pole i wprowadź dany tekst w polu tekstowym. Ten tekst będzie dodawany do pola "Temat" każdej wykrytej zainfekowanej wiadomości e-mail, aby ułatwić ich identyfikowanie i filtrowanie. Warto domyślnie to *****VIRUS*****; zaleca się jej zachowanie.



Właściwości skanowania

W tej sekcji można określić sposób skanowania wiadomości e-mail:

- **Użyj analizy heurystycznej (domyślnie wyłączone)** — 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 potencjalnie niechciane programy oraz oprogramowanie szpiegujące (domyślnie wyłączone)** — zaznacz to pole, aby włączyć skanowanie w poszukiwaniu oprogramowania szpiegującego oprócz 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 włączania tej opcji — znacząco zmniejsza ona poziom ochrony komputera.
- **Raportuj poszerzony zestaw potencjalnie niechcianych programów (domyślnie wyłączone)** — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojemu komputerowi. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego tę opcję domyślnie jest wyłączone.
- **Skanuj wewnątrz archiwów (domyślnie wyłączone)** — zaznaczenie tego pola umożliwia skanowanie zawartości archiwów dołączonych do wiadomości e-mail.
- **Wyłącz szczegółowe skanowanie (domyślnie wyłączone)** — w określonych sytuacjach (np. gdy zachodzi podejrzenie, że komputer jest zainfekowany przez wirus lub zaatakowany) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będzie ono skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest dość czasochłonna.

Raportowanie załączników wiadomości

W tej sekcji można skonfigurować dodatkowe raporty dotyczące potencjalnie niebezpiecznych lub podejrzanych plików. Należy zwrócić uwagę na fakt, że nie zostanie wyświetlone żadne okno dialogowe z ostrzeżeniem, a jedynie na końcu wiadomości e-mail zostanie dodany tekst certyfikacji; wszystkie takie przypadki zostaną wyświetlone w oknie dialogowym [Detekcje Ochrony poczty email](#):

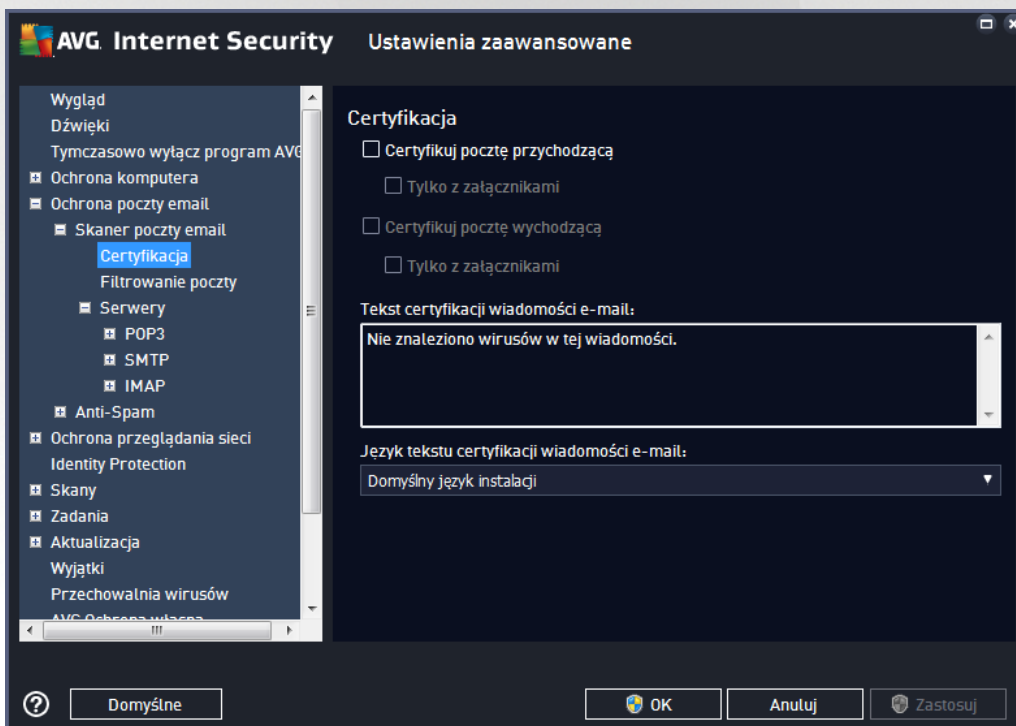
- **Raportuj archiwa chronione hasłem** — archiwów (ZIP, RAR etc.) chronionych hasłem można skanować w poszukiwaniu wirusów. Zaznacz to pole wyboru, aby takie archiwa były zgłaszane jako potencjalnie niebezpieczne.
- **Raportuj dokumenty chronione hasłem** — dokumentów chronionych hasłem można skanować w poszukiwaniu wirusów. Zaznacz to pole wyboru, aby dokumenty takie były zgłaszane jako potencjalnie niebezpieczne.
- **Raportuj pliki zawierające makra** — makro to predefiniowana sekwencja kroków mająca ułatwić wykonywanie określonych czynności (szeroko znane są na przykład makra programu MS Word). Makra mogą być potencjalnie niebezpieczne — warto zaznaczyć to pole, aby mieć pewność, że pliki



zawierające makra będą raportowane jako podejrzane.

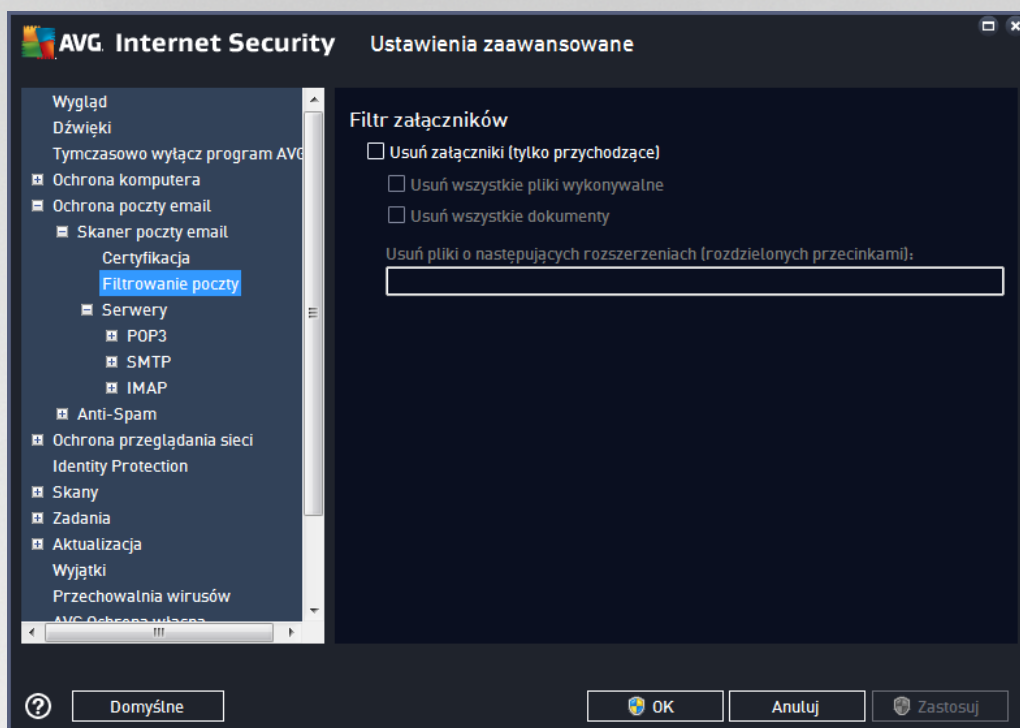
- **Raportuj ukryte rozszerzenia** — ukryte rozszerzenia mogą maskować podejrzane pliki wykonywalne (np. "plik.txt.exe") jako niegroźne pliki tekstowe (np. "plik.txt"). Zaznacz to pole wyboru, aby zgłaszać je jako potencjalnie niebezpieczne.
- **Przeno raportowane załączniki do Przechowalni wirusów** — możesz skonfigurować opcje tak, aby otrzymywać powiadomienia pocztą e-mail o wykrytych archiwach i dokumentach zabezpieczonych hasłem, plikach zawierających makra lub ukrytych rozszerzeniach, które zostaną wykryte w załącznikach skanowanych wiadomości. Określ te, czy w przypadku wykrycia takiej wiadomości podczas skanowania zainfekowany obiekt ma zostać przeniesiony do [Przechowalni wirusów](#).

W oknie **Certyfikacja** znajdują się opcje pozwalające włączyć lub wyłączyć **Certyfikację poczty przychodzącej i wychodzącej**. Zaznaczenie parametru **Tylko z załącznikami** sprawi, że certyfikowane będą jedynie wiadomości zawierające załączniki:



Domyślnie tekst certyfikacji stwierdza, że *Nie znaleziono wirusów w tej wiadomości*. Treść można jednak łatwo zmienić, korzystając z pola **Tekst certyfikacji wiadomości e-mail**, w którym można wpisać odpowiedni tekst. Sekcja **Język tekstu certyfikacji wiadomości e-mail** pozwala na zmianę języka automatycznie generowanej treści certyfikacji (*Nie znaleziono wirusów w tej wiadomości*).

Uwaga: We wskazanym języku będzie wyświetlany jedynie domyślny tekst certyfikacji. Człony zdefiniowane przez użytkownika nie zostaną automatycznie przetłumaczone!



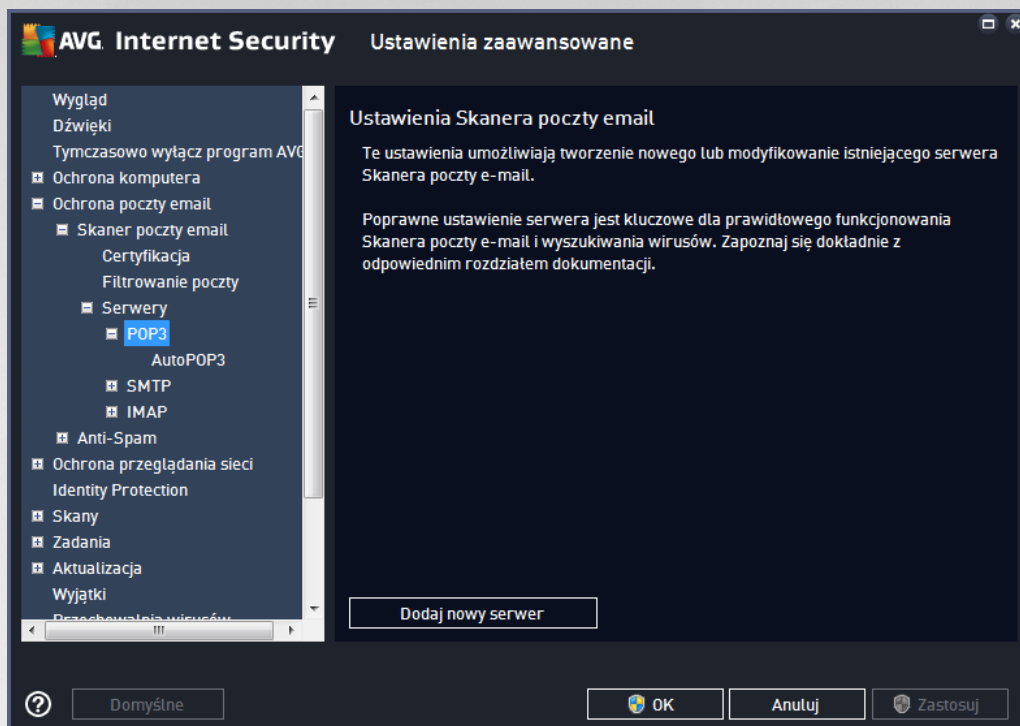
W oknie dialogowym **Filtr załączników** można ustawić parametry skanowania załączników do wiadomości e-mail. Opcja **Usuń załączniki** jest domyślnie wyłączona. Jeśli zostanie włączona, wszystkie załączniki wiadomości zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, będą automatycznie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

- **Usuń wszystkie pliki wykonywalne** — usuwane będą wszystkie pliki *.exe
- **Usuń wszystkie dokumenty** — usuwane będą wszystkie pliki *.doc, *.docx, *.xls, *.xlsx
- **Usuń pliki o następujących rozszerzeniach oddzielonych przecinkami** — usuwane będą wszystkie pliki o zdefiniowanych rozszerzeniach

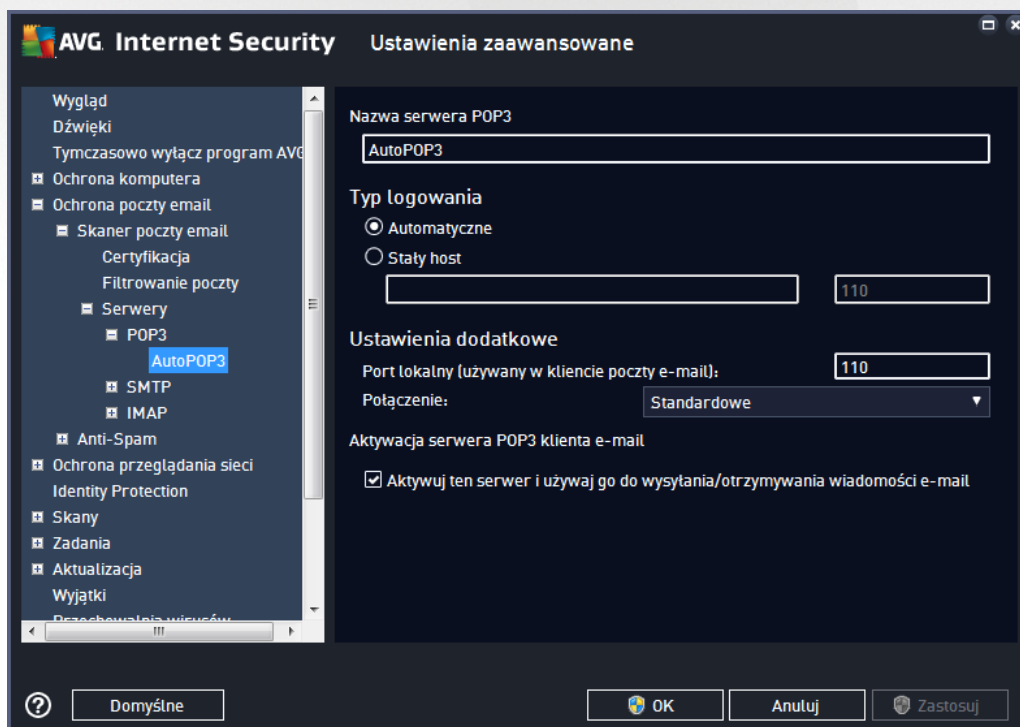
W sekcji **Serwery** edytować można parametry serwerów [Skanera poczty e-mail](#):

- [Serwer POP3](#)
- [Serwer SMTP](#)
- [Serwer IMAP](#)

Dodanie nowego serwera poczty wychodzącej lub przychodzącej możliwe jest za pomocą przycisku **Dodaj nowy serwer**.



W tym oknie dialogowym można zdefiniować na potrzeby [Skanyera poczty email](#) nowy serwer poczty przychodzącej, korzystający z protokołu POP3:

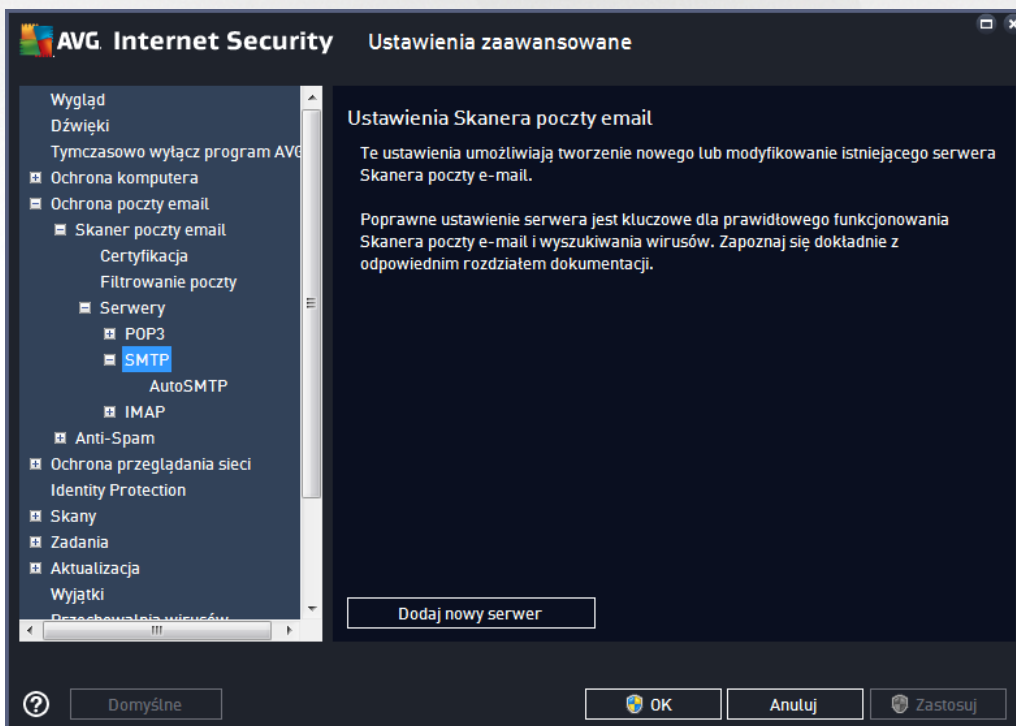


- **Nazwa serwera POP3** — w tym polu można podać nazwę nowo dodanego serwera (aby dodać serwer



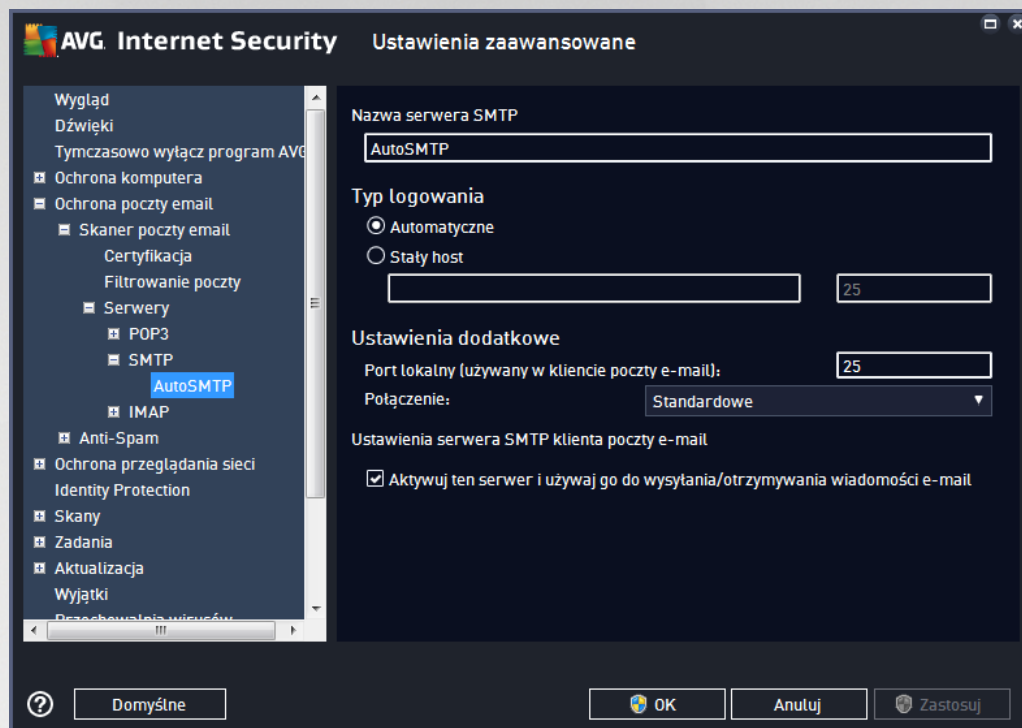
POP3, kliknij prawym przyciskiem myszy pozycję POP3 w menu nawigacyjnym po lewej stronie).

- **Typ logowania** — definiuje metodę określenia serwera pocztowego dla wiadomości przychodzących:
 - **Automatycznie** — logowanie jest przeprowadzane automatycznie zgodnie z ustawieniami klienta poczty e-mail.
 - **Stały host** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Nazwa logowania pozostaje niezmienną. Jako nazwy można użyć nazwy domeny (np. *pop.domena.com*) lub adresu IP (np. *123.45.67.89*). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku, zaraz za nazwą serwera (np. *pop.domena.com:8200*). Standardowym portem do obsługi komunikacji z usługami protokołu POP3 jest 110.
- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
 - **Port lokalny** — określa port komunikacji dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.
 - **Połączenie** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślnie SSL*). Jeśli zostanie wybrane połączenie SSL, wysyłane dane są szyfrowane, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez strony trzecie. Funkcja ta dostępna jest tylko wtedy, gdy obsługujemy docelowy serwer pocztowy.
- **Aktywacja serwera POP3 klienta poczty e-mail** — opcję należy zaznaczyć /odznaczyć, aby aktywować lub dezaktywować określony serwer POP3

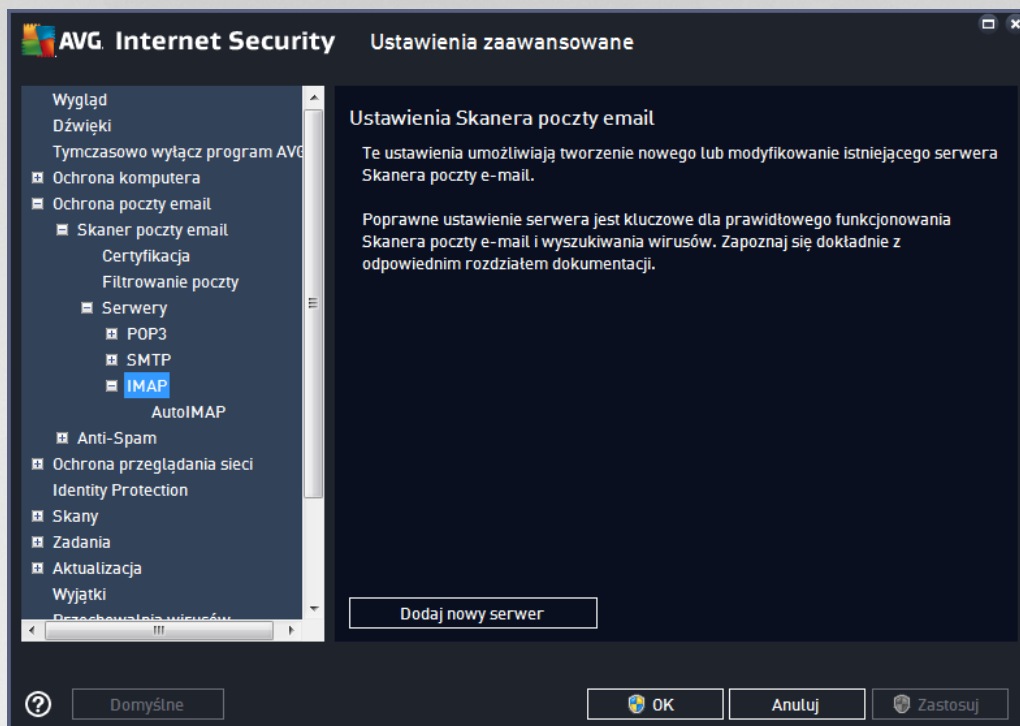


W tym oknie dialogowym można zdefiniować na potrzeby [Skanera poczty Email](#) nowy serwer poczty

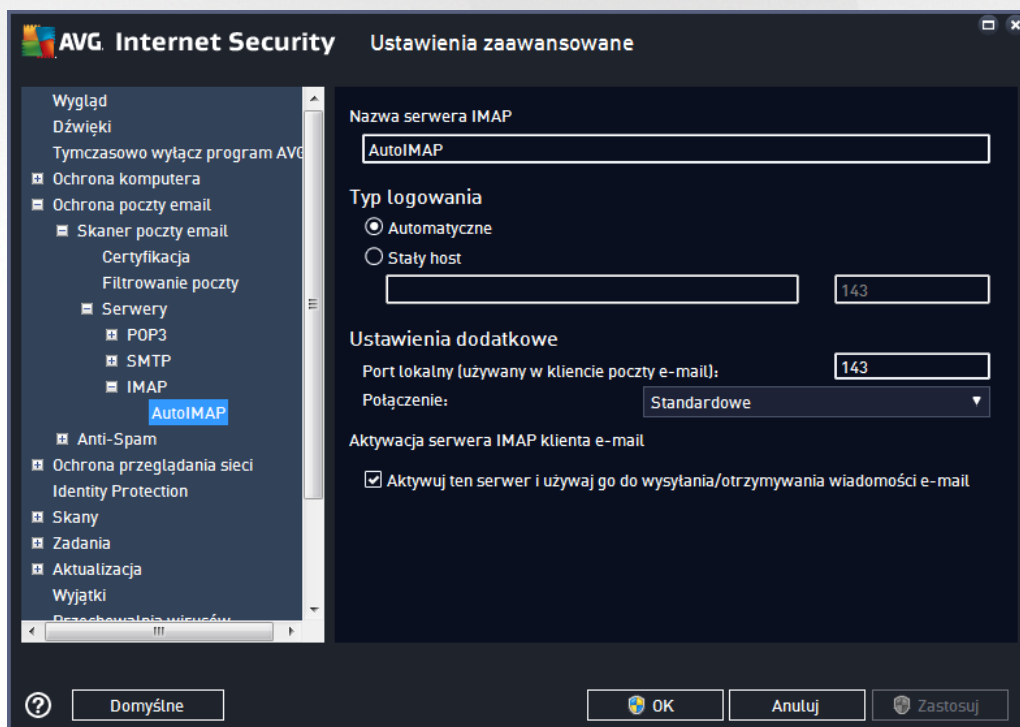
przychodzącej, korzystając z protokołu SMTP:



- **Nazwa serwera SMTP** — w tym polu można podać nazwę nowego dodanego serwera (aby dodać serwer SMTP, kliknij prawym przyciskiem myszy pozycję SMTP w menu nawigacyjnym po lewej stronie). W przypadku automatycznie utworzonych serwerów „AutoSMTP” to pole jest nieaktywne.
- **Typ logowania** — definiuje metodę określenia serwera pocztowego dla wiadomości wychodzących:
 - **Automatycznie** — logowanie jest przeprowadzane automatycznie zgodnie z ustawieniami klienta poczty e-mail
 - **Stały host** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Można użyć nazwy domeny (np. smtp.domena.com) lub adresu IP (np. 123.45.67.89). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku za nazwą serwera (np. smtp.domena.com:8200). Standardowym portem do komunikacji SMTP jest port 25.
- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
 - **Port lokalny** — określa port komunikacji dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port komunikacji SMTP.
 - **Połączenie** — z menu rozwijanego należy wybrać rodzaj używanego połączenia (zwykłe/SSL/domyślne SSL). Jeśli zostanie wybrane połączenie SSL, wysyłane dane są szyfrowane, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez strony trzecie. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje się docelowy serwer pocztowy.
- **Aktywacja serwera SMTP klienta poczty e-mail** — zaznacz/odznacz to pole, aby włączyć/wyłączyć określony powyżej serwer SMTP



W tym oknie dialogowym można zdefiniować na potrzeby [Skanera poczty email](#) nowy serwer poczty wychodzącej, korzystający z protokołu IMAP:



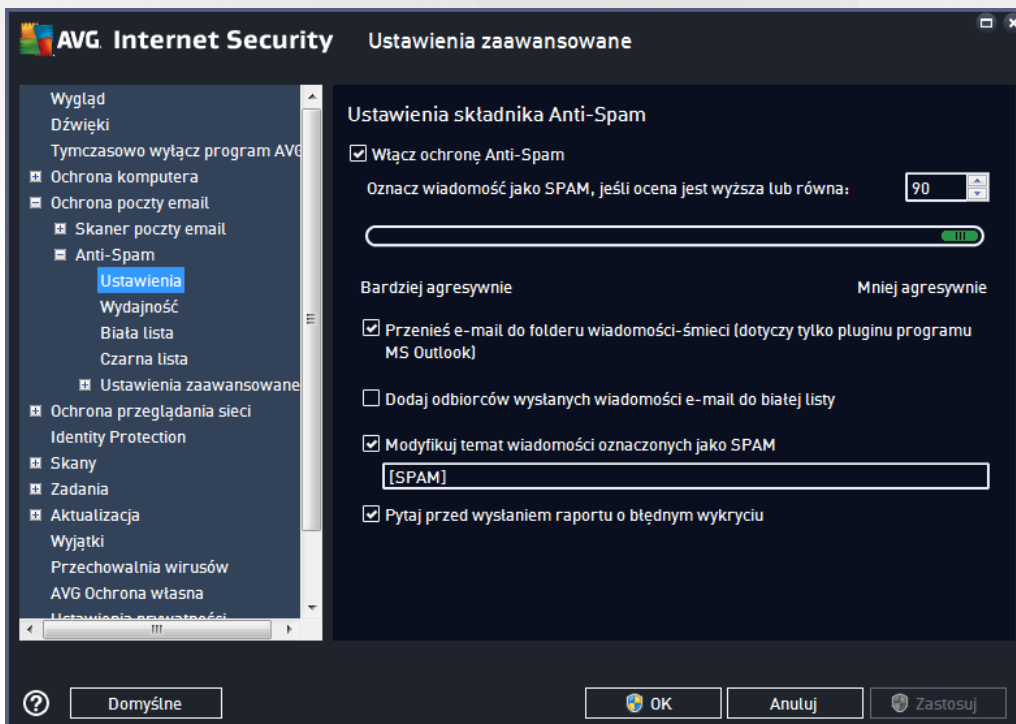
- **Nazwa serwera IMAP** — w tym polu można podać nazwę nowo dodanego serwera (aby dodać serwer



IMAP, kliknij prawym przyciskiem myszy pozycję IMAP w menu nawigacyjnym po lewej stronie).

- **Typ logowania** — definiuje metodę określenia serwera pocztowego dla wiadomości wychodzących:
 - **Automatycznie** — logowanie jest przeprowadzane automatycznie zgodnie z ustawieniami klienta poczty e-mail
 - **Stały host** — po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Można użyć nazwy domeny (np. *smtp.domena.com*) lub adresu IP (np. *123.45.67.89*). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku za nazwą serwera (np. *imap.domena.com:8200*). Standardowym portem protokołu IMAP jest port 143.
- **Ustawienia dodatkowe** — pozwalają zdefiniować bardziej szczegółowe parametry:
 - **Port lokalny używany w** — określa port komunikacji przeznaczony dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port do komunikacji IMAP.
 - **Półczenie** — z menu rozwijanego należy wybrać rodzaj używanego półczenia (*zwykłe/SSL/domyślnie SSL*). Jeśli zostanie wybrane półczenie SSL, dane będą szyfrowane, co zmniejsza ryzyko ich kradzieży lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
- **Aktywacja serwera IMAP klienta poczty e-mail** — zaznacz/odznacz to pole, aby włączyć/wyłączyć określony powyżej serwer IMAP

7.5.2. Anti-Spam



W oknie dialogowym **Ustawienia składowki Anti-Spam** można zaznaczyć pole **Włącz ochronę Anti-Spam**



(albo usun jego zaznaczenie), aby włączyć (lub wyłączyć) skanowanie wiadomości e-mail w poszukiwaniu spamu. Ta opcja jest domyślnie włączona i jak zwykle nie zaleca się zmiany jej konfiguracji bez ważnego powodu.

W tym samym oknie można także wybrać mniej lub bardziej agresywne poziomy oceny. Filtr **Anti-Spam** przypisuje każdej wiadomości ocenę (tj. *wskazanie, jak bardzo jej treść przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. Ustawienie **Oznacz wiadomość jako spam, jeśli ocena jest wyższa niż** można dostosować, wpisując wartość lub przesuwając suwak w lewo albo w prawo.

Wartości muszą mieścić się w zakresie od 50 do 90. Poniżej przedstawiono opis progów oceny:

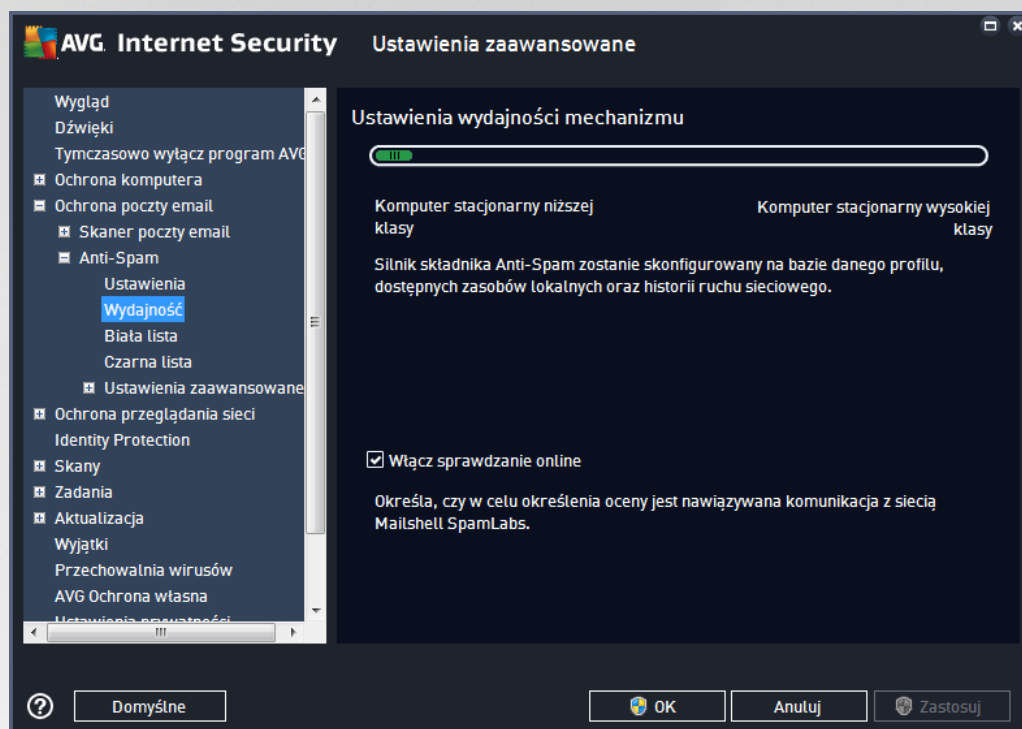
- **Wartość 80-90** — wiadomości e-mail, które stanowią potencjalny spam, są poprawnie odfiltrowywane. Niektóre z wiadomości, które nie są spamem, mogą także zostać przypadkowo odfiltrowane.
- **Wartość 60-79** — umiarkowanie agresywna konfiguracja. Wiadomości e-mail, które mogą stanowić spam, są poprawnie odfiltrowywane. Po dane wiadomości (które nie są spamem) mogą zostać przypadkowo zablokowane.
- **Wartość 50-59** — bardzo agresywna konfiguracja. Po dane wiadomości e-mail są odfiltrowywane w równym stopniu co wiadomości stanowiące spam. **Nie zalecamy stosowania tego progu podczas normalnej pracy.**

W oknie **Ustawienia podstawowe** można również dokładniej zdefiniować sposób traktowania spamu wykrytego w wiadomościach e-mail:

- **Przenieś wiadomość do folderu wiadomości-mieci (tylko plugin Microsoft Outlook)** — jeśli ta opcja jest zaznaczona, wykryty spam będzie automatycznie przenoszony do wskazanego folderu wiadomości-mieci w kliencie poczty e-mail MS Outlook. Obecnie funkcja ta nie jest obsługiwana przez pozostałych klientów poczty e-mail.
- **Dodaj odbiorców wysłanych wiadomości e-mail do białej listy** — zaznacz to pole, aby potwierdzić, że masz zaufanie do odbiorców wysłanych przez Ciebie wiadomości e-mail, a wiadomości z ich kont ma zawsze być dostarczana.
- **Zmodyfikuj temat wiadomości oznaczonych jako spam** — jeśli opcja ta jest zaznaczona, wszystkie wykryte wiadomości zawierające spam będą oznaczane (w temacie) wskazanym frazami lub znakiem; dany tekst można wpisać w polu znajdującym się poniżej.
- **Pytaj przed wysłaniem raportu o bieżącym wykryciu** — opcja ta jest dostępna, jeśli podczas instalacji użytkownik zdecydował się uczestniczyć w projekcie [Ustawienia prywatności](#). Zgoda ta jest równoznaczna z raportowaniem wykrytych zagrożeń firmie AVG. Raporty tworzone są automatycznie. Można jednak zaznaczyć to pole wyboru, aby przed wysłaniem raportu o wykrytym spamie do firmy AVG było wyświetlane pytanie, czy dana wiadomość faktycznie zawiera spam.



Okno **Ustawienia wydajności mechanizmu** (poł czone elementem **Wydajność** z lewej cz ci okna nawigacji) oferuje ustawienia wydajności składnika **Anti-Spam**:



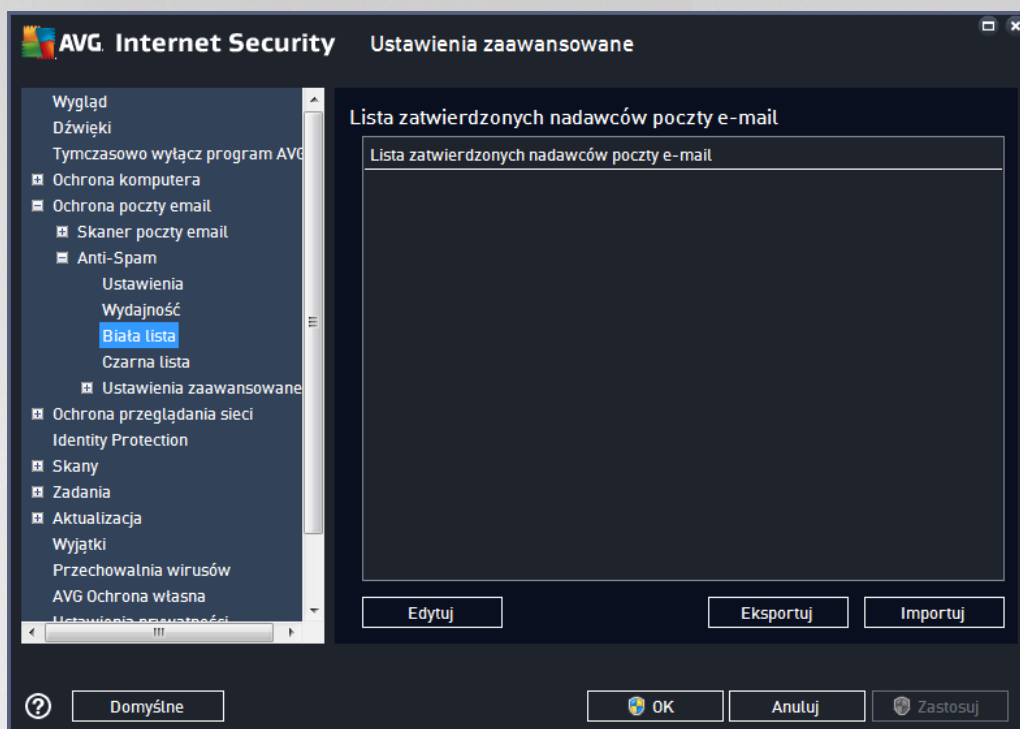
Przesu suwak w lewo lub w prawo, aby zmieni poziom wydajności skanowania pomiędzy opcjami **Komputer ni szej klasy** / **Komputer wysokiej klasy**.

- **Komputer ni szej klasy** — podczas skanowania w poszukiwaniu spamu adne reguły nie b d brane pod uwag . Tylko dane szkoleniowe s u ywane do identyfikacji. Ten tryb nie jest zalecany do cz stego stosowania, chyba e konfiguracja sprz towa komputera jest bardzo słaba.
- **Komputer wysokiej klasy** — tryb ten zajmie znacz n ilo pami ci. W czasie skanowania w poszukiwaniu spamu stosowane b d nast puj ce funkcje: pami podr czna dla reguł i definicji spamu, reguły podstawowe i zaawansowane, adresy IP spamerów i inne bazy danych.

Opcja **Wł cz sprawdzanie online** jest domy lnie wł czona. Pozwala ona skuteczniej wykrywa spam dzi ki współpracy z serwerami [Mailshell](#). Skanowane dane s porównywane z bazami danych online firmy [Mailshell](#).

Zwykle zaleca si zachowanie ustawie domy lnych i zmian ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny by wprowadzane wył cznie przez u ytkowników, którzy doskonale wiedz , co robi !

Klikni cie elementu **Biała lista** pozwala otworzy okno dialogowe **Lista zatwierdzonych nadawców poczty e-mail** zawieraj ce list akceptowanych adresów nadawców i nazw domen, z których wysyłane wiadomo ci nigdy nie s oznaczane jako spam.



W interfejsie tym można utworzyć listę nadawców, którzy nigdy nie wysyłają niepożądanych wiadomości (spamu). Można tak również utworzyć listę nazw całych domen (np. *avg.com*), które nie wysyłają spamu. Jeśli lista adresów nadawców i/lub nazw domen jest już gotowa, jej elementy można wprowadzać pojedynczo lub importować wszystkie adresy jednocześnie.

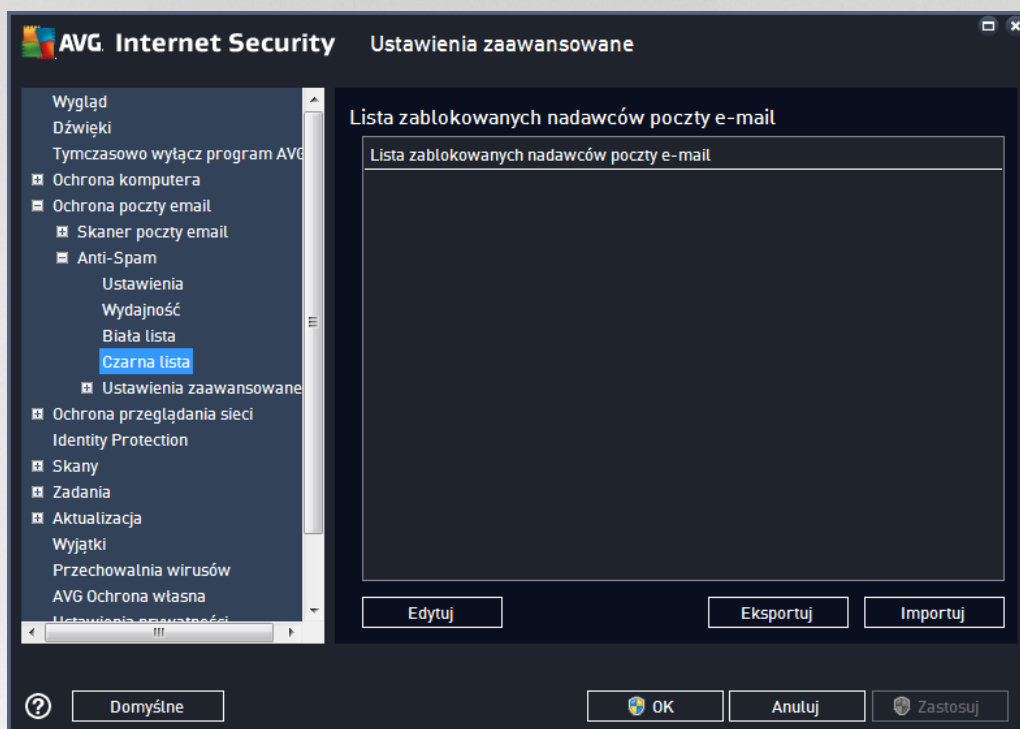
Przyciski kontrolne

Dostępne są następujące przyciski kontrolne:

- **Edytuj** — przycisk ten służy do otwarcia okna dialogowego, w którym można ręcznie wprowadzić listę adresów (również za pomocą metody „kopiuj i wklej”). Każdą pozycję (*nadawca lub nazwa domeny*) należy wprowadzić w osobnym wierszu.
- **Eksportuj** — jeśli z jakiegoś powodu chcesz wyeksportować wpisy, możesz użyć tego przycisku. Wszystkie wpisy zostaną zapisane w zwykłym pliku tekstowym.
- **Importuj** — jeśli masz plik tekstowy z adresami e-mail lub nazwami domen, możesz go zaimportować za pomocą tego przycisku. Plik musi zawierać w każdym wierszu dokładnie jedną pozycję (*adres, nazwa domeny*).



Kliknięcie pozycji **Czarna lista** pozwala otworzyć globalną listę zablokowanych adresów indywidualnych nadawców i domen, z których wiadomości ci zawsze są oznaczane jako spam.



W interfejsie edycji można utworzyć listę nadawców, którzy wysyłają lub prawdopodobnie kiedyś wysłali niepożądane wiadomości (*spam*). Można tak też utworzyć listę pełnych nazw domen (*np. spammingcompany.com*), z których otrzymujesz (lub spodziewasz się otrzymywać) spam. Wszystkie adresy e-mail z listy tych adresów/domen będą identyfikowane jako spam. Jeśli lista adresów nadawców i/lub nazw domen jest już gotowa, jej elementy można wprowadzać pojedynczo lub importować wszystkie adresy jednocześnie.

Przyciski kontrolne

Dostępne są następujące przyciski kontrolne:

- **Edytuj** — przycisk ten służy do otwarcia okna dialogowego, w którym można ręcznie wprowadzić listę adresów (również za pomocą metody „kopiuj i wklej”). Każdą pozycję (*nadawca lub nazwa domeny*) należy wprowadzić w osobnym wierszu.
- **Eksportuj** — jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, możesz użyć tego przycisku. Wszystkie wpisy zostaną zapisane w zwykłym pliku tekstowym.
- **Importuj** — jeżeli masz plik tekstowy z adresami e-mail lub nazwami domen, możesz go zaimportować za pomocą tego przycisku.



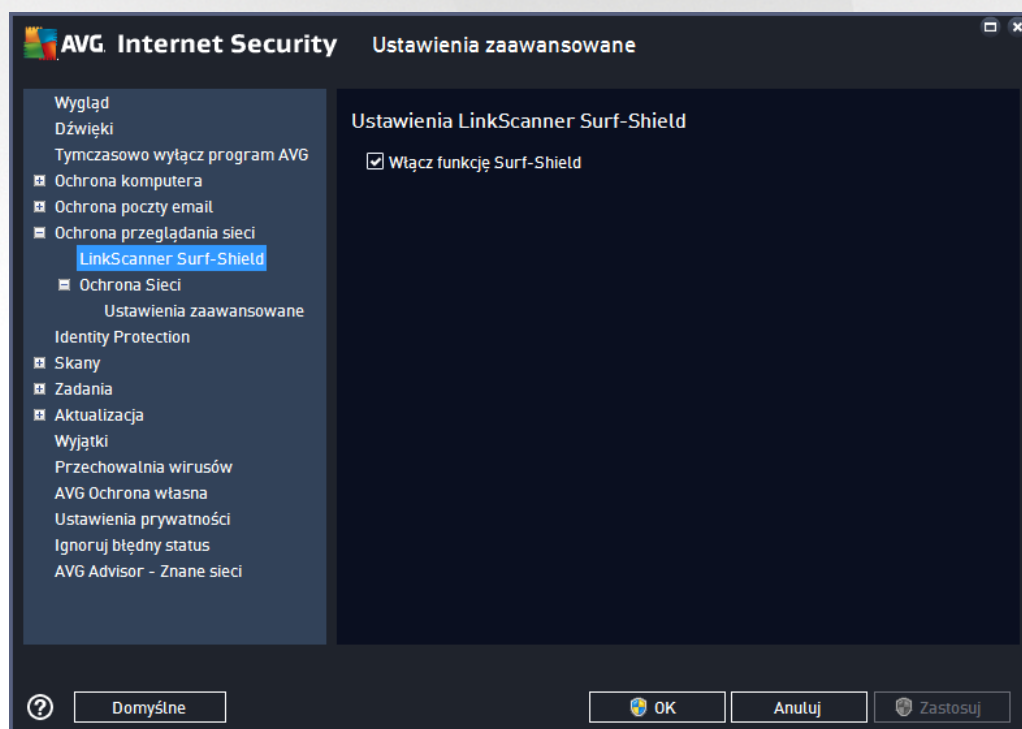
Gał Ustawienia eksperta zawiera wiele dodatkowych opcji funkcji Anti-Spam. Ustawienia te s przeznaczone wył cznie dla do wiadczonych u ytkowników (zwykle administratorów sieci), którzy chc szczególnie skonfigurowa filtry antyspamowe w celu uzyskania optymalnej ochrony serwerów poczty. Z tego wzgl du nie istnieją tematy pomocy dla poszczególnych okien dialogowych, a jedynie krótkie opisy odpowiednich opcji, dost pne bezpo rednio w interfejsie u ytkownika. Stanowczo zalecamy pozostawienie tych ustawie bez zmian, je li nie posiadasz pełnej wiedzy na temat zaawansowanych ustawie silnika antyspamowego Spamcatcher (MailShell Inc.). Nieodpowiednie zmiany mog skutkowa obni on wydajno ci lub nieprawidłowym działaniem składnika.

Aby mimo wszystko zmieni konfiguracj składnika Anti-Spam na bardzo zaawansowanym poziomie, nale y post powa zgodnie z instrukcjami wy wietlanymi w interfejsie u ytkownika. W ka dym oknie znajdziesz jedn , konkretn funkcj , któr mo esz edytowa . Jej opis jest zawsze widoczny w tym samym oknie. Mo esz edytowa nast puj ce parametry:

- **Filtry** — lista j zyków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, fałszywi nadawcy
- **RBL** — serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba adresów IP
- **Poł czenie internetowe** — limit czasu, serwer proxy, uwierzytelnianie na serwerze proxy

7.6. Ochrona przeglądania sieci

Okno **Ustawienia LinkScanner** pozwala zaznaczy /odznaczy nast puj ce funkcje:

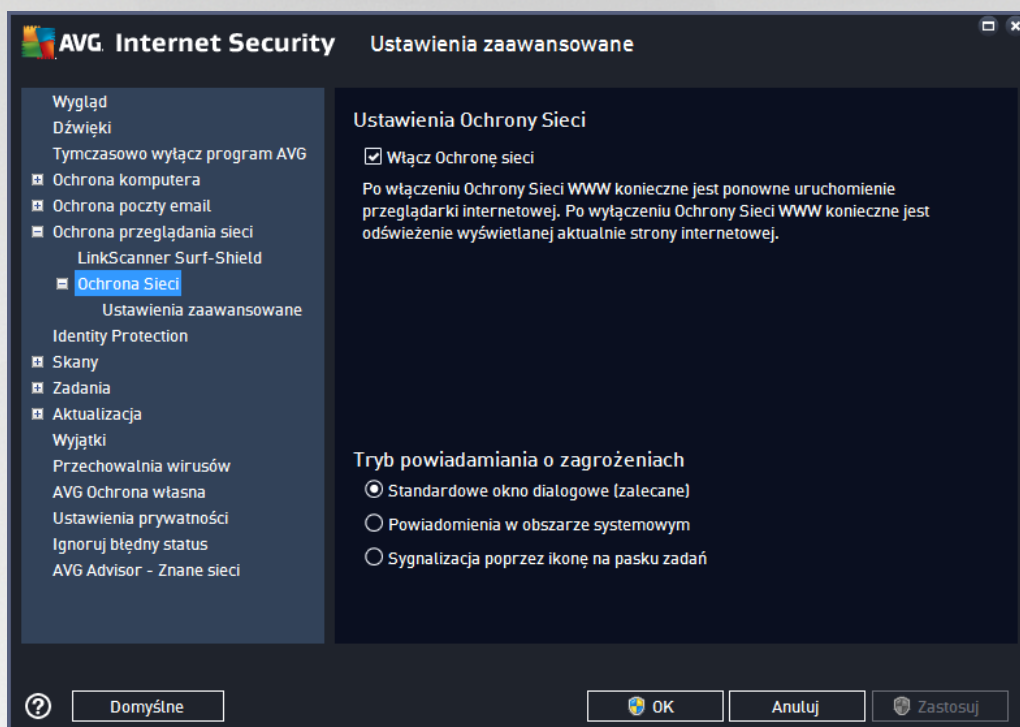


- **Wł cz funkcj Surf-Shield** — (domy lnie wł czona): aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (w czasie rzeczywistym). Znane złe witryny i ich niebezpieczna zawarto blokowane s ju w momencie otwarcia ich przez u ytkownika za pomoc



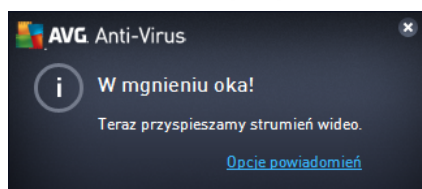
przeładowanie (lub jakiegokolwiek innej aplikacji korzystającej z protokołu HTTP).

7.6.1. Ochrona Sieci



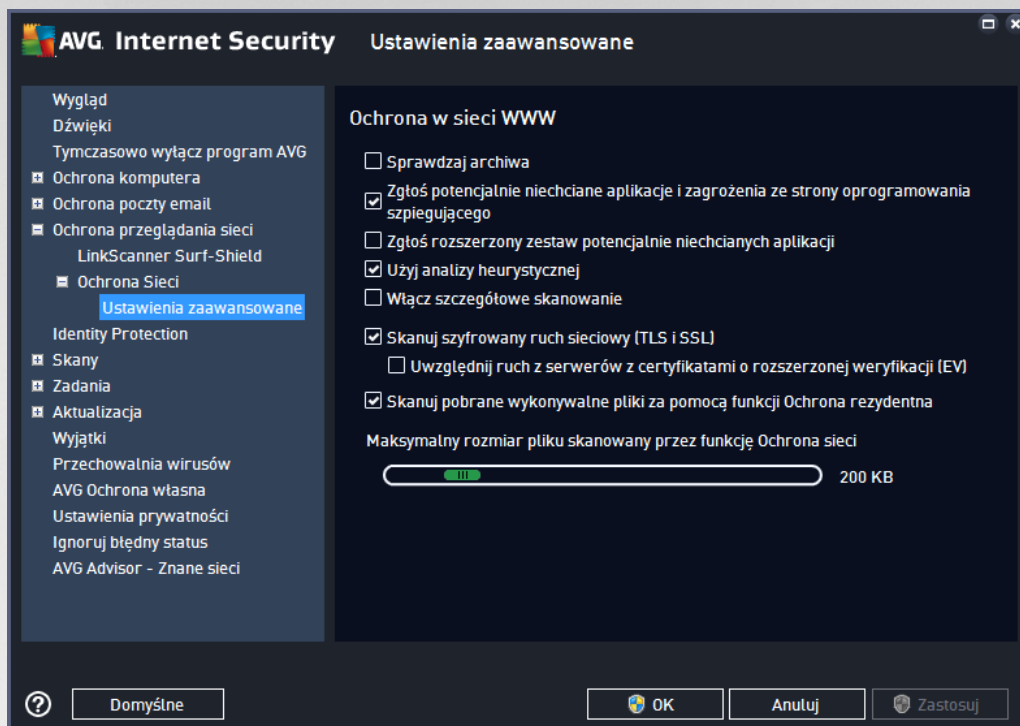
Okno **Ochrona Sieci** zawiera następujące opcje:

- **Włącz Ochronę Sieci** (domyślnie włączona) — włącza/wyłącza wszystkie usługi składnika **Ochrona Sieci**. Zaawansowane ustawienia **Ochrony Sieci** znajdują się w kolejnym oknie, nazwanym [Ochrona w Internecie](#).
- **Włącz AVG Accelerator** (domyślnie włączona) — włącza/wyłącza usługę AVG Accelerator. Usługa AVG Accelerator pozwala na płynniejsze odtwarzanie filmów online i łatwiejsze pobieranie dodatkowych plików. W czasie działania składnika AVG Accelerator będzie wyświetlane odpowiednie powiadomienie nad ikoną AVG w zasobniku systemowym:



Tryb powiadamiania o zagrożeniach

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



W oknie dialogowym **Ochrona w Internecie** można edytować konfigurację składnika dotyczącego skanowania zawartości witryn internetowych. Interfejs pozwala modyfikować następujące ustawienia:

- **Sprawdzaj archiwa** — (domyślnie wyłączone): skanowanie ma obejmować także archiwa zawarte na wyświetlanych stronach internetowych.
- **Raportuj potencjalnie niechciane aplikacje oraz oprogramowanie szpiegujące** (domyślnie wyłączone): zaznaczenie tego pola umożliwia skanowanie 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 zniższa ona poziom ochrony komputera.
- **Zgłoś rozszerzony zestaw potencjalnie niechcianych aplikacji** — (domyślnie wyłączone): zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojemu komputerowi. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego tę domyślnie jest wyłączone.
- **Użyj heurystyki** (domyślnie wyłączone): skanowanie zawartości wyświetlanych stron może wykorzystywać analizę heurystyczną (*dynamiczną emulację instrukcji skanowanego obiektu w wirtualnym środowisku*).
- **Włącz szczegółowe skanowanie** (domyślnie wyłączone): w określonych sytuacjach (gdy zachodzi podejrzenie, że komputer jest zainfekowany) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewnością należy



one skanowa nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest dość czasochłonna.

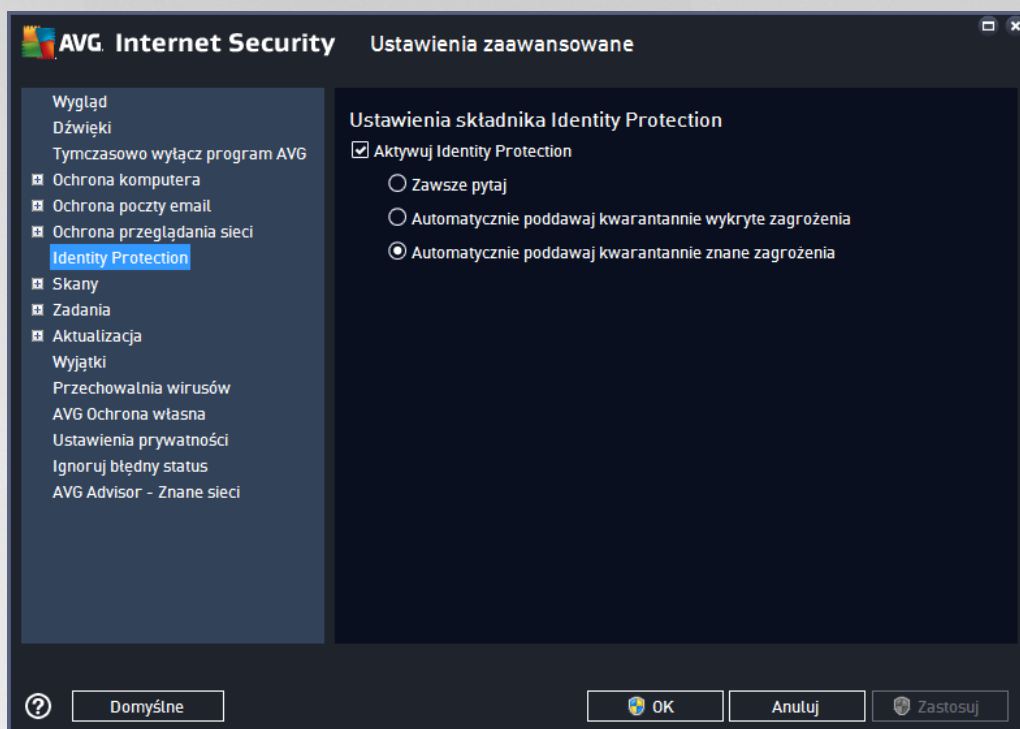
- **Skanuj szyfrowany ruch sieciowy (TLS i SSL)** — (domyślnie włączone): pozostaw tę opcję zaznaczoną, aby program AVG skanował także całą szyfrowaną komunikację sieciową, czyli połączenia obsługiwane za pomocą protokołów zabezpieczeń (SSL i jego nowszej wersji — TLS). To ustawienie dotyczy witryn internetowych korzystających z protokołu HTTPS oraz połączeń z klientami e-mail korzystających z protokołu TLS/SSL. Objęty ochroną ruch sieciowy zostaje odszyfrowany, przeskanowany pod kątem złośliwego oprogramowania i ponownie zaszyfrowany w celu bezpiecznego dostarczenia do komputera. W ramach tej opcji możesz wybrać ustawienie **Uwzględnij ruch z serwerów z certyfikatami o rozszerzonej weryfikacji (EV)**, aby skanować także szyfrowaną komunikację sieciową z serwerów z certyfikatem o rozszerzonej weryfikacji. Wystawienie certyfikatu EV wymaga rozszerzonej weryfikacji ze strony urzędu certyfikacji. Dlatego witryny internetowe posiadające taki certyfikat są bardziej zaufane (*występuje mniejsze prawdopodobieństwo, że rozpowszechnią złośliwe oprogramowanie*). Z tego powodu możesz nie zdecydować się na skanowanie ruchu przychodzącego z serwerów z certyfikatem EV, co nieco przyspieszy obsługę komunikacji szyfrowanej.
- **Skanuj pobrane wykonywalne pliki za pomocą funkcji Ochrona rezydentna** — (domyślnie włączone): skanowanie plików wykonywalnych (*typowe rozszerzenia to exe, bat i com*) po ich pobraniu. Działanie Ochrony rezydentnej polega na skanowaniu plików przed ich pobraniem w celu zapewnienia, że żaden złośliwy kod nie dostanie się do komputera. Ten rodzaj skanowania jest jednak ograniczony wartością opcji **Maksymalny rozmiar czynnika skanowanego pliku** — zobacz następny element w tym oknie dialogowym. Z tego względu duże pliki są skanowane czynniami (dotyczy to także wirusów i plików wykonywalnych). Pliki wykonywalne mogą wykonywać różne zadania w komputerze, dlatego powinny być w 100% bezpieczne. Ich bezpieczeństwo można zapewnić, skanując je jeszcze przed pobraniem oraz całe pliki po pobraniu. Zalecamy pozostawienie zaznaczenia tej opcji. W przypadku odznaczenia tej opcji oprogramowanie AVG może nadal wykrywać potencjalnie niebezpieczny kod. W niektórych przypadkach nie będzie jednak możliwe zbadanie pliku wykonywalnego jako całości, co może czasami prowadzić do wywołania fałszywych alarmów.

Suwak w dolnej części tego okna dialogowego umożliwia zdefiniowanie wartości **Maksymalny rozmiar czynnika skanowanego pliku** — jeżeli wywołana strona zawiera pliki, można skanować ich zawartość jeszcze przed pobraniem na dysk twardy. Ponieważ jednak skanowanie obszernych plików zajmuje dużo czasu, otwieranie stron internetowych może zostać znacznie spowolnione. Za pomocą tego suwaka można określić maksymalny rozmiar plików, które mają być skanowane przez składnik **Ochrona Sieci**. Nawet jeżeli pobierany plik jest większy od wybranego limitu i nie zostanie przeskanowany przez Ochronę Sieci, nie zmniejsza to Twojego bezpieczeństwa: jeżeli plik jest zainfekowany, **Ochrona rezydentna** natychmiast to wykryje.

7.7. Identity Protection

Identity Protection to składnik chroniący przed wszelkimi rodzajami złośliwego kodu (*oprogramowanie szpiegujące, boty, kradzieże tożsamości*) przy użyciu technologii behawioralnych zdolnych wykrywać również najnowsze wirusy (*szczegółowy opis funkcji składnika znajduje się w rozdziale [Identity Protection](#)*).

Okno dialogowe **Ustawienia Identity Protection** umożliwia włączenie/wyłączenie podstawowych funkcji składnika [Identity Protection](#):



Aktywuj Identity Protection (opcja domyślnie wyłączona) — usuź zaznaczenie tego pola, aby wyl czy składnik [To samo](#). **Stanowczo odradza si wyl czenie tej funkcji bez wa nego powodu!** Je li składnik Identity Protection jest aktywny, mo na okre li jego zachowanie w przypadku wykrycia zagro enia:

- **Zawsze pytaj** — w przypadku wykrycia zagro enia u ytkownik zostanie zapytany, czy dany proces ma zosta poddany kwarantannie. Dzi ki temu aplikacje, które maj zosta uruchomione, nie zostan usuni te.
- **Automatycznie poddawaj kwarantannie wykryte zagro enia** — zaznacz to pole wyboru, aby wszystkie wykryte zagro enia były natychmiast przenoszone w bezpieczne miejsce (do [Przechowalni wirusów](#)). Je li ustawienia domyślne zostaną zachowane, w przypadku wykrycia zagro enia u ytkownik zostanie zapytany, czy dany proces ma zosta przeniesiony do kwarantanny. Dzi ki temu aplikacje, które maj pozosta uruchomione, nie zostaną usuni te.
- **Automatycznie poddawaj kwarantannie znane zagro enia** (opcja domyślnie wyłączona) — zaznaczenie tej opcji powoduje, e wszystkie aplikacje uznane za potencjalnie zło liwe oprogramowanie s automatycznie i natychmiast poddawane kwarantannie (przenoszone do [Przechowalni wirusów](#)).

7.8. Skany

Zaawansowane ustawienia skanowania s podzielone na cztery kategorie odnosz ce si do okre lonych typów testów:

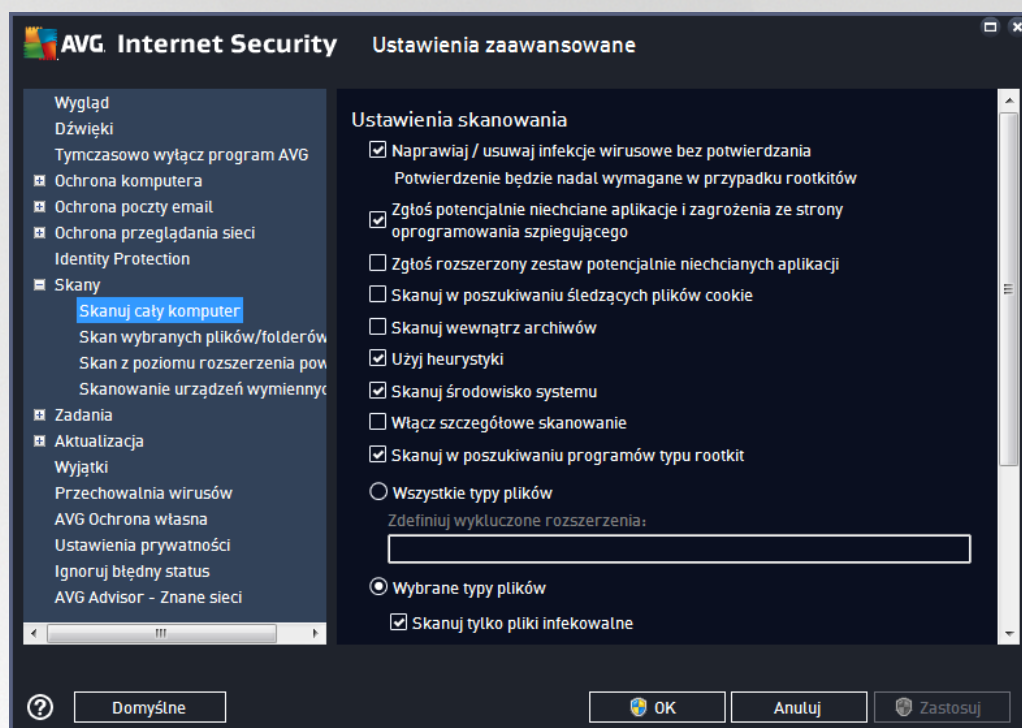
- [Skan całego komputera](#) — standardowe, zdefiniowane wst pnie skanowanie całego komputera.
- [Skan wybranych plików lub folderów](#) — standardowe, zdefiniowane wst pnie skanowanie wskazanych obszarów komputera



- [Skan rozszerzenia powłoki](#) — skanowanie wybranych obiektów bezpośrednio z interfejsu Eksploratora Windows.
- [Skan urządzeń wymiennych](#) — skanowanie urządzeń wymiennych podłączonych do komputera.

7.8.1. Skan całego komputera

Opcja **Skan całego komputera** umożliwia edycję parametrów jednego z testów zdefiniowanych wcześniej przez dostawcę oprogramowania, tj. [Skan całego komputera](#):



Ustawienia skanowania

Obszar **Ustawienia skanowania** zawiera listę parametrów skanowania, które można włączyć i wyłączyć:

- **Naprawiaj / usuwaj infekcje wirusowe bez potwierdzenia** (domyślnie włączone) — jeżeli podczas skanowania zostanie wykryty wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeżeli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane programy oraz oprogramowanie szpiegujące** (domyślnie włączone) — zaznacz to pole, aby włączyć skanowanie w poszukiwaniu oprogramowania szpiegującego oprócz 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 zmniejsza ona poziom ochrony komputera.
- **Raportuj poszerzony zestaw potencjalnie niechcianych programów** (domyślnie wyłączone) — zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli



programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio 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 tę domyślnie jest wyłączona.

- **Skanuj w poszukiwaniu ledzych plików cookie** (domyślnie wyłączona) — ten parametr określa, czy wykrywane mają być pliki cookie; (używane w protokole HTTP do uwierzytelniania, ledzenia i przechowywania określonych informacji o użytkownikach, np. preferencji wyglądu witryny i zawartości koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** (domyślnie wyłączona) — ten parametr określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.
- **Użyj heurystyki** (domyślnie włączona) — analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej) jest jedną z metod wykrywania wirusów w czasie skanowania.
- **Skanuj środowisko systemu** (domyślnie włączona) — skanowanie obejmie także obszary systemowe komputera.
- **Włącz szczegółowe skanowanie** (domyślnie włączona) — w określonych sytuacjach (gdy zachodzi podejrzenie, że komputer jest zainfekowany) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będzie one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest dość czasochłonna.
- **Skanuj w poszukiwaniu programów typu rootkit** (domyślnie włączona) — skan [Anti-Rootkit](#) sprawdza komputer pod kątem rootkitów, czyli programów i technik pozwalających ukryć działanie szkodliwego oprogramowania. Wykrycie programu typu rootkit nie jest równoznaczne z tym, że komputer jest zainfekowany. W niektórych przypadkach pewne sterowniki lub elementy zwykłych aplikacji mogą omyłkowo zostać zaklasyfikowane jako programy typu rootkit.

Możesz także zdecydować, czy chcesz wykonać skanowanie

- **Wszystkie typy plików** z opcji zdefiniowania wytyków skanera przez wprowadzenie rozdzielonych przecinkami rozszerzeń plików (po zapisaniu przecinki zostają zamienione na redniki), które mają być pomijane.
- **Wybrane typy plików** — skanowane będą tylko pliki, które mogą zostać zainfekowane (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 — jeżeli to pole pozostanie niezaznaczone, czas skanowania 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 wybrać pozycję **Skanowanie plików bez rozszerzenia** — ta opcja jest domyślnie wyłączona i zaleca się, aby nie zmieniać tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane łącznie.

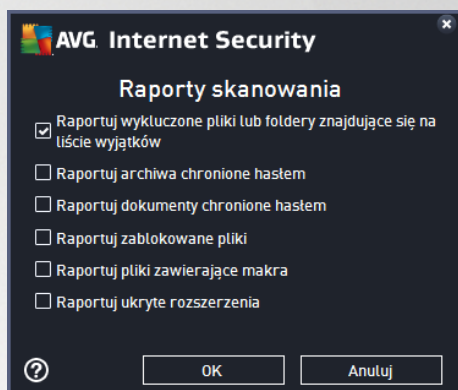


Określ, jak długo ma trwać skanowanie

W obszarze **Określ, jak długo ma trwać skanowanie** można określić czas trwania skanowania, która jest zależna od poziomu wykorzystania zasobów systemowych. Domyślną wartością tej opcji to poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Jeżeli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowodować działanie innych procesów i aplikacji (opcji można miało używać wtedy, gdy komputer jest wyłączony, ale nikt na nim nie pracuje). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

Ustaw dodatkowe raporty skanowania...

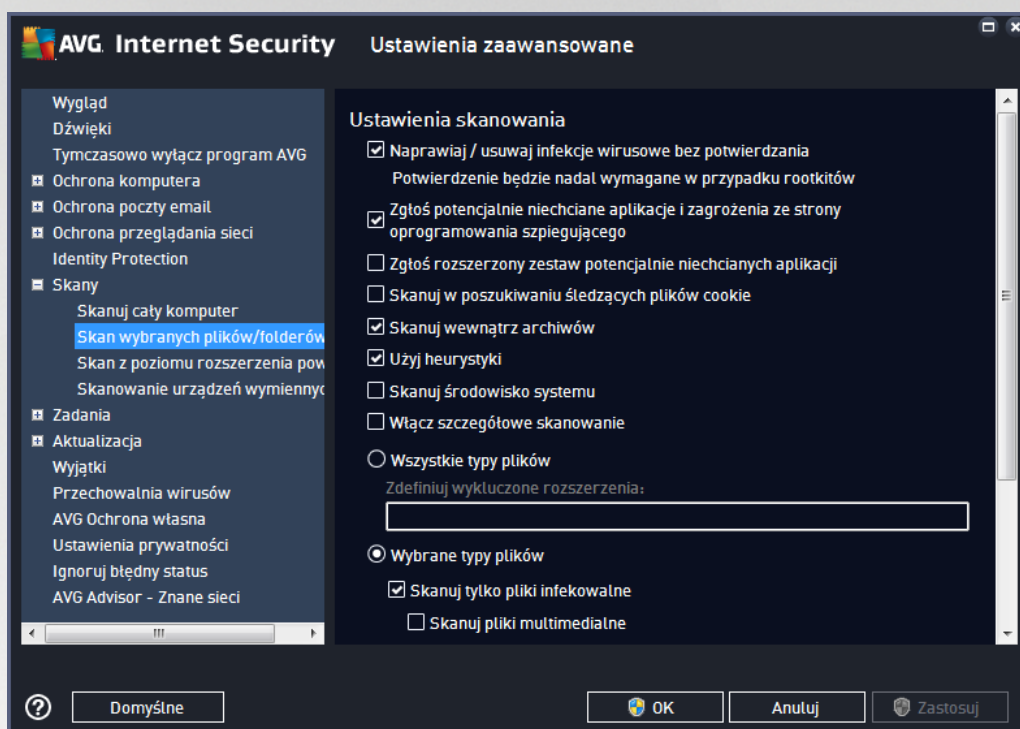
Kliknięcie linku **Ustaw dodatkowe raporty skanowania** powoduje otwarcie osobnego okna dialogowego **Raporty skanowania**, w którym można określić szczegółowo raportów, zaznaczając dane elementy:





7.8.2. Skan wybranych plików/folderów

Interfejs edycji **Skanuj wybrane pliki lub foldery** jest prawie identyczny jak okno dialogowe [Skan całego komputera](#), ale w przypadku okna [Skan całego komputera](#) ustawienia domyślne są bardziej restrykcyjne:

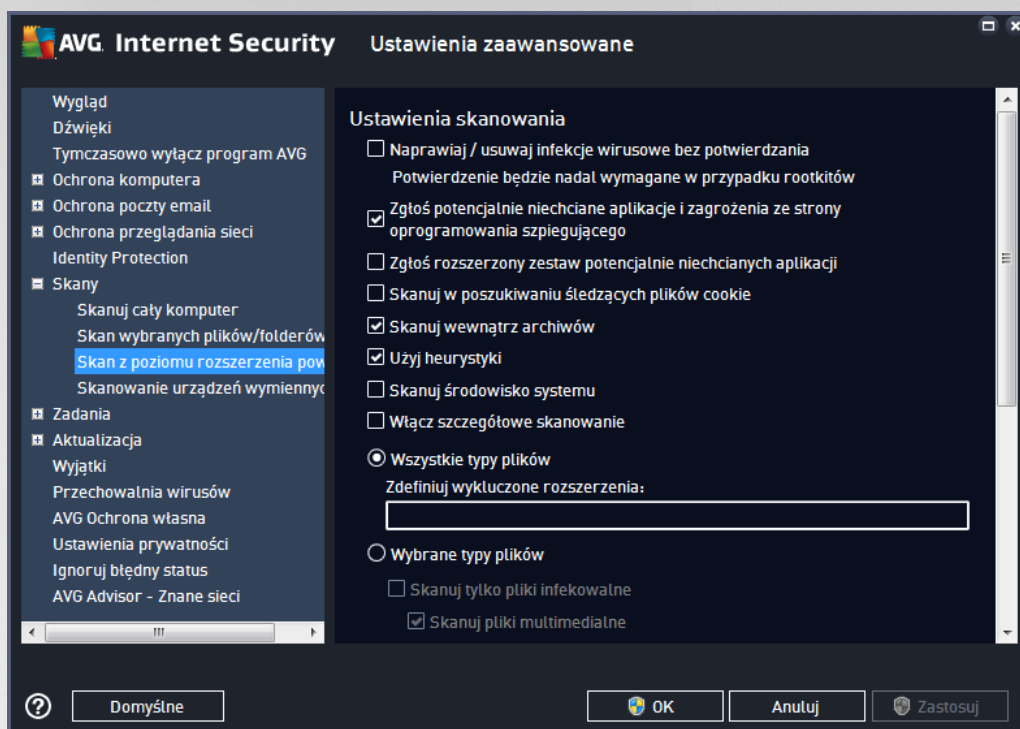


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych za pomocą opcji [Skanuj wybrane pliki lub foldery](#).

Uwaga: Opis poszczególnych parametrów zawiera rozdział [Ustawienia zaawansowane AVG / Skany / Skan całego komputera](#).

7.8.3. Skan z poziomu rozszerzenia powłoki

Analogicznie do elementu [Skan całego komputera](#), **Skan rozszerzenia powłoki** także oferuje szereg opcji umożliwiających edycję parametrów domyślnych. W tym przypadku konfiguracja odnosi się do [skanowania określonych obiektów bezpośrednio z interfejsu Eksploratora Windows \(rozszerzenie powłoki\)](#); zobacz rozdział [Skanowanie z poziomu Eksploratora Windows](#):



Opcje edycji są niemal identyczne jak te, które są dostępne w przypadku opcji [Skan całego komputera](#). Jednak ustawienia domyślne obu skanów różnią się (*np. funkcja Skan całego komputera nie sprawdza archiwów, ale skanuje środowisko systemowe, podczas gdy Skan rozszerzenia powłoki — odwrotnie*).

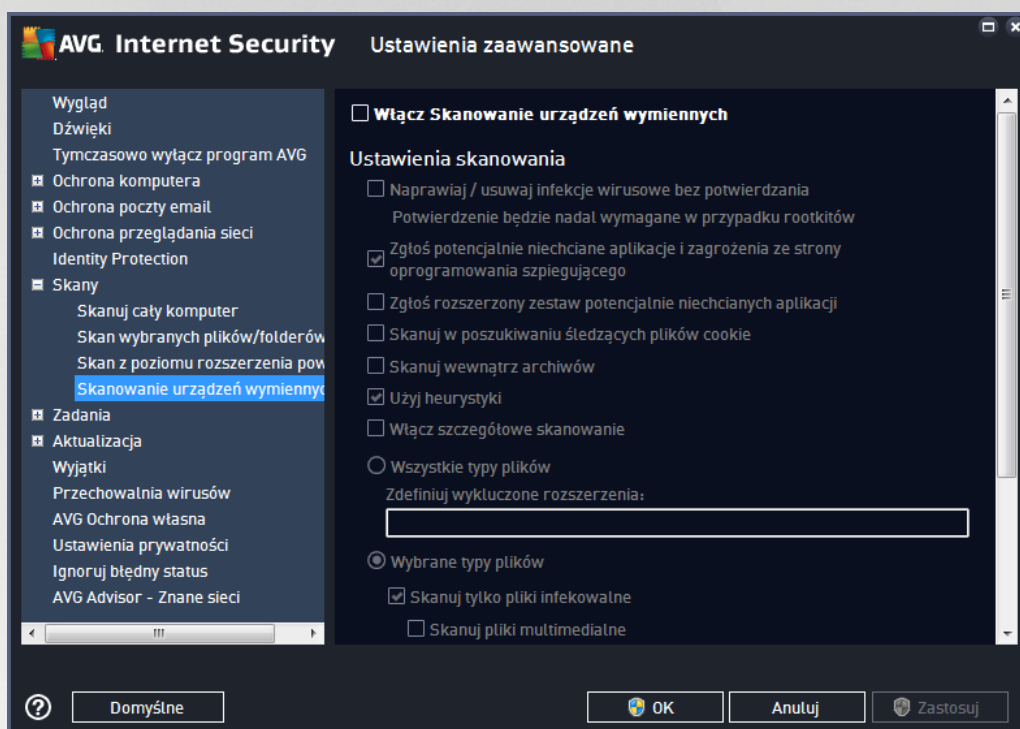
Uwaga: Opis poszczególnych parametrów zawiera rozdział [Ustawienia zaawansowane AVG / Skany / Skan całego komputera](#).

Podobnie jak w przypadku okna [Skan całego komputera](#), okno dialogowe **Skan rozszerzenia powłoki** również zawiera sekcję o nazwie **Wyświetlanie postępów i wyników skanowania**, w której można określić, czy informacje o postępach i wynikach skanowania mają być dostępne z poziomu interfejsu użytkownika systemu AVG. Możliwa jest również taka konfiguracja, przy której wyniki skanowania będą prezentowane tylko w razie wykrycia infekcji.



7.8.4. Skanowanie urządzeń wymiennych

Okno konfiguracji **Skanu urządzeń wymiennych** jest również bardzo podobne do okna dialogowego [Skan całego komputera](#):



Skan urządzeń wymiennych jest uruchamiany automatycznie po podłączeniu do komputera dowolnego urządzenia wymiennego. Domyślnie jest on wyłączony. Skanowanie urządzeń wymiennych w poszukiwaniu potencjalnych zagrożeń jest jednak bardzo ważne, ponieważ służy ono czystym źródłem infekcji. Jeśli skanowanie ma być uruchamiane automatycznie, należy zaznaczyć opcję **Włącz skanowanie urządzeń wymiennych**.

Uwaga: Opis poszczególnych parametrów zawiera rozdział [Ustawienia zaawansowane AVG / Skany / Skan całego komputera](#).

7.9. Zaplanowane zadania

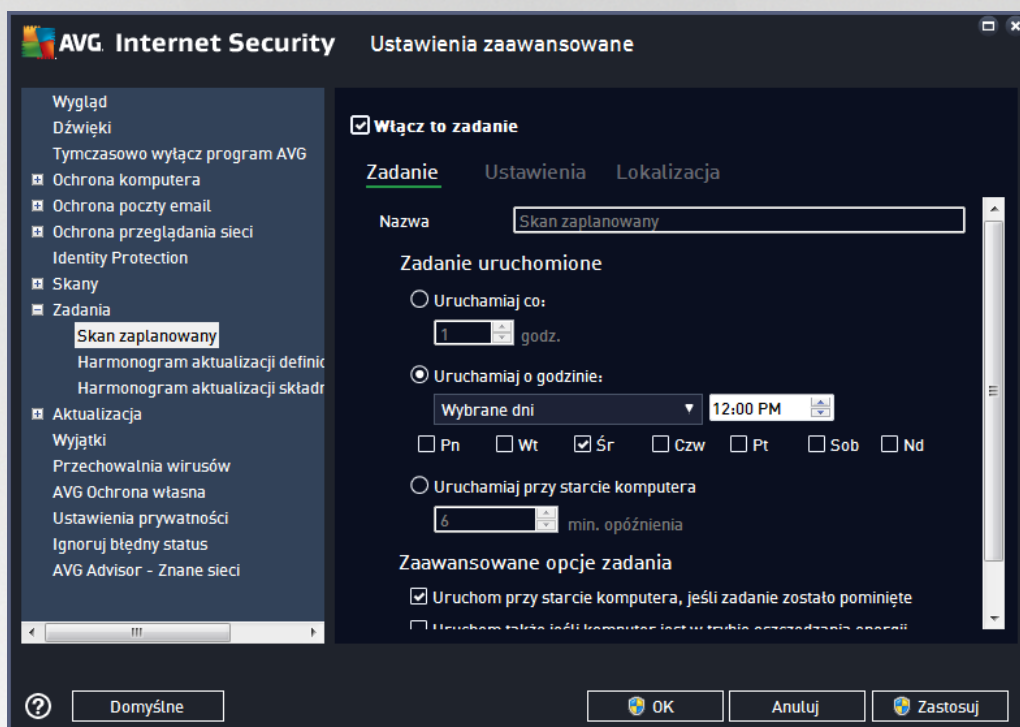
W oknie **Zadania** można edytować domyślne ustawienia następujących pozycji:

- [Skan zaplanowany](#)
- [Harmonogram aktualizacji definicji](#)
- Harmonogram aktualizacji programu
- [Harmonogram aktualizacji składnika Anti-Spam](#)



7.9.1. Skan zaplanowany

Parametry zaplanowanego skanu można edytować (podobnie jak przy tworzeniu nowego harmonogramu) na trzech kartach. Na każdej karcie można zaznaczyć / odznaczyć pole **Włącz to zadanie**, aby tymczasowo wyłączyć czy zaplanowany test lub włączyć go ponownie, gdy zajdzie taka potrzeba:



W polu tekstowym Nazwa (nieaktywne w przypadku harmonogramów domyślnych) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta oprogramowania. 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 skrótów, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości.

Przykład: Nazwy typu „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”. Nie ma potrzeby określenia w nazwie skanowania, czy skanowany jest cały komputer, czy tylko jego wybrane obszary — własne skany użytkownika są zawsze specyficznym [skanowaniem określonych plików lub folderów](#).

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

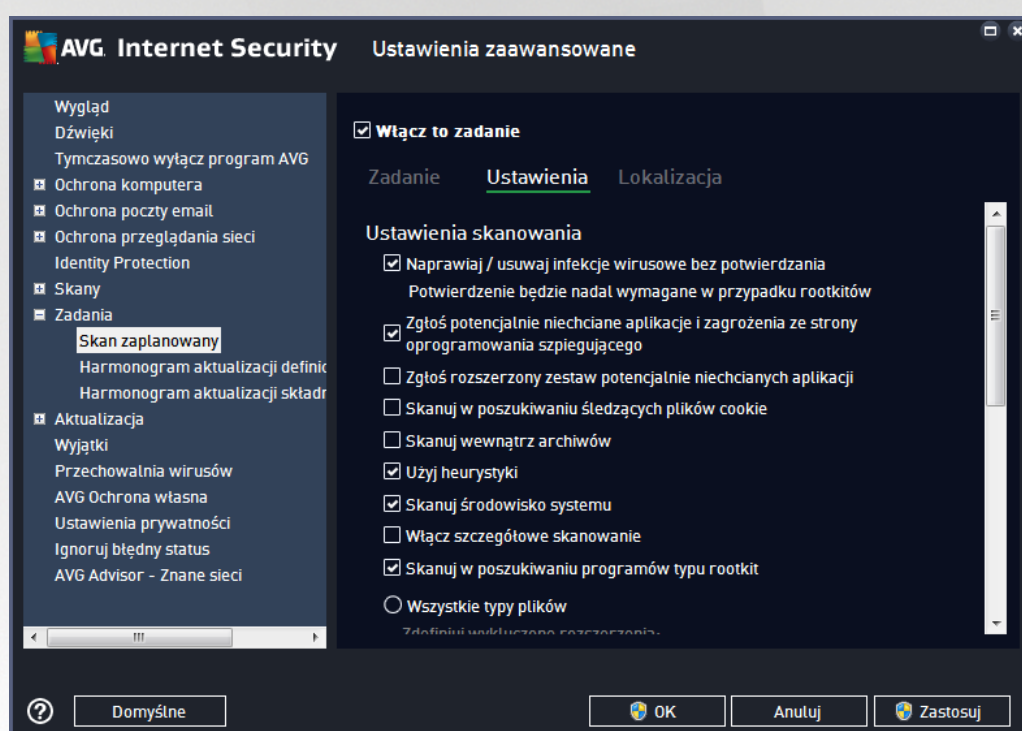
Zadanie uruchomione

W tym miejscu można określić, jak często ma być uruchamiane nowe skanowanie. Uruchamianie skanowania może być powtarzane w określonych odstępach czasu (**Uruchamiaj co**) lub danego dnia i o danej godzinie (**Uruchamiaj o określonych godzinach**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**Uruchamiaj przy starcie komputera**).



Zaawansowane opcje harmonogramu

- **Uruchom przy starcie komputera, je li zadanie zostało pominięte** — gdy komputer będzie wyłączony o zaplanowanej porze, AVG może przełożyć zaplanowane zadanie na najbliższy rozruch systemu.
- **Uruchom także je li komputer jest w trybie oszczędzania energii** — skanowanie zostanie przeprowadzone o zaplanowanej godzinie nawet wtedy, gdy komputer jest zasilany z baterii.



Karta **Ustawienia** zawiera listę parametrów skanowania, które można włączyć/wyłączyć. Domyślnie włączona jest funkcja, a odpowiadające im ustawienia stosowane podczas skanowania. **Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachować predefiniowaną konfigurację:**

- **Naprawiaj / usuwaj infekcje wirusowe bez potwierdzania** (domyślnie włączona): Je li podczas skanowania zostanie wykryty wirus, system AVG podejmie próbę automatycznego wyleczenia go. Je li zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).
- **Zgłoś potencjalnie niechciane aplikacje i zagrożenia ze strony oprogramowania szpiegującego** (domyślnie włączona): zaznaczenie tego pola aktywuje skanowanie 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 zwiksza ona poziom ochrony komputera.
- **Zgłoś rozszerzony zestaw potencjalnie niechcianych aplikacji** (domyślnie wyłączona):



zaznaczenie tej opcji pozwala wykrywać wieszaki oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojemu komputerowi. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego tę opcję nie jest wyłączone.

- **Skanuj w poszukiwaniu niedozwolonych plików cookie** (domyślnie wyłączone): ten parametr określa, czy wykrywane mają być pliki cookie; (używane w protokole HTTP do uwierzytelniania, ledzenia i przechowywania określonych informacji o użytkownikach, np. ustawienia witryn i zawartości koszyków w sklepach internetowych).
- **Skanuj wewnętrzne archiwów** (domyślnie wyłączone): ten parametr określa, czy skanowanie ma obejmować wszystkie pliki, nawet te znajdujące się w wewnętrznych archiwach, np. ZIP, RAR itd.
- **Użyj heurystyki** (domyślnie wyłączone): analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej) jest jedną z metod wykrywania wirusów w czasie skanowania.
- **Skanuj środowisko systemu** (domyślnie wyłączone): skanowanie obejmie także obszary systemowe komputera.
- **Wyłącz szczegółowe skanowanie** (domyślnie wyłączone): w określonych sytuacjach (gdy zachodzi podejrzenie, że komputer jest zainfekowany) można na zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będzie one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.
- **Skanuj w poszukiwaniu programów typu rootkit** (domyślnie wyłączone): skan Anti-Rootkit sprawdza komputer pod kątem rootkitów, czyli programów i technik pozwalających ukryć działanie szkodliwego oprogramowania. Wykrycie programu typu rootkit nie jest równoznaczne z tym, że komputer jest zainfekowany. W niektórych przypadkach pewne sterowniki lub elementy zwykłych aplikacji mogą omyłkowo zostać zaklasyfikowane jako programy typu rootkit.

Możesz także zdecydować, czy chcesz wykonać skanowanie

- **Wszystkie typy plików** z opcji zdefiniowania wyjść skanera przez wprowadzenie rozdzielonych przecinkami rozszerzeń plików (po zapisaniu przecinki zostają zamienione na redniki), które mają być pomijane.
- **Wybrane typy plików** — skanowane będą tylko pliki, które mogą zostać zainfekowane (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 — jeżeli to pole zostanie niezaznaczone, czas skanowania 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 wybrać pozycję **Skanowanie plików bez rozszerzenia** — ta opcja jest domyślnie wyłączone i zaleca się, aby nie zmieniać tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane łącznie z innymi.

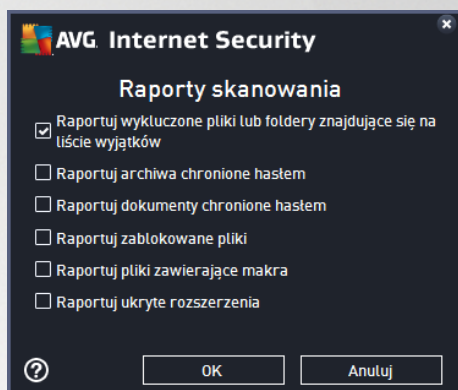


Określ, jak długo ma trwać skanowanie

W tej sekcji można szczegółowo określić parametry skanowania w zależności od wykorzystania zasobów systemowych. Domyślną wartością jest poziom *Zależny od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Jeżeli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowodować działanie innych procesów i aplikacji (*tej opcji można używać wtedy, gdy komputer jest wyłączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przyspieszy jednocześnie czas skanowania.

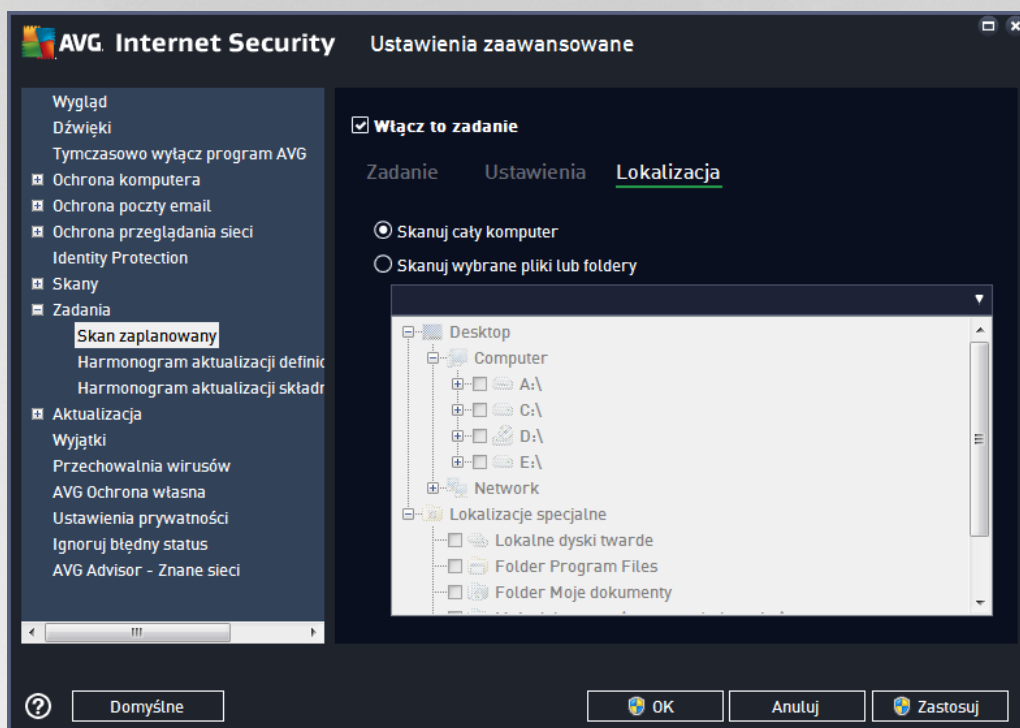
Ustaw dodatkowe raporty skanowania

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



Opcje zamykania komputera

W sekcji **Opcje zamykania komputera** można zdecydować, czy komputer ma zostać automatycznie wyłączony po zakończeniu bieżącego procesu skanowania. Wybranie opcji (**Zamknij komputer po ukończeniu skanowania**) spowoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet wtedy, gdy w danej chwili jest on zablokowany (**Wymuś zamknięcie, jeśli komputer jest zablokowany**).

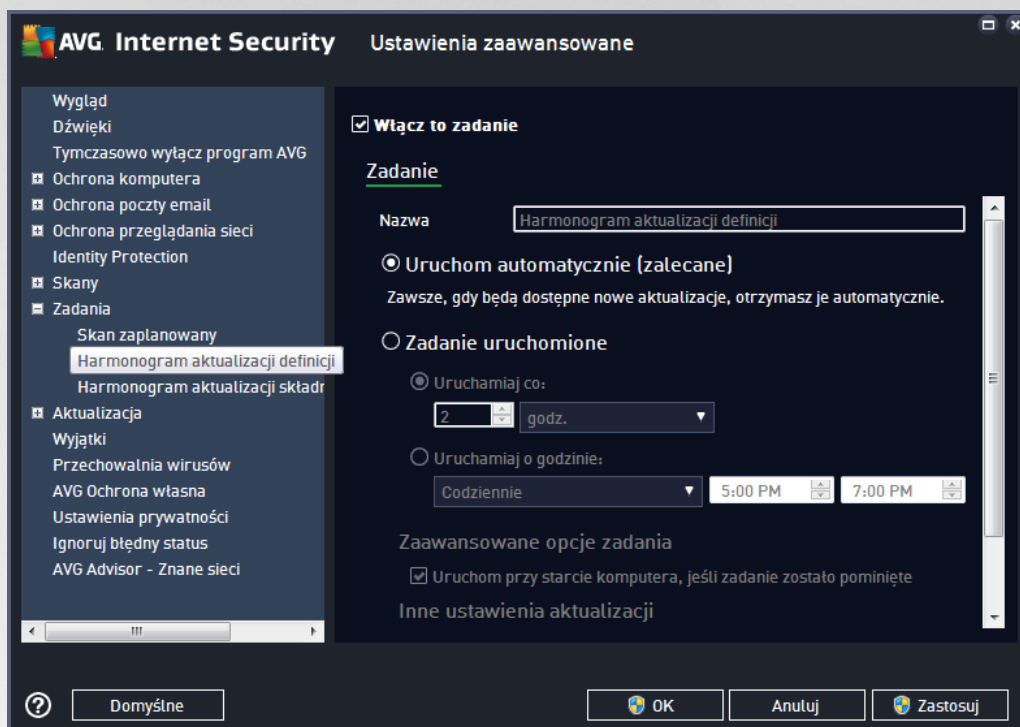


Na karcie **Lokalizacja** można określić, czy planowane jest [skanowanie całego komputera](#), czy [skanowanie określonych plików lub folderów](#). W przypadku skanowania określonych plików lub folderów, w dolnej części okna dialogowego aktywowane jest drzewo katalogów, w którym można wybrać obiekty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



7.9.2. Harmonogram aktualizacji definicji

Jeśli **jest to naprawdę konieczne**, tymczasowo można dezaktywować zaplanowaną aktualizację programu, odznaczając pole **Włącz to zadanie** i zaznaczając je ponownie później:



W tym oknie dialogowym można ustawić szczegółowe parametry harmonogramu aktualizacji definicji. W polu tekstowym **Nazwa** (*nieaktywne dla harmonogramów domyślnych*) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta oprogramowania.

Zadanie uruchomione

Domyślnie zadanie jest uruchamiane automatycznie (**Uruchom automatycznie**), gdy tylko zostanie udostępniona nowa aktualizacja definicji wirusów. Zalecamy pozostanie przy tej konfiguracji, chyba że masz jakiś powód, aby zrobić inaczej! Następnie można skonfigurować ręczne uruchomienie zadania i określić odstępy czasowe uruchomienia nowo zaplanowanych aktualizacji definicji. Aktualizacja definicji może być powtarzana w określonych odstępach czasu (**Uruchamiaj co**) lub danego dnia i o danej godzinie (**Uruchamiaj o określonych godzinach**).

Zaawansowane opcje harmonogramu

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

Inne ustawienia aktualizacji

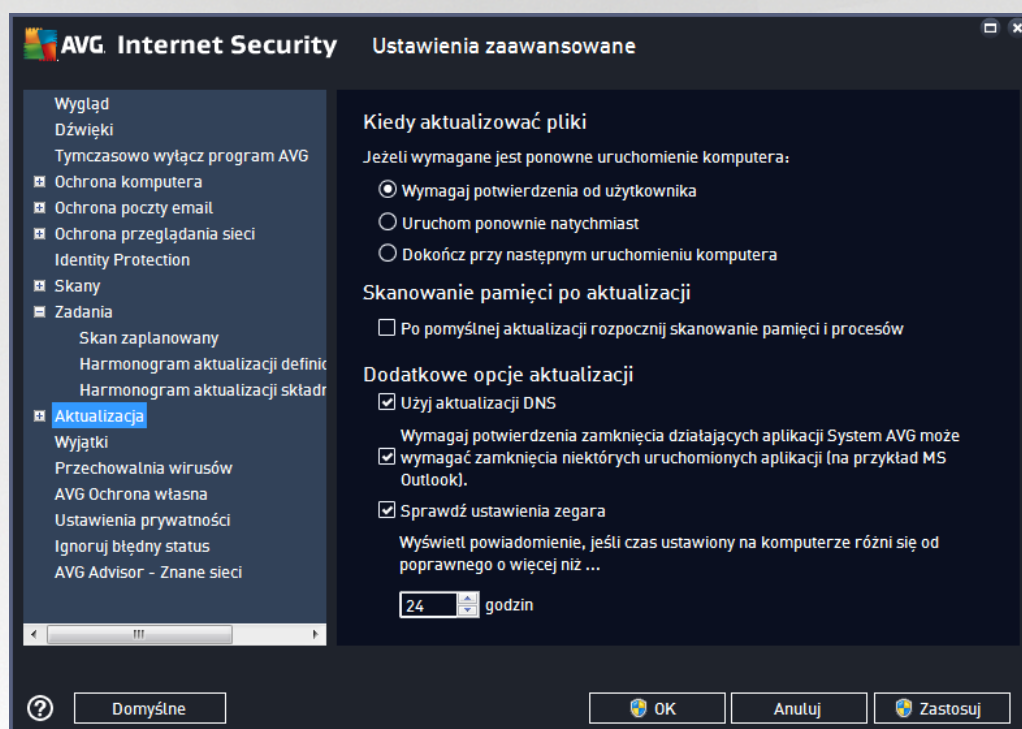
Na koniec zaznacz pole wyboru **Uruchom aktualizację natychmiast po nawiązaniu połączenia**



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 AVG na pasku systemowym** wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji [Ustawienia zaawansowane/Wygląd](#)*).

7.9.3. Harmonogram aktualizacji składnika Anti-Spam

Jeżeli zajdzie taka potrzeba, możesz skorzystać z pola **Wyłącz to zadanie**, aby tymczasowo wyłączyć zaplanowaną aktualizację składnika [Anti-Spam](#), a później ponownie ją włączyć:



W tym oknie dialogowym można ustawić szczegółowe parametry harmonogramu aktualizacji. W polu tekstowym **Nazwa** (*nieaktywne dla harmonogramów domyślnych*) jest wyświetlana nazwa przypisana do tego harmonogramu przez producenta oprogramowania.

Zadanie uruchomione

W tym miejscu należy określić interwały czasowe uruchamiania nowo zaplanowanych aktualizacji składnika Anti-Spam. Aktualizacja składnika Anti-Spam może być powtarzana w określonych odstępach czasu (**Uruchamiaj co**) lub o zadanej godzinie (**Uruchamiaj o określonych godzinach**), a także na skutek wystąpienia zdefiniowanego zdarzenia (**Uruchamiaj przy starcie komputera**).

Zaawansowane opcje harmonogramu

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

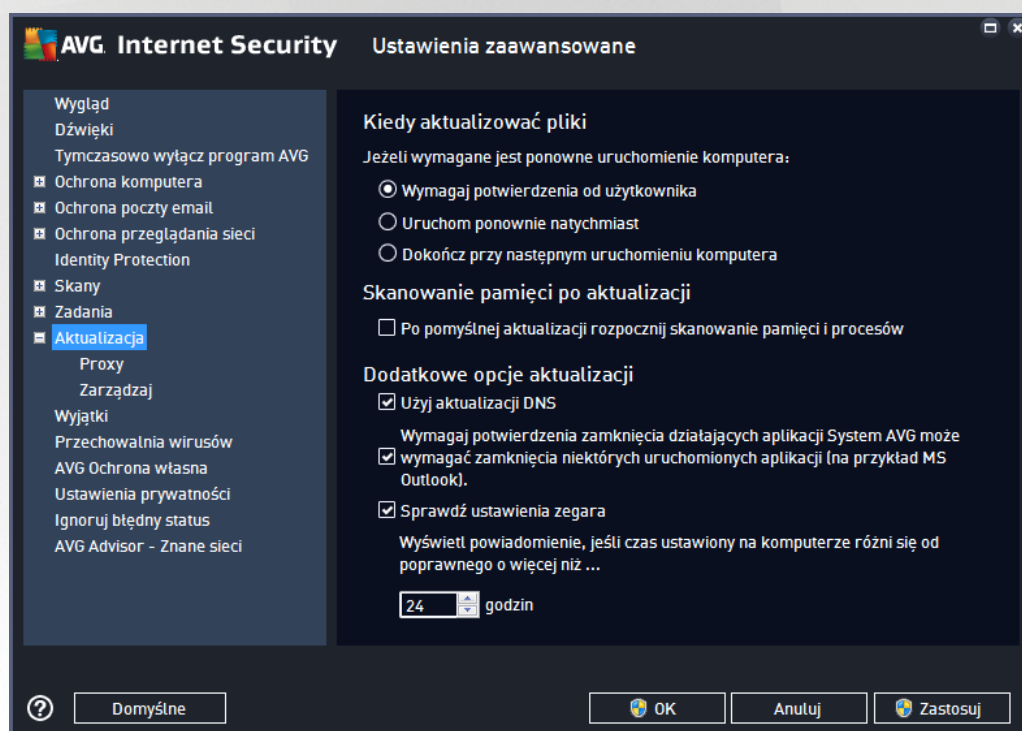


Inne ustawienia aktualizacji

Zaznacz pole wyboru **Uruchom aktualizacji natychmiast po nawiązaniu połączenia z internetem**, aby upewnić się, że aktualizacja zostanie wznowiona po ponownym połączeniu z siecią, jeżeli połączenie internetowe zostanie przerwane, a proces aktualizacji składnika Anti-Spam nie powiodzie się. Po rozpoczęciu zaplanowanego skanowania nad [ikoną AVG na pasku zadań](#) zostanie wyświetlone odpowiednie powiadomienie (jeżeli w sekcji [Ustawienia zaawansowane/Wygląd](#) zastosowano domyślną konfigurację).

7.10. Aktualizacja

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



Kiedy aktualizować pliki

W tej sekcji dostępne są trzy opcje, których można użyć, gdy proces aktualizacji będzie wymagał ponownego uruchomienia komputera. Dokończenie aktualizacji wymaga restartu komputera, który można od razu wykonać:

- **Wymagaj potwierdzenia od użytkownika** (opcja domyślna) — przed zakończeniem aktualizacji system zapyta użytkownika o pozwolenie na ponowne uruchomienie komputera.
- **Uruchom ponownie natychmiast** — komputer zostanie automatycznie zrestartowany zaraz po zakończeniu aktualizacji; potwierdzenie ze strony użytkownika nie będzie wymagane.
- **Dokończ przy następnym uruchomieniu komputera** — aktualizacja zostanie automatycznie



odło ona i ukończona przy najbliższym restarcie komputera. Należy pamiętać, że ta opcja należy zaznaczyć wyłącznie, jeżeli komputer jest regularnie uruchamiany ponownie (co najmniej raz dziennie)!

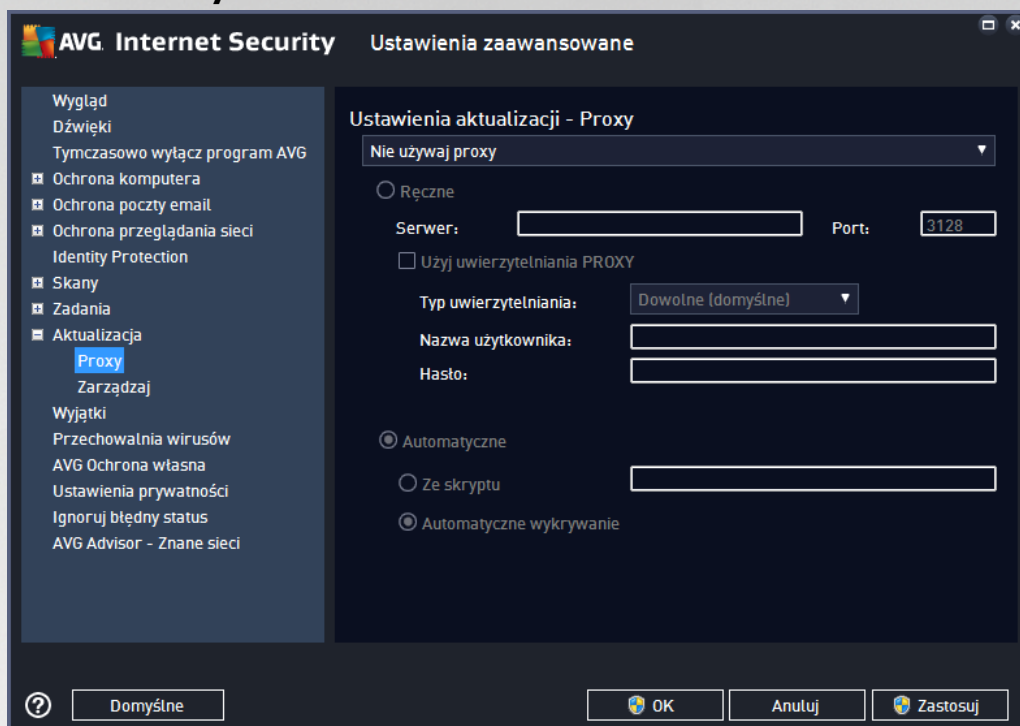
Skanowanie pamięci po aktualizacji

Pole to należy zaznaczyć, jeżeli po każdej nowej aktualizacji systemu 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 podczas każdej aktualizacji programu** (domyślnie włączone) przed każdą aktualizacją programu AVG tworzony będzie punkt przywracania systemu. W przypadku niepowodzenia aktualizacji i awarii systemu operacyjnego można odtworzyć pierwotną konfigurację systemu, używając tego punktu. Aby przywrócić system, należy wybrać kolejno opcje: Start / Wszystkie programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoświadczonym użytkownikom! Aby można było korzystać z tej funkcji, pole wyboru musi pozostać zaznaczone.
- **Użyj aktualizacji DNS** (opcja domyślnie włączona) — gdy to pole jest zaznaczone, przy uruchamianiu aktualizacji oprogramowanie **AVG Internet Security** wyszukuje informacje o najnowszej wersji bazy wirusów i programu na serwerze DNS. Następnie pobierane i instalowane są jedynie niewielkie niezbędne pliki aktualizacyjne. Dzięki temu łączna ilość pobieranych danych jest minimalizowana, a proces aktualizacji przebiega szybciej.
- **Wymagaj potwierdzenia zamknięcia działających aplikacji** (domyślnie włączone) — daje pewność, że aktywne działające aplikacje nie zostaną zamknięte bez potwierdzenia ze strony użytkownika, jeżeli do zakończenia aktualizacji będzie wymagane ponowne uruchomienie komputera.
- **Sprawdź ustawienia zegara** (domyślnie włączone) — zaznacz to pole, jeżeli chcesz, aby program wysłał powiadomienie, gdy różnica między lokalnym czasem komputera przekroczy określony liczbę godzin.

7.10.1. Proxy



Serwer proxy jest samodzielnym serwerem lub uruchomion na komputerze usług gwarantując bezpieczniejsze połączenie internetowe. Zgodnie z określonymi zasadami sieciowymi połączenie internetowe może być bezpośrednie lub przez serwer proxy. Można tak też zezwolić na korzystanie z obu opcji jednocześnie. Dlatego też w oknie **Ustawienia aktualizacji – Proxy** należy najpierw wybrać jedną z dostępnych opcji:

- **Nie używaj proxy** — ustawienia domyślne
- **Użyj proxy**
- **Spróbuj połączenia bezpośrednio, a w razie niepowodzenia połączenia 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 **Ręcznie aktywuje odpowiednią sekcję**) należy podać następujące informacje:

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



Na serwerze proxy mogą być skonfigurowane specjalne reguły dla każdego użytkownika. Jeśli serwer proxy jest skonfigurowany w ten sposób, należy zaznaczyć opcję **Użyj uwierzytelniania PROXY**, aby serwer weryfikował nazwę użytkownika i hasło przed nawizaniem połączenia.

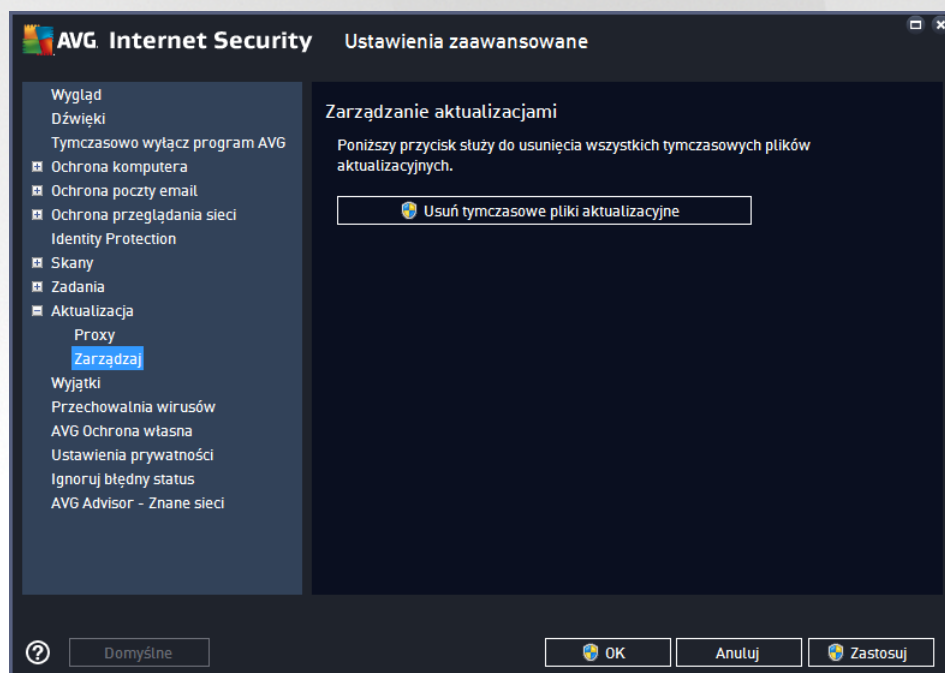
Konfiguracja automatyczna

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 funkcję zwracającą adres serwera proxy
- **Automatyczne wykrywanie** — konfiguracja zostanie wykryta automatycznie bezpośrednio na serwerze proxy

7.10.2. Zarządzaj

Okno **Zarządzaj aktualizacjami** oferuje dwie funkcje uruchamiane przyciskami:



- **Usuń tymczasowe pliki aktualizacyjne** — pozwala usunąć z dysku twardego wszystkie zbędne pliki aktualizacyjne (są one domyślnie przechowywane przez 30 dni)
- **Cofnij bazy wirusów do poprzedniej wersji** — pozwala usunąć z dysku twardego ostatnią wersję bazy wirusów i przywrócić ją do poprzedniego stanu (nowa baza będzie czyszczyć najbliższe aktualizacji)



7.11. Wyjątki

W oknie **Wyjątki** można zdefiniować wyjątki, czyli obiekty, które oprogramowanie **AVG Internet Security** ma ignorować. Zazwyczaj trzeba zdefiniować wyjątek, gdy system AVG w jakiś sposób wykrywa program lub plik jako zagrożenie lub blokuje bezpieczną stronę, uważając ją za zagrożenie. Dodaj taki plik lub stronę do listy wyjątków, aby system AVG już ich nie zgłaszał ani nie blokował.

Prosimy upewnić się, że plik, program lub strona jest absolutnie bezpieczna!

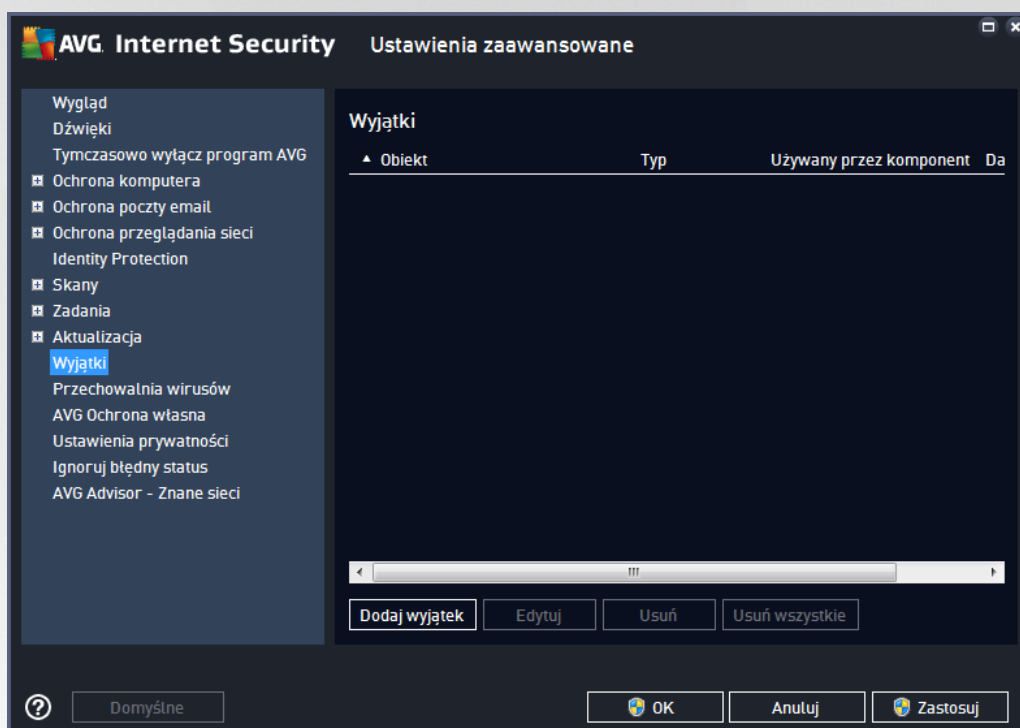
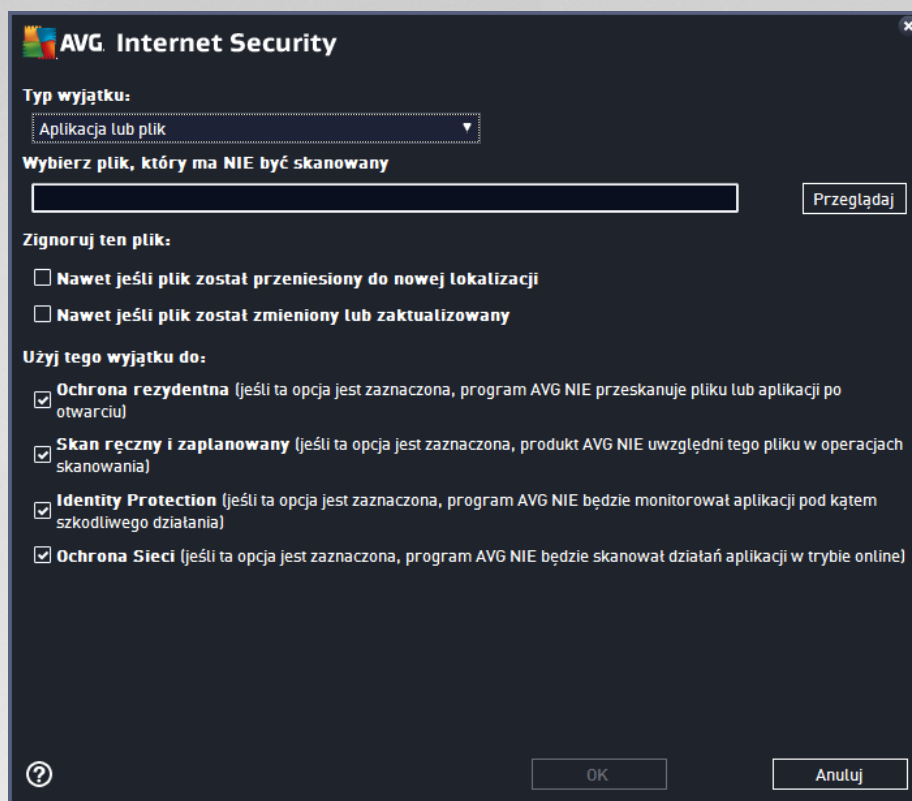


Tabela w tym oknie zawiera listę wyjątków, o ile zostały one już zdefiniowane. Obok każdej pozycji znajduje się pole wyboru. Jeśli pole wyboru jest zaznaczone, obiekt pozostanie wykluczony ze skanowania. Jeśli nie, to znaczy, że wyjątek jest zdefiniowany, ale w danej chwili nie jest aktywny. Klikając nagłówek kolumny, można posortować dozwolone obiekty według odpowiednich kryteriów.

Przyciski kontrolne

- **Dodaj wyjątek** — kliknij ten przycisk, aby otworzyć nowe okno, które umożliwia zdefiniowanie nowego obiektu wykluczonego ze skanowania AVG.

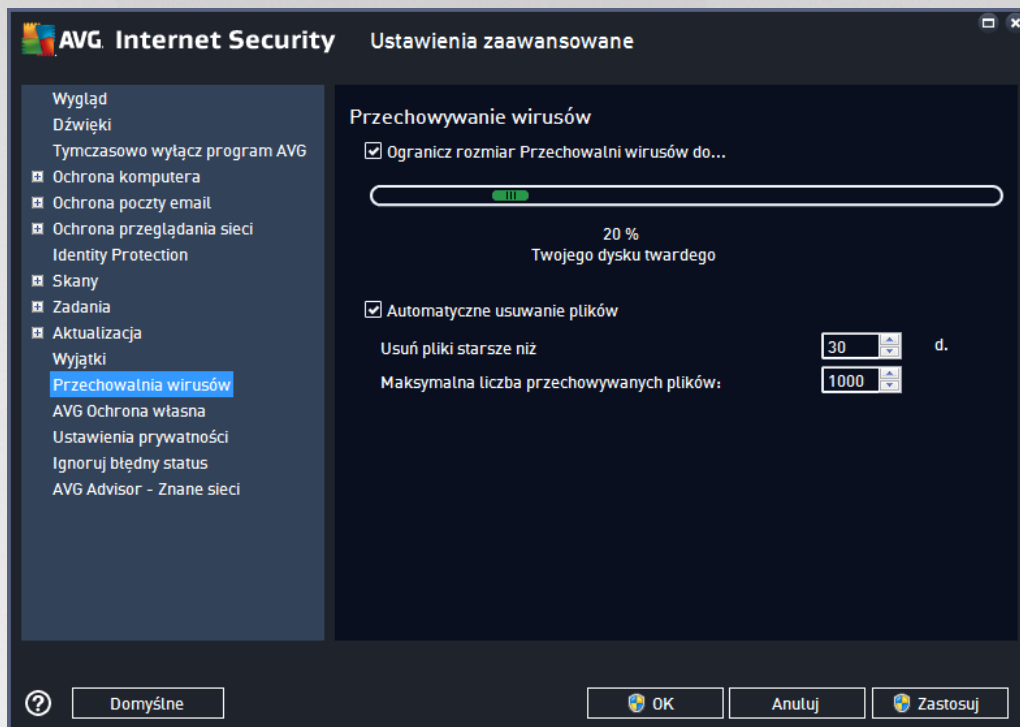


W pierwszej kolejności ci trzeba zdefiniować typ obiektu — czy jest on aplikacją, plikiem, folderem, adresem URL, czy certyfikatem. Następnie trzeba wskazać cię do obiektu na dysku lub wprowadzić adres URL. Na końcu możesz tak określić, które funkcje oprogramowania AVG powinny ignorować wskazany obiekt (*Ochrona rezydentna*, *Identity Protection*, *Skaner*).

- **Edytuj** — ten przycisk aktywny jest tylko wówczas, gdy już zostały zdefiniowane wyjątki i znajdują się one na liście. Uciśnięcie tego przycisku spowoduje otwarcie nowego okna umożliwiającego konfigurację parametrów wybranego wyjątku.
- **Usu** — uciśnięcie tego przycisku, aby anulować wcześniej zdefiniowany wyjątek. Możesz usunąć wyjątki pojedynczo lub zaznaczyć blok wyjątków na liście i anulować je wszystkie. Po anulowaniu zdefiniowanego wyjątku system AVG będzie znów sprawdzał dany plik, folder lub adres URL. Usunięty zostanie jedynie wyjątek, a nie sam plik czy folder.
- **Usu wszystko** — uciśnięcie tego przycisku, aby usunąć wszystkie wyjątki zdefiniowane na liście.



7.12. Przechowalnia wirusów

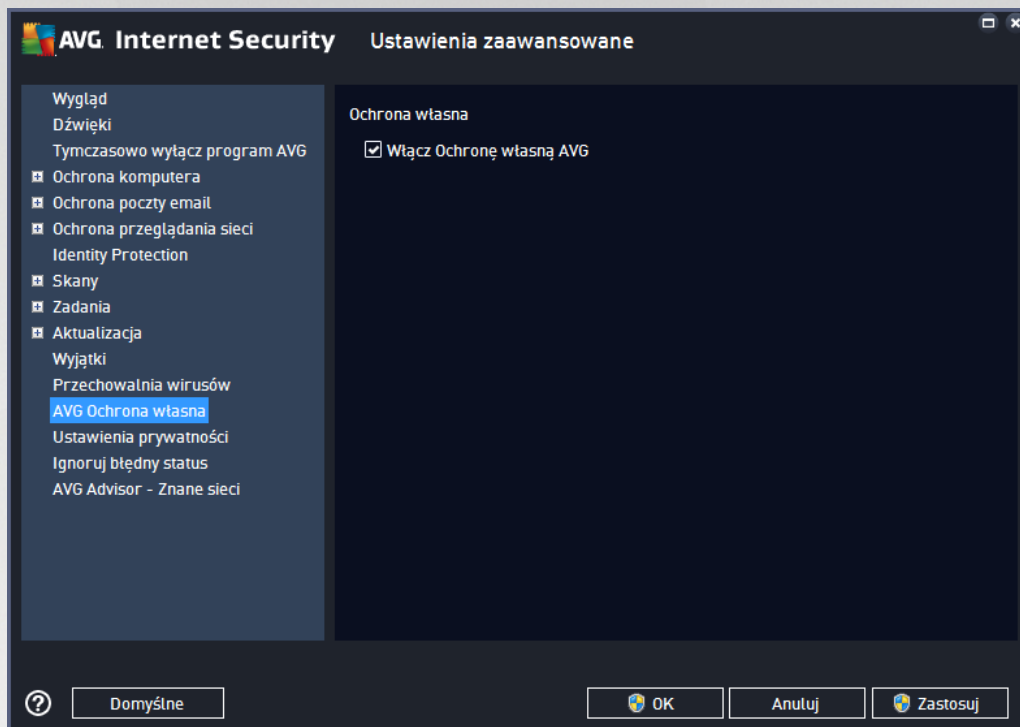


Okno dialogowe **Przechowalnia wirusów** pozwala zdefiniować kilka parametrów dotyczących administrowania obiektami znajdującymi się w [Przechowalni wirusów](#):

- **Ogranicz rozmiar Przechowalni wirusów** — za pomocą suwaka należy określić maksymalny rozmiar [Przechowalni wirusów](#). Rozmiar jest określany w stosunku do rozmiaru dysku lokalnego.
- **Automatyczne usuwanie plików** — w tym obszarze można zdefiniować maksymalny okres przetrzymywania obiektów w [Przechowalni wirusów](#) (**Usuń pliki starsze niż ... dni**) oraz maksymalną liczbę plików, które mogą znajdować się w [Przechowalni wirusów](#) (**Maksymalna liczba przechowywanych plików**).



7.13. Ochrona własna AVG

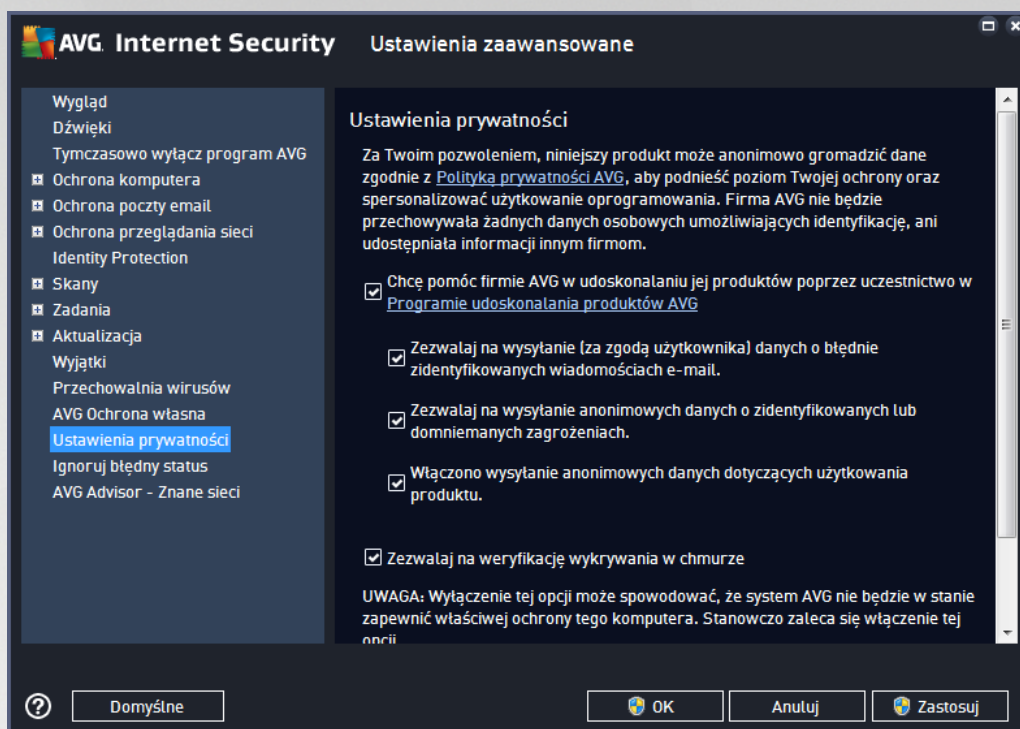


Funkcja **Ochrona własna AVG** pozwala programowi **AVG Internet Security** chronić własne procesy, pliki, klucze rejestru i sterowniki przed zmianami i dezaktywacją. Głównym powodem stosowania tej ochrony jest istnienie pewnych zaawansowanych zagrożeń, które próbują rozbroić oprogramowanie antywirusowe, a następnie wykonywać działania szkodliwe dla komputera.

Zalecamy zachowanie tej funkcji włączoną!

7.14. Ustawienia prywatności

Okno **Ustawienia prywatności** wyświetla zaproszenie do uczestnictwa w programie udoskonalania produktów AVG oraz pomagania nam w podnoszeniu ogólnego poziomu bezpieczeństwa w internecie. Twoje raporty pomogą nam w gromadzeniu aktualnych informacji o najnowszych wirusach. Wiedza ta jest konieczna, jeżeli mamy im przeciwdziałać. Raportowanie odbywa się automatycznie, więc nie powinno powodować niedogodności. W raportach nie są zawarte żadne dane osobowe. Zgłaszanie wykrytych zagrożeń jest opcjonalne — prosimy jednak o pozostawienie tej opcji włączoną. Pozwala ona na udoskonalenie ochrony zapewnianej Tobie i innym użytkownikom AVG.



W tym oknie dostępne są następujące opcje:

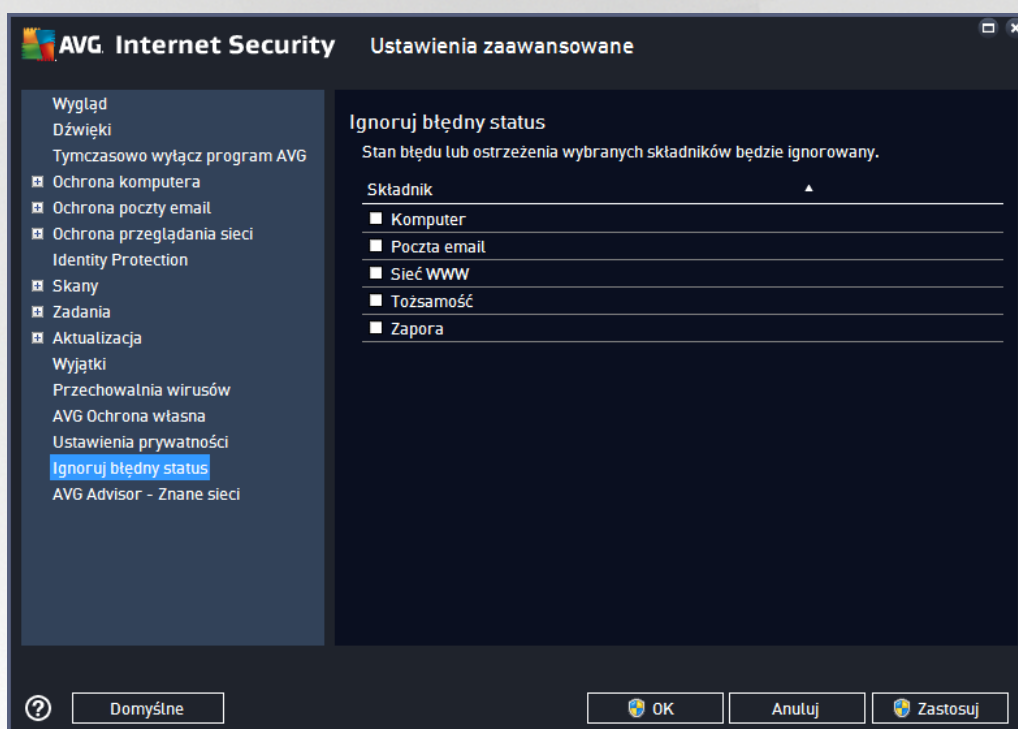
- **Chcę pomóc firmie AVG w udoskonalaniu jej produktów przez uczestnictwo w Programie udoskonalania produktów AVG (domyślnie włączone)** — jeśli chcesz pomóc nam udoskonalona produkt **AVG Internet Security**, pozostaw to pole zaznaczone. Umożliwi to zgłaszanie wszystkich napotkanych zagrożeń do firmy AVG, co pozwoli nam gromadzić aktualne informacje o najnowszych wirusach i szkodliwym oprogramowaniu od wszystkich użytkowników z całego świata, aby udoskonalona ochrona. Zgłaszanie witryn obsługiwane jest automatycznie, więc nie powoduje żadnych niedogodności. Raporty nie zawierają żadnych poufnych danych.
- **Zezwalaj na wysyłanie (za zgodą użytkownika) danych o błędnie zaklasyfikowanych wiadomościach e-mail (domyślnie włączone)** — funkcja ta umożliwia wysyłanie informacji o wiadomościach e-mail nieprawidłowo oznaczonych jako spam lub wiadomościach błędnie zaklasyfikowanych jako spam, które nie zostały poprawnie wykryte przez usługę Anti-Spam. Przed wysłaniem tego rodzaju informacji użytkownik będzie proszony o potwierdzenie.
- **Zezwalaj na wysyłanie anonimowych danych o zidentyfikowanych lub domniemyanych zagrożeniach (opcja domyślnie włączona)** — wysyłanie informacji o wszelkim podejrzanym lub niebezpiecznym kodzie lub zachowaniu (może to być wirus, oprogramowanie szpiegujące lub witryna internetowa zawierająca szkodliwe oprogramowanie, do której użytkownik próbuje uzyskać dostęp) wykrytym na komputerze.
- **Zezwalaj na wysyłanie anonimowych danych dotyczących użytkownika produktu (opcja domyślnie włączona)** — wysyłanie podstawowych statystyk dotyczących korzystania z aplikacji, takich jak liczba wykrytych zagrożeń, uruchomionych skanów, pominiętych lub nieudanych aktualizacji itd.
- **Zezwalaj na weryfikację detekcji w chmurze (opcja domyślnie włączona)** — wykryte zagrożenia będą sprawdzane pod kątem infekcji w celu uniknięcia błędnych wykryć.



- **Chcę, aby firma AVG spersonalizowała mój sposób korzystania z oprogramowania, włącz funkcję Personalizacja AVG (funkcja domyślnie wyłączona)** — funkcja ta anonimowo analizuje zachowanie programów i aplikacji zainstalowanych na komputerze. Na podstawie tej analizy firma AVG może zaoferować usługi precyzyjnie dostosowane do Twoich potrzeb, aby zapewnić maksymalne bezpieczeństwo.

7.15. Ignoruj błędny stan

W oknie dialogowym **Ignoruj wadliwe warunki** można wskazać składniki, które mają być pomijane w powiadomieniach o stanie systemu AVG:



Domyślnie żaden składnik nie jest zaznaczony. Oznacza to, że jeśli dowolny składnik znajdzie się w stanie błędny, natychmiast wygenerowane zostanie powiadomienie:

- [ikona w zasobniku systemowym](#) — gdy wszystkie składniki systemu AVG działają prawidłowo, wyświetlana ikona jest czterokolorowa; w przypadku błędny wyświetlany jest żółty wykrzyknik,
- tekstowy opis problemu jest widoczny w sekcji [Informacje o stanie bezpieczeństwa](#) w oknie głównym AVG

Istnieją jednak sytuacje, w których z jakiegoś powodu trzeba tymczasowo wyłączyć wybrany składnik. **Nie jest to zalecane — wszystkie składniki powinny być stale włączone i pracować z domyślną konfiguracją**, ale taka sytuacja może się zdarzyć. W takim przypadku ikona w zasobniku systemowym automatycznie informuje o stanie błędny składnika. Nie występuje tu jednak faktyczny błąd, ponieważ wyłączenie składnika było celowe, a ryzyko z tym związane jest znane. Ponadto, gdy ikona jest szara, nie można jej informować o ewentualnych realnych błędach.

W takim przypadku należy w oknie dialogowym **Ignoruj błędny status** zaznaczyć składniki, które mogą być w stanie błędny (*lub wyłączone*) bez wyświetlania odpowiednich powiadomień. Kliknij przycisk **OK**, aby

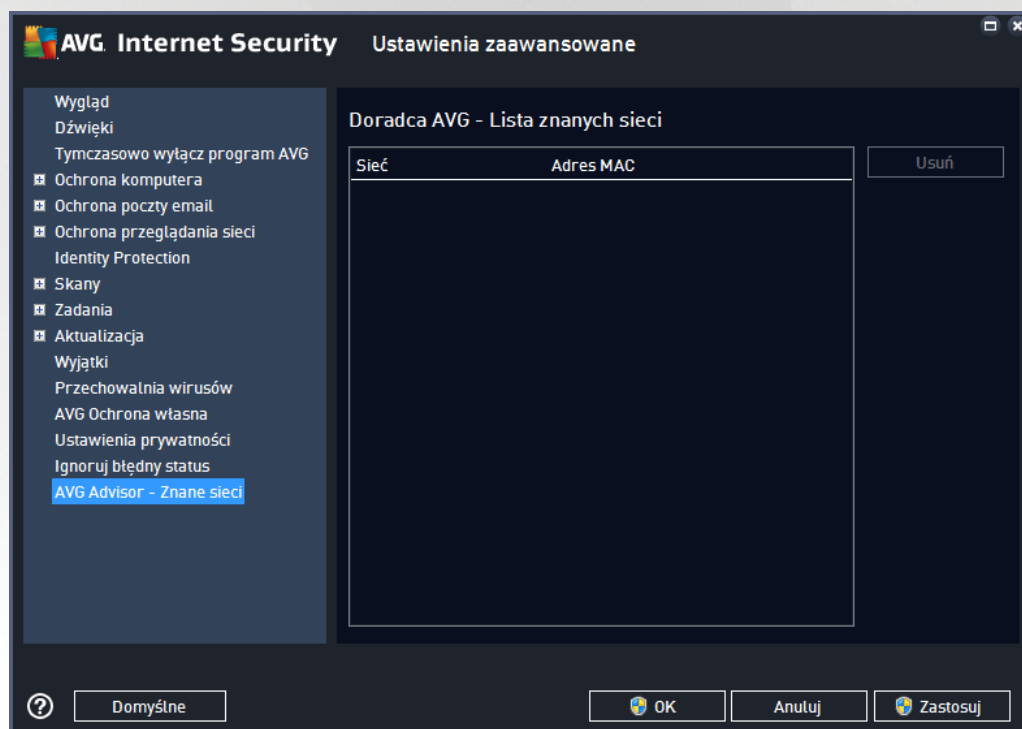


potwierdzi .

7.16. Doradca AVG – znane sieci

[Doradca AVG](#) zawiera funkcję monitorowania sieci bezprzewodowych, z którymi się łączysz, aby w razie wykrycia nowej sieci (o znajomej nazwie, która mogłaby wprowadzić Cię w błąd) powiadomi Cię o tym i doradzi Ci upewnienie się co do jej bezpieczeństwa. Jeśli zdecydujesz się połączyć z nową siecią, jest bezpieczna, możesz zapisać jej nazwę (za pomocą linku widocznego w powiadomieniu Doradcy AVG, które pojawia się nad zasobnikiem systemowym po wykryciu nowej sieci). Szczegóły można znaleźć w rozdziale [Doradca AVG](#). [Doradca AVG](#) zapamięta wówczas unikalne atrybuty danej sieci (a dokładniej jej adres MAC) i nie będzie ponownie wyświetlał tego powiadomienia. Każda sieć, z którą nawiążesz połączenie, będzie automatycznie uznawana za znaną i dodawana do listy. Możesz usunąć pojedynczą sieć klikając przycisk **Usuń** – zostanie ona znów uznana za potencjalnie niebezpieczną.

W tym oknie dialogowym możesz sprawdzić, które sieci są uznawane za znane:



Uwaga: Funkcja rozpoznawania znanych sieci przez Doradcę AVG nie jest obsługiwana w 64-bitowym systemie Windows XP.



8. Ustawienia Zapory

Konfiguracja [Zapory](#) otwierana jest w nowym oknie, gdzie w kilku sekcjach można określić nawet najbardziej zaawansowane parametry tego składnika. Konfiguracja Zapory otwierana jest w nowym oknie, które umożliwia edycję zaawansowanych parametrów tego składnika dzięki kilku stronom konfiguracyjnym. Konfiguracja może być wyświetlana w trybie podstawowym lub trybie eksperta. Gdy po raz pierwszy przejdziesz do okna konfiguracji, zostanie ono otwarte w trybie podstawowym, które umożliwia edycję następujących parametrów:

- [Ogólne](#)
- [Aplikacje](#)
- [Udostępnianie plików i drukarek](#)

W dolnej części okna znajduje się przycisk **Tryb eksperta**. Kliknij ten przycisk, by wyświetlić kolejne pozycje, które udostępnią bardzo zaawansowaną konfigurację Zapory:

- [Ustawienia zaawansowane](#)
- [Zdefiniowane sieci](#)
- [Usługi systemowe](#)
- [Dzienniki](#)

8.1. Ogólne

Okno **Informacje ogólne** wyświetla przegląd wszystkich dostępnych trybów Zapory. Bieżący tryb Zapory może być zmieniony poprzez prosty wybór innego trybu z menu.

Dostawca oprogramowania skonfigurował jednak wszystkie składniki systemu AVG Internet Security pod kątem optymalnej wydajności. Nie należy modyfikować konfiguracji domyślnej, je li nie ma ku temu ważnych powodów. Wszelkie zmiany powinny być wprowadzane wyłącznie przez dozwolonych użytkowników.



Zapora umożliwia definiowanie określonych reguł bezpieczeństwa na podstawie środowiska i trybu pracy komputera. Każda opcja wymaga innego poziomu zabezpieczenia, a dostosowywanie poziomów odbywa się za pomocą odpowiednich trybów. Krótko mówiąc, tryb Zapory to określona konfiguracja tego składnika. Dostępna jest pewna liczba wcześniej zdefiniowanych konfiguracji:

- **Automatyczny** — w tym trybie Zapora obsługuje cały ruch sieciowy automatycznie. Nie musisz podejmować żadnych decyzji. Zapora zezwoli na połączenia wszystkich znanych aplikacji, tworząc jednocześnie reguły umożliwiające im nadal używanie połączeń w przyszłości. W przypadku innych aplikacji Zapora zdecyduje, czy je pozwoli na komunikację, czy je zablokuje, na podstawie analizy działania aplikacji. W takich sytuacjach nie utworzy ona jednak reguły, więc aplikacja będzie sprawdzana przy każdej kolejnej próbie połączenia. **Tryb automatyczny działa dyskretnie i jest polecany wszystkim użytkownikom.**
- **Interaktywny** — tryb ten może być przydatny, jeśli chcesz w pełni kontrolować ruch przychodzący i wychodzący z Twojego komputera. Zapora będzie monitorowała ruch i przy każdej próbie połączenia lub transferu danych pozwoli Ci zdecydować, czy chcesz na to zezwolić. Ten tryb jest zalecany tylko w przypadku użytkowników zaawansowanych.
- **Blokuj dostęp do internetu** — połączenia z internetem będzie całkowicie zablokowane, uniemożliwiając Ci dostęp do internetu, a także do zewnętrznego świata — do Twojego komputera. Ten tryb jest przeznaczony tylko do stosowania tymczasowo i w szczególnych sytuacjach.
- **Wyłącz Zaporę** — wyłączenie Zapory zezwoli na cały ruch przychodzący do komputera i wychodzący z niego. W rezultacie stanie się on podatny na ataki hakerów. Ta opcja należy do rozważnych.

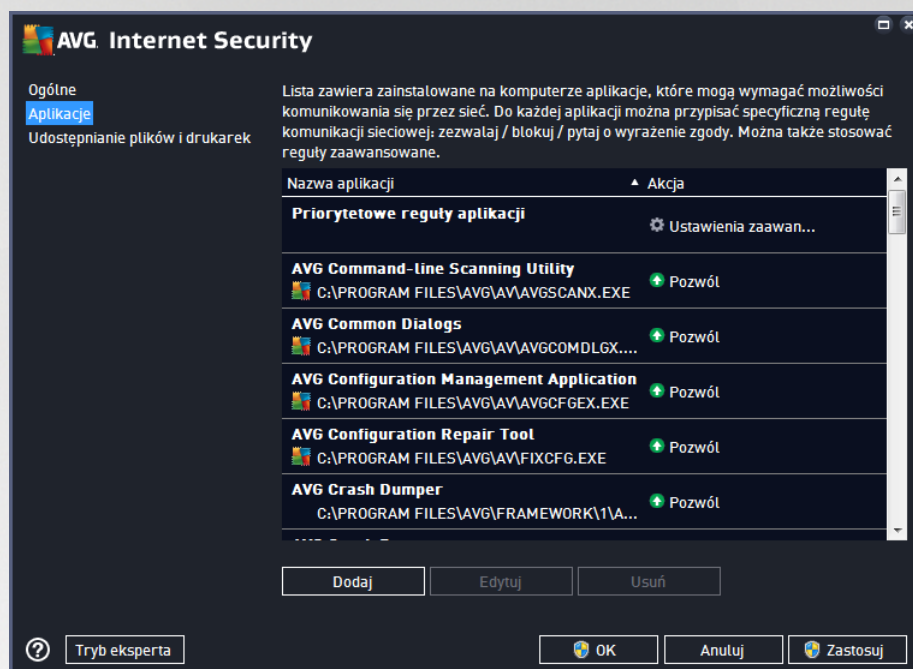
Należy zwrócić uwagę na specyficzny automatyczny tryb pracy Zapory. Tryb ten jest aktywowany w tle także wtedy, gdy składnik [Komputer](#) lub [Identity Protection](#) zostanie wyłączony, co naraża komputer na zwiększone niebezpieczeństwo. W takim przypadku Zapora zezwoli automatycznie na ruch sieciowy dotyczący tylko znanych i całkowicie bezpiecznych aplikacji. We wszystkich pozostałych przypadkach będzie wyświetlał monitory o podjętych decyzjach. Służy to zrównoważeniu ryzyka spowodowanego wyłączeniem



składnikami i jest sposobem na zachowanie bezpieczeństwa Twojego komputera.

8.2. Aplikacje

Okno **Aplikacje** wyświetla listę wszystkich aplikacji, które próbowały dotychczas nawiązać komunikację sieciową, oraz ikony pod tych akcji:



Aplikacje na liście **Lista aplikacji** zostały już wykryte na Twoim komputerze (i mają przypisane akcje). Dostępne akcje to:

- — odblokuj komunikację dla wszystkich sieci
- — zablokuj komunikację
- — zdefiniowano ustawienia zaawansowane

Przypominamy, że można wykryć tylko już zainstalowane aplikacje. Domyślnie, kiedy nowa aplikacja próbuje połączyć się z siecią po raz pierwszy, Zapora automatycznie utworzy dla niej regułę na podstawie bazy zaufanych aplikacji lub zapyta, czy komunikacja ma zostać zaakceptowana, czy zablokowana. W tym drugim przypadku można również zapisać odpowiedź jako stałą regułę (która wówczas zostanie dodana do listy w tym oknie dialogowym).

Można natychmiast zdefiniować reguły dla nowej aplikacji, używając w tym oknie dialogowym przycisku **Dodaj** i podać 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. w przypadku nieznanymi lub niezdefiniowanymi aplikacjami. Wybierz akcję, która ma zostać uruchomiona, gdy taka aplikacja próbuje skomunikować się przez sieć: **Blokuj** (komunikacja będzie zawsze blokowana), **Zezwól** (komunikacja



b dzie dozwolona we wszystkich sieciach), Pytaj (ka dorazowo zostanie wy wietlony monit o podj cie decyzji, czy nale y zezwoli na komunikacj). **Te pozycje maj inne opcje ni zwykle ustawienia aplikacji i s przeznaczone tylko dla do wiadczonych u ytkownikow. Stanowczo zalecamy, aby nie modyfikowa tych ustawie !**

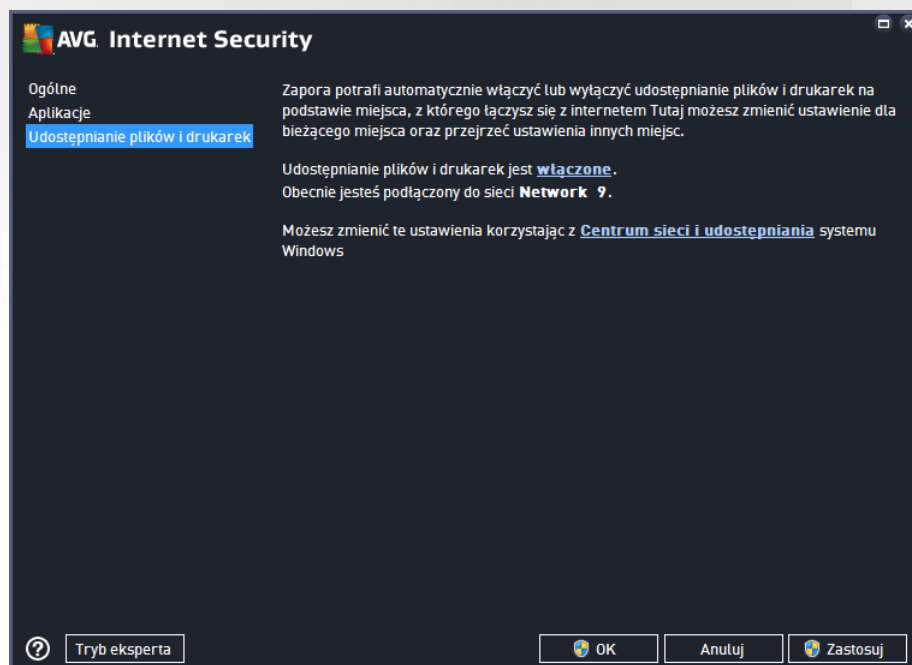
Przyciski kontrolne

List mo na edytowa przy u yciu nast puj cych przyciskow kontrolnych:

- **Dodaj** — otwiera puste okno dialogowe pozwalaj ce zdefiniowa nowe reguly aplikacji.
- **Edytuj** — otwiera to samo okno dialogowe pozwalaj ce edytowa zestaw regul aplikacji.
- **Usu** — usuwa wybran aplikacj z listy.

8.3. Udostępnianie plików i drukarek

Udostępnianie plików i drukarek oznacza w praktyce udostępnianie wszystkich plików i folderów, które oznaczysz jako udostępnione w systemie Windows, popularnych jednostkach dyskowych, drukarkach, skanerach i podobnych urządzeniach. Udostępnianie tego typu elementów jest po dane jedynie w sieciach uważanych za bezpieczne (np. w domu, w pracy lub w szkole). Je li jednak masz połączenie z sieci publicznej (np. sieci Wi-Fi na lotnisku lub w kawiarence internetowej), lepiej niczego nie udostępnia . Zapora AVG umo liwia łatwe zablokowanie lub odblokowanie udostępniania, a tak e zapisanie Twojej decyzji dotycz cej ju odwiedzonych sieci.

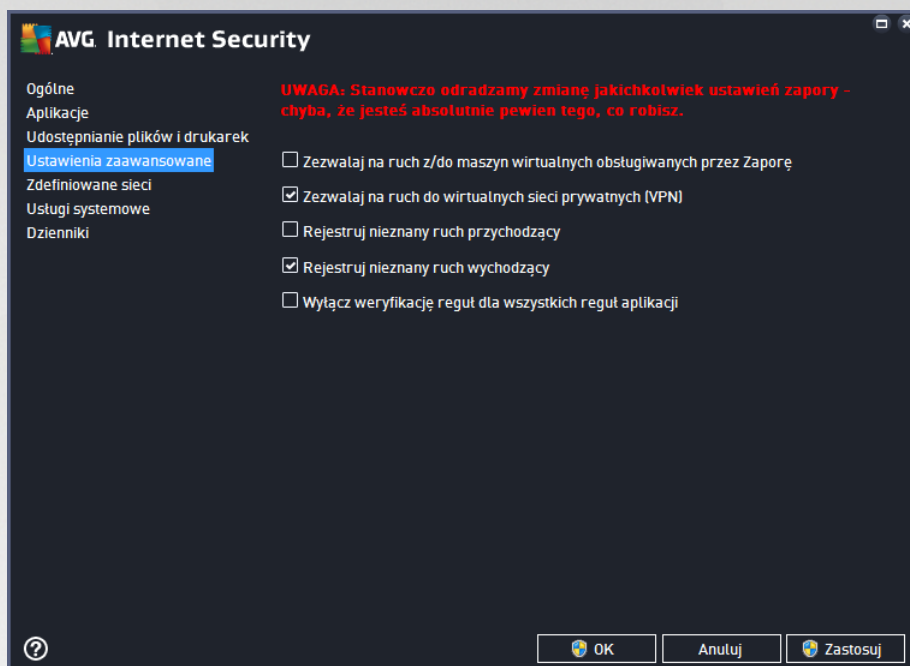


W oknie **Udostępnianie plików i drukarek** mo esz edytowa konfiguracj udostępniania plików i drukarek, a tak e obecnie podł czone sieci. W systemie Windows XP nazwa sieci odpowiada nazwie wybranej dla danej sieci podczas pierwszego połączenia z ni . W systemie Windows Vista i nowszych nazwa sieci pobierana jest automatycznie z Centrum sieci i udostępniania.



8.4. Ustawienia zaawansowane

Jakiegokolwiek zmiany w oknie Ustawie zaawansowanych powinny by wprowadzane JEDYNIEM PRZEZ DO WIADCZONYCH U YTKOWNIKÓW!



Okno **Ustawie zaawansowanych** umożliwia włączenie/wyłączenie następujących parametrów Zapory:

- **Zezwalaj na cały ruch z/do maszyn wirtualnych obsługiwanych przez zaporę** — obsługa połączeń sieciowych w maszynach wirtualnych, takich jak VMware.
- **Zezwalaj na cały ruch do wirtualnych sieci prywatnych (VPN)** — obsługa połączeń VPN (używanych do łączenia się z zdalnymi komputerami).
- **Rejestruj nieznaną ruch przychodzący/wychodzący** — wszystkie próby komunikacji (przychodzącej/wychodzącej) nieznanymi aplikacjami będą zapisywane w [dzienniku Zapory](#).
- **Wyłącz weryfikację reguł dla wszystkich reguł aplikacji** — Zapora w sposób ciągły monitoruje wszystkie pliki objęte poszczególnymi regułami aplikacji. W przypadku modyfikacji pliku binarnego Zapora ponownie potwierdzi wiarygodność aplikacji standardowymi sposobami, tzn. weryfikując jej certyfikat, wyszukując aplikacji w [bazie danych zaufanych aplikacji](#) itp. Jeśli aplikacji nie można uznać za bezpieczną, Zapora będzie nadal traktować ją zgodnie z [wybrany trybem](#):
 - o jeśli Zapora działa w [trybie automatycznym](#), aplikacja domyślnie nie będzie blokowana;
 - o jeśli Zapora działa w [trybie interaktywnym](#), aplikacja będzie blokowana i zostanie wyświetlone okno dialogowe z monitorem o podjęciu decyzji dotyczącej sposobu obsługi aplikacji.

Odpowiednie procedury obsługi dla każdej aplikacji można oczywiście zdefiniować w oknie dialogowym [Aplikacje](#).



8.5. Zdefiniowane sieci

Jakiegokolwiek modyfikacje w oknie Zdefiniowane sieci powinny by wprowadzane JEDYNIEM PRZEZ DO WIADCZONYCH U YTKOWNIKÓW!

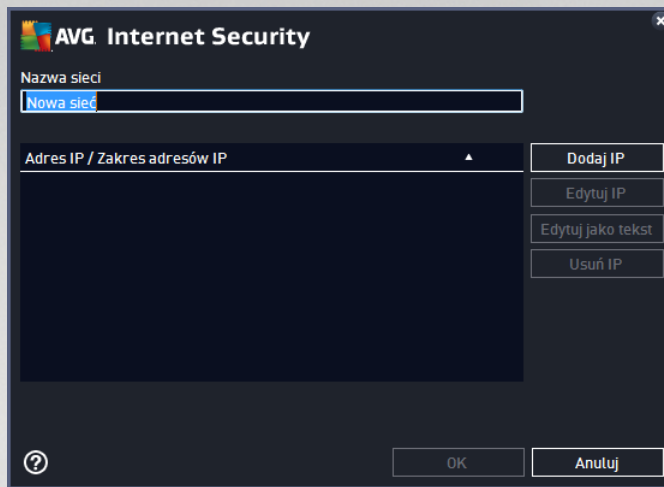


Okno dialogowe **Zdefiniowane sieci** zawiera listę wszystkich sieci, z którymi połączony jest Twój komputer. Lista zawiera następujące informacje o każdej z sieci:

- **Sieci** — lista nazw wszystkich sieci, do których połączony jest komputer.
- **Zakres adresów IP** — każda sieć zostanie automatycznie wykryta i określona w formie zakresu adresów IP.

Przyciski kontrolne

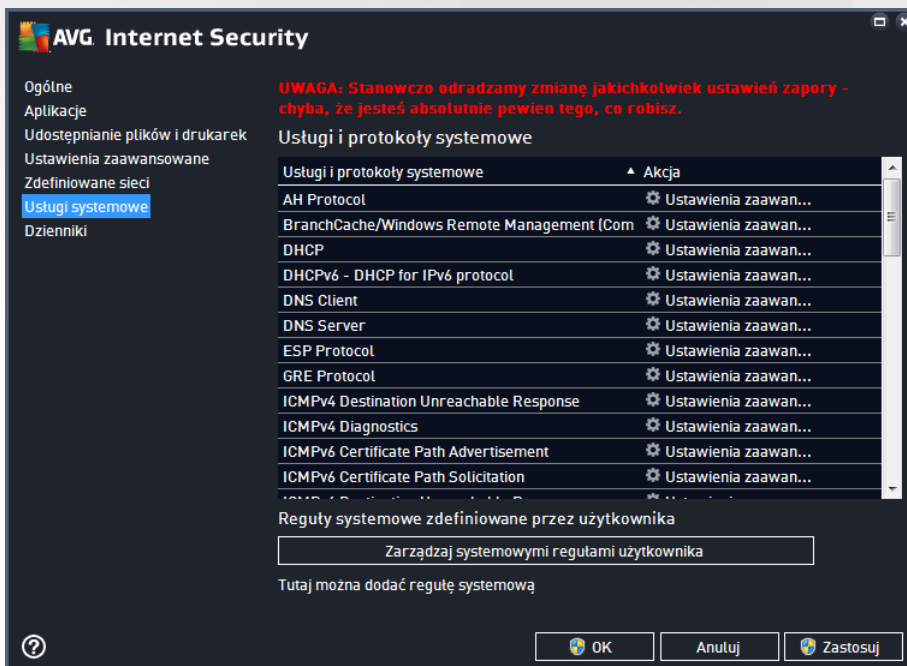
- **Dodaj sieć** — otwiera nowe okno dialogowe, w którym możesz edytować parametry nowo tworzonej sieci, tj. wprowadzić dane, takie jak **Nazwa sieci** i **Zakres adresów IP**.



- **Edytuj sieć** — powoduje otwarcie okna dialogowego *Właściwości sieci* (patrz wyżej), w którym można edytować parametry zdefiniowanej sieci (okno to jest identyczne jak okno wyświetlane podczas dodawania nowej sieci — zobacz opis w poprzednim akapicie).
- **Usuń sieć** — usuwa wybraną sieć z listy.

8.6. Usługi systemowe

Wszelkie zmiany w konfiguracji usług i protokołów systemowych powinny być wprowadzane JEDYNIEM przez dołączonych 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:

- **Usługi i protokoły systemowe** — w tej kolumnie wyświetlana jest nazwa odpowiedniej usługi



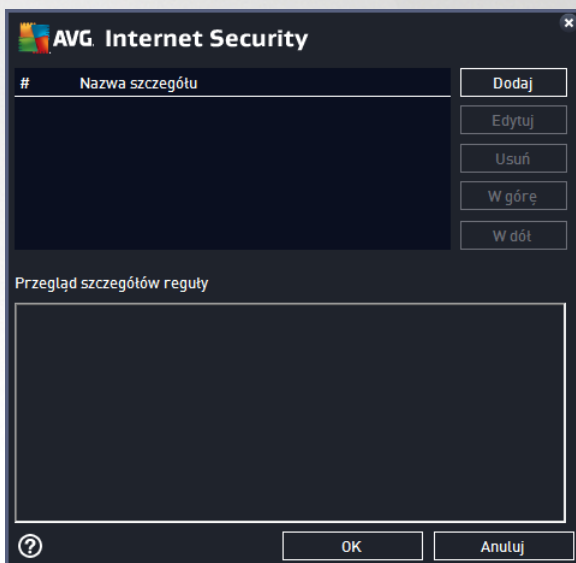
systemowej.

- **Akcja** — w tej kolumnie wyświetlana jest ikona przypisanej akcji:
 - Pozwól na komunikację we wszystkich sieciach
 - Blokuj komunikację

Aby edytować ustawienia dowolnej pozycji z listy (w tym przypisanych akcji), kliknij tą pozycję prawym przyciskiem myszy i wybierz polecenie **Edytuj**. **Edycja reguł systemowych powinna być przeprowadzana jedynie przez zaawansowanych użytkowników. Nie zaleca się ich zmieniania.**

Reguły systemowe zdefiniowane przez użytkownika

Aby otworzyć nowe okno dialogowe pozwalające definiować własne reguły usług systemowych (patrz ilustracja poniżej), kliknij przycisk **Zarządzaj systemowymi regułami użytkownika**. To samo okno dialogowe zostanie otwarte, gdy zechcesz edytować konfigurację dowolnej z istniejących pozycji usług systemowych i protokołów. Górna sekcja tego okna dialogowego zawiera przegląd wszystkich szczegółów edytowanej reguły systemowej. W dolnej sekcji wyświetlany jest wybrany szczegół. Szczegóły reguły mogą być dodawane, edytowane i usuwane, dzięki odpowiednim przyciskom



Należy pamiętać, że te ustawienia zaawansowane — przeznaczone przede wszystkim dla 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.

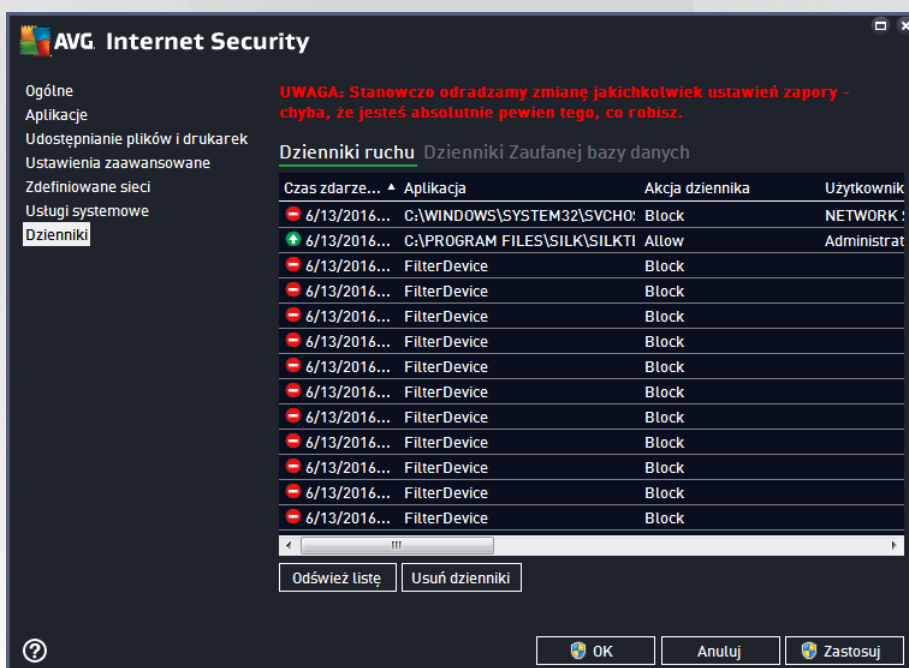


8.7. Dzienniki

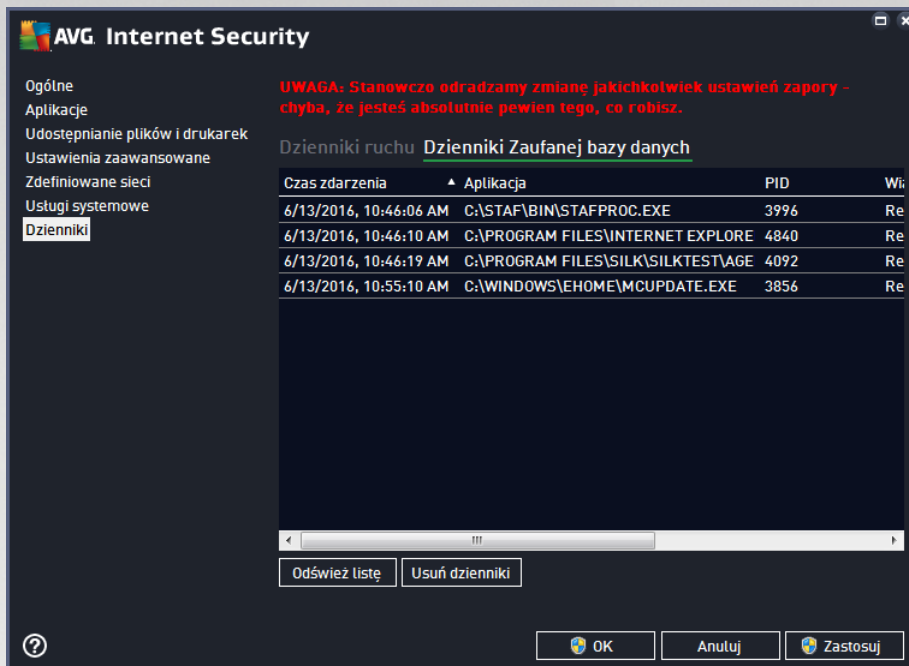
Jakiegokolwiek modyfikacje w oknie Dzienniki powinny by wprowadzane JEDYNIEM PRZEZ DO WIADCZONYCH U YTKOWNIKÓW!

Okno dialogowe **Dzienniki** umo liwia przegl danie listy wszystkich zarejestrowanych działa Zapory, ze szczególowym opisem odpowiednich parametrów na dwóch kartach:

- **Dzienniki ruchu** — ta karta wy wietla informacje o aktywno ci wszystkich aplikacji, które próbowały połączy si z sieci . Każda pozycja zawiera informacje o czasie wyst pienia zdarzenia, nazwie aplikacji, zarejestrowanej akcji, nazwie u ytkownika, numerze PID, kierunku ruchu, typie protokołu, numerze portu zdalnego i lokalnego, a tak e zdalnym i lokalnym adresie IP.



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



Przyciski kontrolne

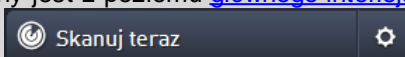
- **Od wie list** — wszystkie zarejestrowane parametry mo na uporz dkowa według wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) — wystarczy klikn odpowiedni nagłówek kolumny. U yj przycisku **Od wie list** , aby zaktualizowa wy wietlane informacje.
- **Usu dzienniki** — pozwala usun wszystkie wpisy z wykresu.



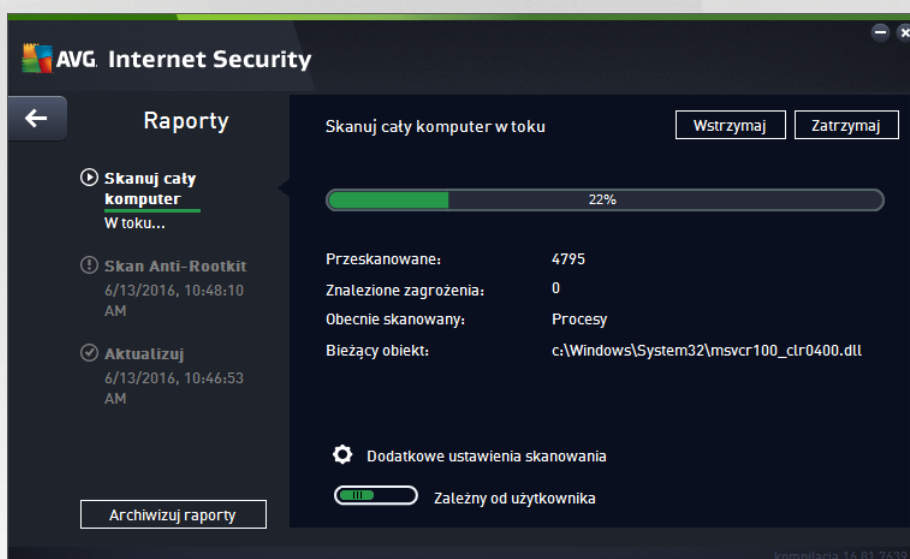
9. Skanowanie AVG

Domylnie program **AVG Internet Security** nie uruchamia żadnych skanowań, ponieważ po przeprowadzeniu wstępnego skanowania (o którego wykonaniu przypomni monitor ochrony) zapewnia rezydentne składniki programu **AVG Internet Security**, które przez cały czas pilnują, aby złe oprogramowanie nie dostało się na Twój komputer. Oczywiście możesz też [zaplanować skanowanie](#) w regularnych odstępach czasu lub uruchamiać je ręcznie w zależności od potrzeb.

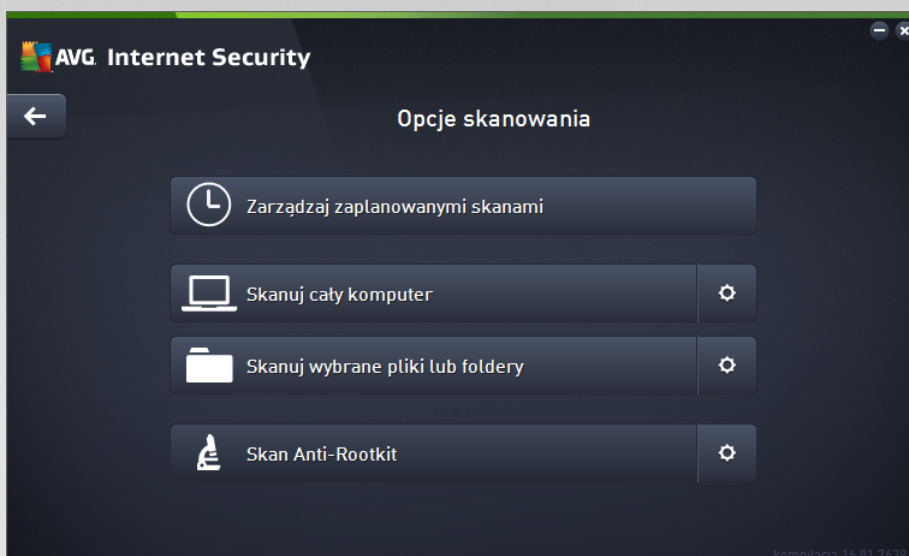
Interfejs skanera AVG dostępny jest z poziomu [głównego interfejsu użytkownika](#) za pośrednictwem przycisku podzielonego na dwie sekcje:



- **Skanuj teraz** — kliknij ten przycisk, aby natychmiast uruchomić funkcję [Skanowanie całego komputera](#) i obserwować jego postęp oraz wyniki w otwartym oknie [Raporty](#):



- **Opcje** — użyj tego przycisku (przedstawionego graficznie jako trzy poziome linie na zielonym tle) aby otworzyć obszar **Opcje skanowania**, który umożliwia [zarządzanie zaplanowanymi skanowaniami](#) oraz edytowanie parametrów funkcji [Skanowania całego komputera/Skanowania określonych plików lub folderów](#).



W oknie **Opcje skanowania** s widoczne trzy główne sekcje konfiguracji skanowania:

- **Zarządzaj zaplanowanymi skanami** — wybierz tę opcję, aby otworzyć nowe [okno dialogowe zawierające przegląd wszystkich harmonogramów skanowania](#). Zanim zdefiniujesz własne harmonogramy, zobaczysz jedynie jeden skan zaplanowany, zdefiniowany wstępnie przez producenta oprogramowania. Skanowanie to jest domyślnie wyłączone. Aby je włączyć, kliknij jego prawym przyciskiem i wybierz z menu kontekstowego opcję *Włącz zadanie*. Po włączeniu skanu zaplanowanego możesz [edytować jego konfigurację](#), klikając przycisk *Edytuj harmonogram skanowania*. Możesz także kliknąć przycisk *Dodaj harmonogram skanowania*, aby utworzyć nowy, własny harmonogram.
- **Skanuj cały komputer / Ustawienia** — Ten przycisk składa się z dwóch sekcji. Kliknij opcję *Skanuj cały komputer*, aby natychmiast uruchomić skanowanie całego komputera (*szczegóły dotyczące skanowania całego komputera można znaleźć w odpowiednim rozdziale, zatytułowanym [Predefiniowane skany / Skanuj cały komputer](#)*). Kliknięcie sekcji *Ustawienia* przeniesie Cię do okna [konfiguracji skanowania całego komputera](#).
- **Skanuj wybrane pliki lub foldery / Ustawienia** — ten przycisk również podzielony jest na dwie części. Kliknij opcję *Skanuj wybrane pliki lub foldery*, aby natychmiast uruchomić skanowanie wybranych obszarów komputera (*szczegóły dotyczące skanowania określonych plików lub folderów znajdują się w odpowiednim rozdziale, zatytułowanym [Predefiniowane skany / Skan wybranych plików lub folderów](#)*). Kliknięcie sekcji *Ustawienia* przeniesie Cię do [okna konfiguracji skanowania wybranych plików lub folderów](#).
- **Skanuj komputer w poszukiwaniu programów typu rootkit / Ustawienia** — lewa część przycisku z etykietą *Skanuj komputer w poszukiwaniu programów typu rootkit* uruchamia automatyczne skanowanie anty-rootkit (*więcej szczegółów na temat skanowania rootkit znajdziesz w odpowiednim rozdziale zatytułowanym [Predefiniowane skany / Skanuj komputer w poszukiwaniu programów typu rootkit](#)*). Kliknięcie sekcji *Ustawienia* przeniesie Cię do [okna konfiguracji skanowania programów typu rootkit](#).



9.1. Wstępnie zdefiniowane skany

Jedną z głównych funkcji oprogramowania **AVG Internet Security** jest skanowanie na żądanie. Testy na żądanie służą do skanowania konkretnych obszarów komputera, gdy użytkownik podejrzewa obecność wirusa. Stanowczo zaleca się jednak wykonywanie tych testów regularnie, nawet w przypadku, gdy brak jest takich podejrzeń.

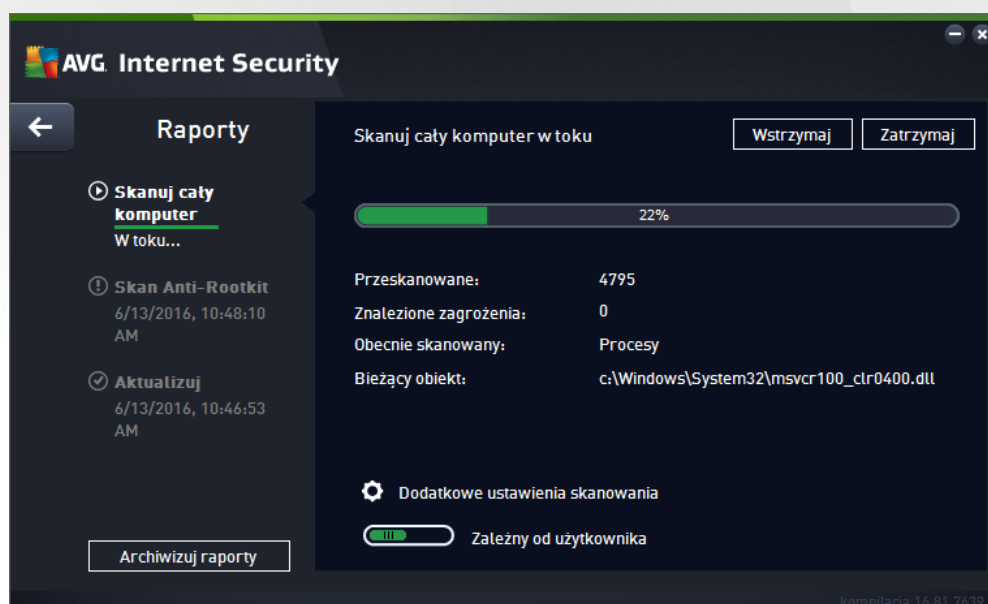
W oprogramowaniu **AVG Internet Security** dostępne są następujące typy skanowania zdefiniowane wstępnie przez producenta:

9.1.1. Skanuj cały komputer

Skanuj cały komputer — skanuje cały komputer w poszukiwaniu możliwych infekcji i/lub potencjalnie niechcianych aplikacji. Ten test 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.

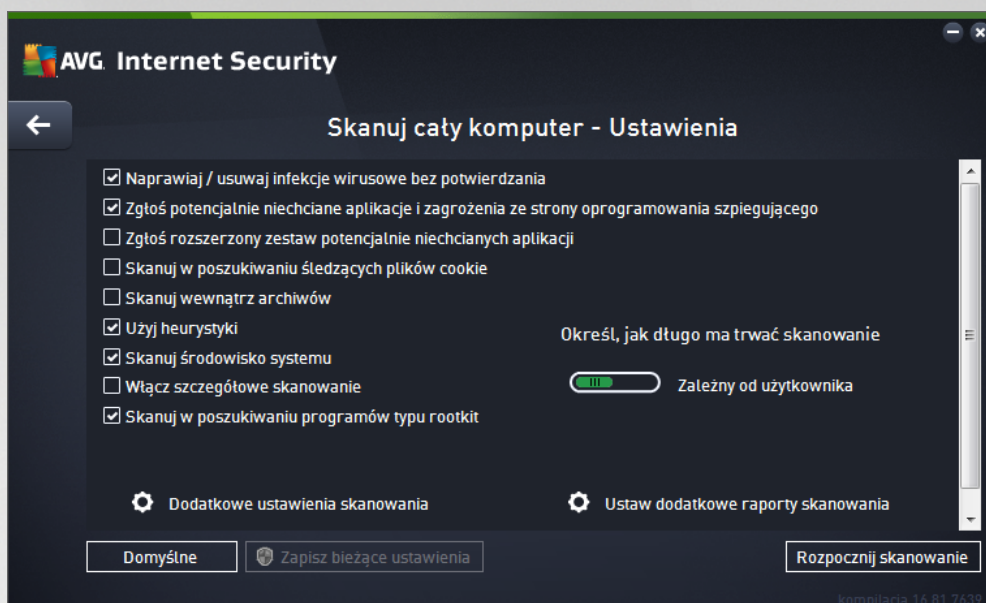
Uruchamianie skanowania

Funkcja **Skanuj cały komputer** może zostać uruchomiona bezpośrednio z poziomu [głównego interfejsu użytkownika](#) przez kliknięcie przycisku **Skanuj teraz**. Dla tego rodzaju skanowania nie są wymagane żadne dodatkowe ustawienia; skanowanie rozpocznie się natychmiast. W oknie **Skan całego komputera w toku** (patrz zrzut ekranu) możesz obserwować jego postęp i wyniki. W razie potrzeby skanowanie można tymczasowo przerwać (**Wstrzymaj**) lub anulować (**Zatrzymaj**).



Edycja konfiguracji skanowania

Możesz edytować konfigurację opcji **Skanuj cały komputer** w oknie **Skanuj cały komputer — ustawienia** (okno jest dostępne przez kliknięcie linku [Ustawienia w oknie Opcje skanowania](#)). **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



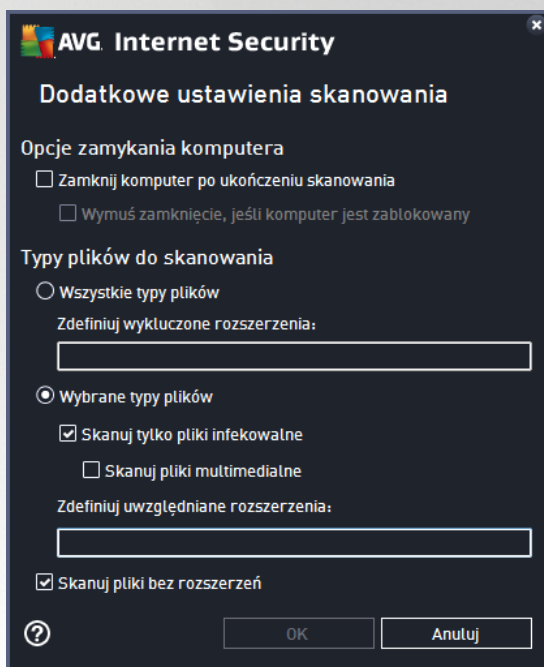
Na liście parametrów skanowania można włączyć / wyłączyć określone parametry w zależności od potrzeb:

- **Naprawiaj / usuwaj infekcje wirusowe bez potwierdzenia** (opcja domyślnie włączona) — jeżeli podczas skanowania wykryty zostanie wirus, oprogramowanie AVG podejmie próbę automatycznego wyleczenia go. Jeżeli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).
- **Raportuj potencjalnie niechciane aplikacje oraz oprogramowanie szpiegujące** (domyślnie włączone) — zaznaczenie tego pola umożliwia skanowanie 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 zniższa ona poziom ochrony komputera.
- **Zgłoś rozszerzony zestaw potencjalnie niechcianych aplikacji** (domyślnie wyłączona) — zaznaczenie tej opcji pozwala wykrywać wieszaki oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojemu komputerowi. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego ta opcja domyślnie jest wyłączona.
- **Skanuj w poszukiwaniu śledzących plików cookie** (opcja domyślnie wyłączona) — ten parametr 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 zawartości koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** (domyślnie wyłączona) — ten parametr określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz 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 skanowania.
- **Skanuj środowisko systemu** (domyślnie włączona) — skanowanie obejmie także obszary



systemowe komputera.

- **Wł cz szczegółowe skanowanie** (domy Inie wł czone) — w okre lonych sytuacjach (gdy zachodzi podejrzenie, e komputer jest zainfekowany) mo na zaznaczy t opcj , aby aktywowa dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewno ci b d one skanowa nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Naley pami ta , e ta metoda skanowania jest do czasochłonna.
- **Skanuj w poszukiwaniu programów typu rootkit** (domy Inie wł czone) — uwzgl dnia skanowanie anti-rootkit podczas skanu całego komputera. [Skan anti-rootkit](#) mo e by równie uruchomiony osobno.
- **Dodatkowe ustawienia skanowania** — link do okna dialogowego Dodatkowe ustawienia skanowania, w którym mo na okre li nast puj ce parametry:

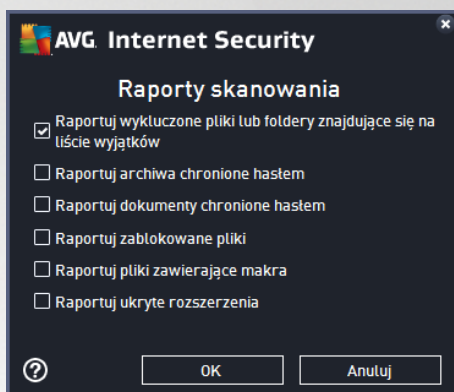


- **Opcje wył czania komputera** — okre l, czy komputer ma zosta automatycznie wył czony po zako czeniu skanowania. Wybranie opcji (**Zamknij komputer po uko czeniu skanowania**) spowoduje aktywowanie nowej funkcji, która pozwala zamkn komputer nawet wtedy, gdy w danej chwili jest on zablokowany (**Wymu zamkni cie, je li komputer jest zablokowany**).
- **Typy plików do skanowania** — zdecyduj, które z poni szych elementów maj by skanowane:
 - **Wszystkie typy plików** z opcj zdefiniowania wyj tków skanera przez wprowadzenie rozdzielonych przecinkami rozszerze , które nie powinny by skanowane;
 - **Wybrane typy plików** — skanowane b d tylko pliki, które mog zosta zainfekowane (pliki, które nie mog zosta zainfekowane, nie b d skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne) z uwzgl dnieniem plików multimedialnych (plików wideo i audio — je li to pole pozostanie niezaznaczone, czas skanowania skróci



si jeszcze bardziej, ponieważ takie pliki cz sto s du e, a nie s podatne na infekcje). Za pomoc rozszerze mo na okre li , które pliki maj by zawsze skanowane.

- Opcjonalnie mo na wybra **Skanowanie plików bez rozszerzenia** — ta opcja jest domy lnie wł czona i zaleca si , aby nie zmienia tego stanu bez wa nego powodu. Pliki bez rozszerzenia s podejrzane i powinny by skanowane za ka dym razem.
- **Okre l, jak dugo ma trwa skanowanie** — za pomoc suwaka mo na zmieni priorytet procesu skanowania. Domy lna warto to poziom *Zale ny od u ytkownika*, co oznacza automatycznie dobre wykorzystanie zasobów. Dost pne s tak e inne opcje: mo na wybra skanowanie wolne, które minimalizuje obci enie zasobów systemowych (*przydatne, gdy komputer jest u ywany w czasie skanowania, a czas jego trwania nie ma znaczenia*), lub skanowanie szybkie, które oznacza intensywniejsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo u ywany*).
- **Ustaw dodatkowe raporty skanowania** — ten link pozwala otworzy nowe okno dialogowe **Raporty skanowania**, w którym mo na okre li raportowane elementy lub zdarzenia:



Ostrze enie: Ustawienia te s identyczne jak domy lne parametry nowo utworzonego skanowania — zgodnie z opisem w rozdziale [Skanowanie AVG / Planowanie skanowania / Jak skanowa](#) . Je li jednak domy lna konfiguracja testu **Skan caego komputera** zostanie zmieniona, nowe ustawienia mo na zapisa jako konfiguracj domy ln , aby były u ywane we wszystkich przyszłych skanach caego komputera.

9.1.2. Skanuj wybrane pliki lub foldery

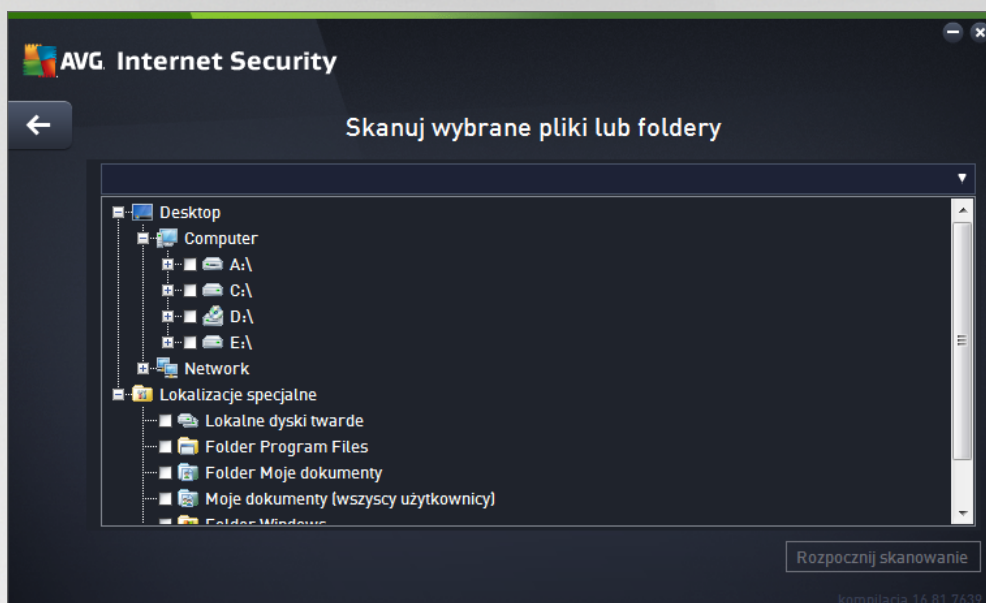
Skanuj wybrane pliki lub foldery — skanowane s tylko wskazane obszary komputera (*wybrane foldery, dyski twarde, pamici flash, dyski CD itp.*). Post powanie w przypadku wykrycia wirusów jest takie samo jak przy skanowaniu caego komputera: ka dy znaleziony wirus jest leczony lub przenoszony do [Przechowalni wirusów](#) . Skanowanie okre lonych plików lub folderów mo e postu y do utworzenia własnych testów i planowania ich zgodnie z konkretnymi potrzebami.

Uruchamianie skanowania

Funkcj **Skanuj wybrane pliki lub foldery** mo na wywoła bezpo rednio z okna [Opcje skanowania](#) przez klikni cie przycisku **Skanuj wybrane pliki lub foldery**. Zostanie wy wietlone nowe okno dialogowe **Wybierz pliki lub foldery do przeskanowania**. W drzewie dysków komputera wybierz foldery, które maj zosta przeskanowane. kieki do wszystkich wybranych folderów zostan wygenerowane automatycznie i wy wietlone w polu tekstowym w górnej cz ci okna dialogowego. Mo na tak e przeskanowa wybrany folder, wykluczaj c jednocze nie ze skanowania wszystkie jego podfoldery: nale y wprowadzi znak minus „-”

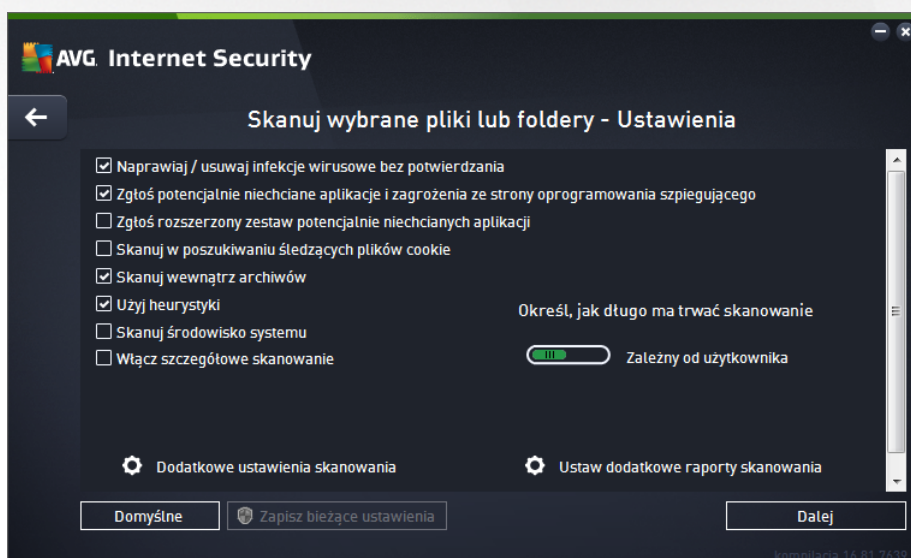


przed jego nazwą w wygenerowanej ścieżce (*patrz zrzut ekranu*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „!”. Na koniec, aby uruchomić skanowanie, należy kliknąć przycisk **Rozpocznij skanowanie**; proces skanowania jest w zasadzie taki sam jak w przypadku [Skanu całego komputera](#).



Edycja konfiguracji skanowania

Możesz edytować konfigurację funkcji **Skan określonych plików lub folderów** w oknie **Skanuj wybrane pliki lub foldery — ustawienia** (to okno jest dostępne przez kliknięcie linku [Ustawienia widocznego w oknie Opcje skanowania](#)). **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



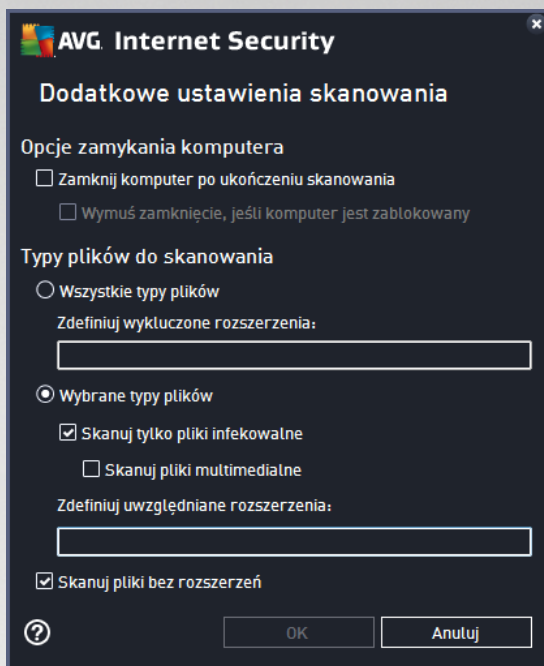
Na liście parametrów skanowania możesz w miarę potrzeb włączyć / wyłączyć następujące parametry:

- **Naprawiaj / usuwaj infekcje wirusowe bez potwierdzenia** (domyślnie włączone): Jeśli podczas skanowania zostanie wykryty wirus, system AVG podejmie próbę automatycznego wyleczenia go.



Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).

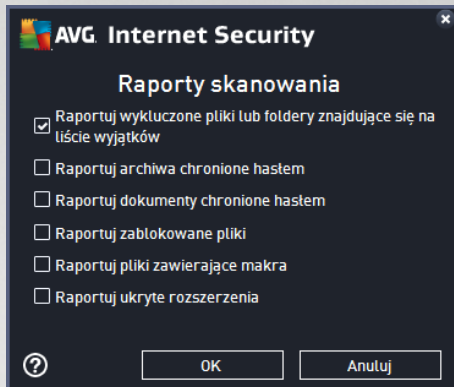
- **Zgłoś potencjalnie niechciane aplikacje i zagrożenia ze strony oprogramowania szpiegującego** (domyślnie wyłączone): zaznaczenie tego pola aktywuje skanowanie w poszukiwaniu oprogramowania szpiegującego (a nie tylko wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączenia tej opcji — znacząco zmniejsza ona poziom ochrony komputera.
- **Zgłoś rozszerzony zestaw potencjalnie niechcianych aplikacji** (domyślnie wyłączone): zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojemu komputerowi. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego ta opcja domyślnie jest wyłączona.
- **Skanuj w poszukiwaniu ledzących plików cookie** (domyślnie wyłączone): ten parametr określa, czy wykrywane mają być pliki cookie (używane w protokole HTTP do uwierzytelniania, ledzenia i przechowywania określonych informacji o użytkownikach, np. ustawień witryn i zawartości koszyków w sklepach internetowych).
- **Skanuj wewnątrz archiwów** (domyślnie wyłączone): ten parametr określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR.
- **Użyj heurystyki** (domyślnie wyłączone): analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej) jest jedną z metod wykrywania wirusów w czasie skanowania.
- **Skanuj środowisko systemu** (domyślnie wyłączone): skanowanie obejmie także obszary systemowe komputera.
- **Wyłącz szczegółowe skanowanie** (domyślnie wyłączone): w określonych sytuacjach (gdy zachodzi podejrzenie, że komputer jest zainfekowany) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będzie one skanowały nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest dość czasochłonna.
- **Dodatkowe ustawienia skanowania** — link do okna dialogowego **Dodatkowe ustawienia skanowania**, w którym można określić następujące parametry:



- **Opcje wyłączenia komputera** — określa, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie opcji (**Zamknij komputer po ukończeniu skanowania**) spowoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet wtedy, gdy w danej chwili jest on zablokowany (**Wymuś zamknięcie, jeśli komputer jest zablokowany**).
- **Typy plików do skanowania** — zdecyduj, które z poniższych elementów mają być skanowane:
 - **Wszystkie typy plików** z opcji zdefiniowania wyłączeń skanera przez wprowadzenie rozdzielonych przecinkami rozszerzeń, które nie powinny być skanowane;
 - **Wybrane typy plików** — skanowane będą tylko pliki, które mogą zostać zainfekowane (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 — jeżeli to pole zostanie niezaznaczone, czas skanowania 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 wybrać **Skanowanie plików bez rozszerzenia** — ta opcja jest domyślnie wyłączona i zaleca się, aby nie zmieniać tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane łącznie.
- **Określ, jak długo ma trwać skanowanie** — za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślną wartością jest poziom *Zalecany od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Dostępne są także inne opcje: można wybrać skanowanie wolne, które minimalizuje obciążenie zasobów systemowych (*przydatne, gdy komputer jest używany w czasie skanowania, a czas jego trwania nie ma znaczenia*), lub skanowanie szybkie, które oznacza intensywniejsze wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).



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



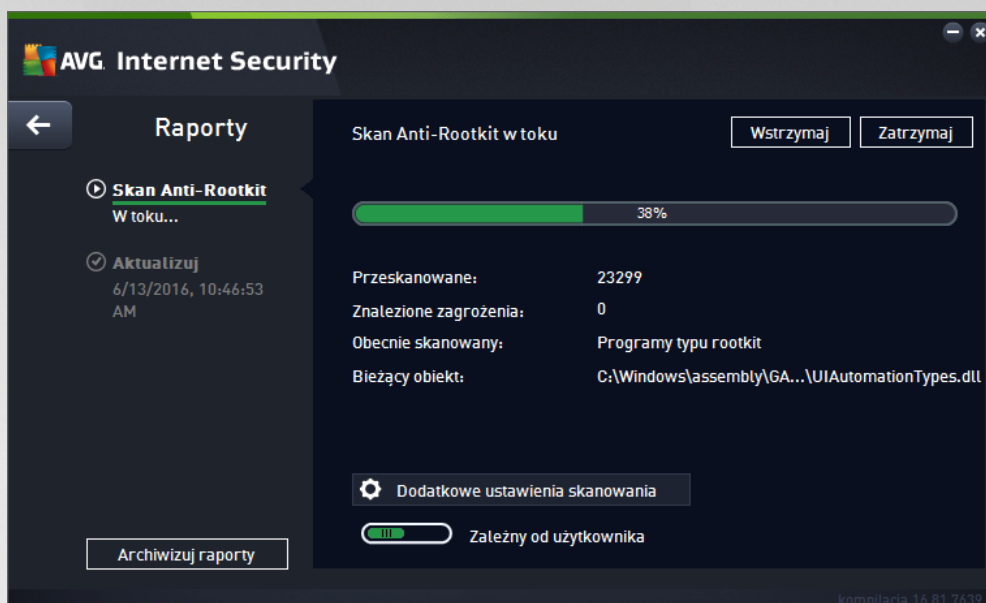
Ostrzeżenie: Ustawienia te są identyczne jak domyślne parametry nowo utworzonego skanowania — zgodnie z opisem w rozdziale [Skanowanie AVG / Planowanie skanowania / Jak skanować](#). Jeśli jednak domyślna konfiguracja testu **Skanuj wybrane pliki lub foldery** zostanie zmieniona, nowe ustawienia będą zapisane jako konfiguracja domyślna, która będzie używana we wszystkich zdefiniowanych w przyszłości skanach określonych plików lub folderów. Stanie się ona również szablonem dla wszystkich nowych skanów zaplanowanych ([wszystkie testy u użytkownika są oparte na bieżącej konfiguracji skanu wybranych plików lub folderów](#)).

9.1.3. Skanuj komputer w poszukiwaniu rootkitów

Skanuj komputer w poszukiwaniu rootkitów to specjalistyczne narzędzie do wykrywania i skutecznego usuwania niebezpiecznych rootkitów (programów i technologii, które mogą kamuflować obecność szkodliwego oprogramowania na komputerze). Rootkit to program zaprojektowany w celu przejęcia całkowitej kontroli nad systemem komputerowym bez zgody jego właścicieli czy upoważnionych administratorów. Składnik ten umożliwia wykrywanie rootkitów na podstawie wstępnie zdefiniowanego zestawu reguł. Jeśli znaleziony zostanie plik rootkit, nie zawsze oznacza to, że jest on zainfekowany. Niekiedy programy typu rootkit są używane jako sterowniki lub jako komponenty innych, pożytecznych aplikacji.

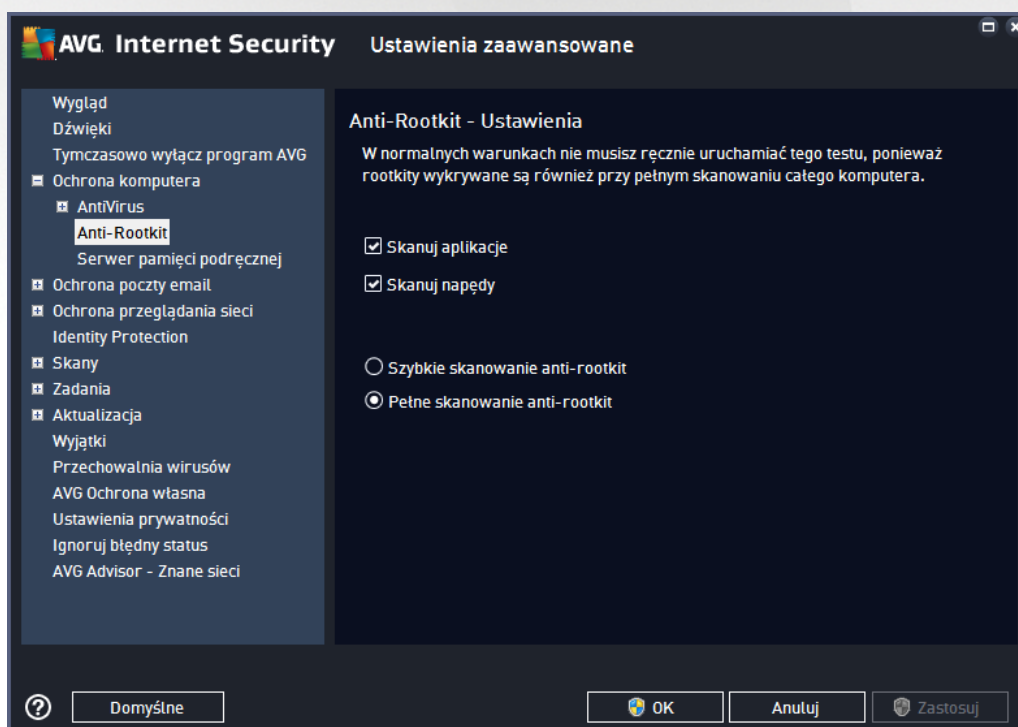
Uruchamianie skanowania

Funkcja **Skanuj komputer w poszukiwaniu rootkitów** może być uruchomiona bezpośrednio z okna [Opcje skanowania](#) po kliknięciu przycisku **Skanuj komputer w poszukiwaniu rootkitów**. Pojawi się wówczas nowe okno o tytule **Trwa skanowanie plików Anti-rootkit**, w którym wyświetlony będzie postęp skanowania:



Edycja konfiguracji skanowania

Możesz edytować konfigurację skanu Anti-Rootkit w oknie dialogowym **Ustawienia Anti-Rootkit** (okno to jest dostępne przez link [Ustawienia](#) w sekcji [Skanowanie komputera](#) w poszukiwaniu rootkitów w oknie [Opcje skanowania](#)). **Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!**



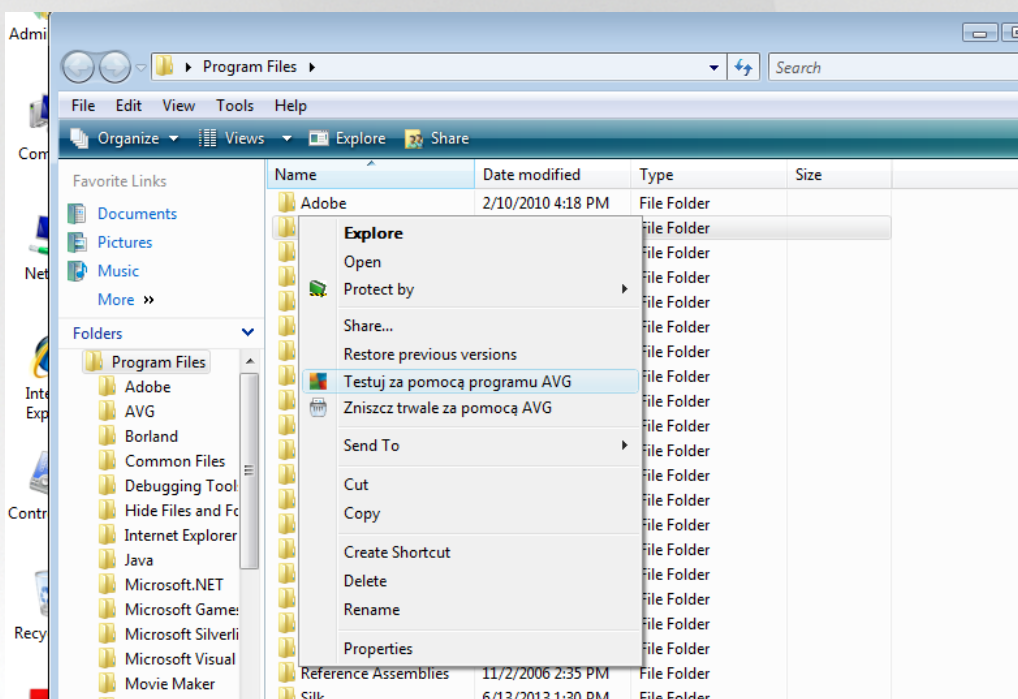
Opcje **Skanuj aplikacje** i **Skanuj napędy** pozwalają szczegółowo określić zakres skanowania Anti-Rootkit. Ustawienia te są przeznaczone dla użytkowników zaawansowanych. Zaleca się pozostawienie wszystkich opcji włączonych. Można również wybrać tryb skanowania w poszukiwaniu rootkitów:



- **Szybkie skanowanie anti-rootkit** — skanuje wszystkie uruchomione procesy, załadowane sterowniki i folder systemowy (zazwyczaj *c:\Windows*)
- **Pełne skanowanie anti-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 dyskietyk/płyt CD)

9.2. Skanowanie w Eksploratorze Windows

Oprócz wstępnie zdefiniowanych skanowań obejmujących cały komputer lub wybrane obszary, system **AVG Internet Security** 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 danie”. W tym celu należy wykonać następujące kroki:



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

9.3. Skanowanie z wiersza polecenia

Oprogramowanie **AVG Internet Security** oferuje możliwość uruchamiania skanowania z wiersza polecenia. Opcji tej można używać na przykład na serwerach lub przy tworzeniu skryptu wsadowego, który ma być uruchamiany po każdym rozruchu komputera. Uruchamiając skanowanie z wiersza polecenia, można używać różnych parametrów dostępnych w graficznym interfejsie użytkownika AVG.

Aby uruchomić skanowanie z wiersza polecenia, należy wykonać następujące polecenie w folderze, w którym zainstalowano system:



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

9.3.1. Składnia polecenia

Składnia polecenia jest następująca:

- **avgscanx /parametr** — np. **avgscanx /comp** w celu przeskanowania całego komputera
- **avgscanx /parametr /parametr** — jeżeli używanych jest wiele parametrów, należy wpisać je w jednym wierszu, rozdzielając spacjami i ukośnikami
- Jeżeli parametry wymagają podania określonych wartości, (np. parametr **/scan** wymaga informacji o wybranych do przeskanowania obszarach komputera, więc należy wskazać dokładnie kolumny), należy je rozdzielić średnikami, na przykład: **avgscanx /scan=C:\;D:**

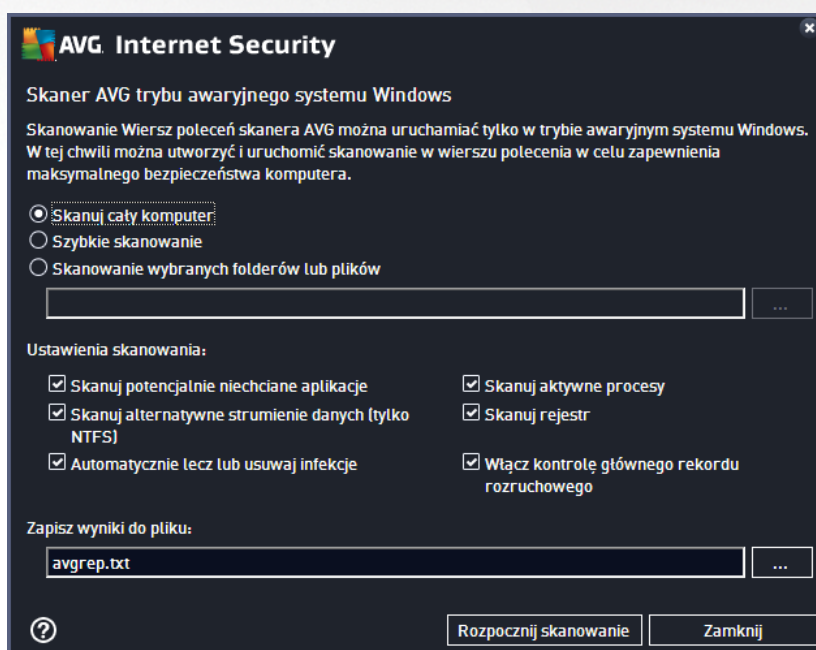
9.3.2. Parametry skanowania

Aby wyświetlić pełny przegląd dostępnych parametrów, wpisz odpowiednie polecenie z parametrem **/?** 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 [przebieg parametrów wiersza poleceń](#).

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

9.3.3. 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:





Tryb awaryjny umożliwia uruchamianie skanowania z wiersza polecenia. To okno dialogowe umożliwia określenie parametrów skanowania przy użyciu wygodnego interfejsu graficznego.

Najpierw wybierz obszary komputera, które mają zostać przeskanowane: Możesz wybrać wcześniej zdefiniowaną opcję **Skanuj cały komputer** lub opcję **Skanuj wybrane foldery lub pliki**. Trzecia opcja, **Szybkie skanowanie**, powoduje uruchomienie skanowania specjalnie przeznaczonego dla trybu awaryjnego i obejmującego wszystkie niewrażliwe obszary komputera niezbędne do jego uruchomienia.

Ustawienia skanowania w następującej sekcji pozwalają określić dodatkowe szczegółowe parametry skanowania. Każde z nich jest domyślnie zaznaczone i zalecamy pozostawienie takiej konfiguracji. Zaznaczenia tych parametrów nie należy usuwać bez wyraźnej przyczyny.

- **Skanuj „potencjalnie niechciane aplikacje”** — skanowanie w poszukiwaniu oprogramowania szpiegującego (oprócz wirusów)
- **Skanuj alternatywne strumienie danych (tylko w systemie plików NTFS)** — skanowanie alternatywnych strumieni danych NTFS tj. funkcji systemu Windows, która może być wykorzystywana przez hakerów do ukrywania danych (w szczególności szkodliwego kodu).
- **Lecz lub usuwaj infekcje automatycznie** — wszystkie możliwe detekcje zostaną automatycznie wyleczone lub usunięte z komputera
- **Skanuj aktywne procesy** — skanowanie procesów i aplikacji załadowanych do pamięci komputera
- **Skanuj rejestr** — skanowanie rejestru systemu Windows
- **Włącz sprawdzanie głównego rekordu rozruchowego** — skanowanie tablicy partycji i sektora rozruchowego

W dolnej części okna dialogowego można określić nazwę pliku i typ raportu skanowania.

9.3.4. Parametry skanowania CMD

Oto lista parametrów dostępnych dla skanowania z wiersza poleceń:

- /? Wyświetl pomoc na ten temat
- /@ Plik polecenia/nazwa pliku/
- /ADS Skanuj alternatywne strumienie danych (*tylko NTFS*)
- /ARC Skanuj archiwa
- /ARCBOMBSW Raportuj wielokrotnie spakowane archiwa
- /ARCBOMBSW Raportuj archiwa wielokrotnie (*wielokrotnie skompresowane*)
- /BOOT Włącz sprawdzanie MBR/sektora rozruchowego
- /BOOTPATH Uruchom szybkie skanowanie
- /CLEAN Oczyszczaj automatycznie



- /CLOUDCHECK Sprawdzaj pod kątem błędnych wykry
- /COMP [Skan całego komputera](#)
- /COO Skanuj pliki cookie
- /EXCLUDE Wyklucz ze skanowania cię k lub pliki
- /EXT Skanuj te rozszerzenia *(na przykład EXT=EXE,DLL)*
- /FORCESHUTDOWN Wymuś zamknięcie komputera po ukończeniu skanowania
- /HELP Wyświetl pomoc na ten temat
- /HEUR Użyj analizy heurystycznej
- /HIDDEN Raportuj pliki z ukrytymi rozszerzeniami
- /IGNLOCKED Ignoruj pliki zablokowane
- /INFECTABLEONLY Skanuj tylko pliki z rozszerzeniami umożliwiającymi infekcje
- /LOG Generuj plik z wynikami skanowania
- /MACROW Raportuj makra
- /NOBREAK Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- /NOEXT Nie skanuj tych rozszerzeń *(na przykład NOEXT=JPG)*
- /PRIORITY Ustaw priorytet skanowania *(Niski, Automatyczny, Wysoki — zobacz [Ustawienia zaawansowane/Skany](#))*
- /PROC Skanuj aktywne procesy
- /PUP Raportuj potencjalnie niechciane aplikacje
- /PUPEXT Raportuj rozszerzony zestaw potencjalnie niechcianych aplikacji
- /PWDW Raportuj pliki chronione hasłem
- /QT Szybki test
- /REG Skanuj rejestr
- /REPAPPEND Dopisz do pliku raportu
- /REPOK Raportuj niezainfekowane pliki jako OK
- /REPORT Raportuj do pliku *(nazwa pliku)*
- /SCAN [Skanuj określone pliki lub foldery](#) *(SCAN= cię ka; cię ka np. /SCAN=C:\;D:\)*

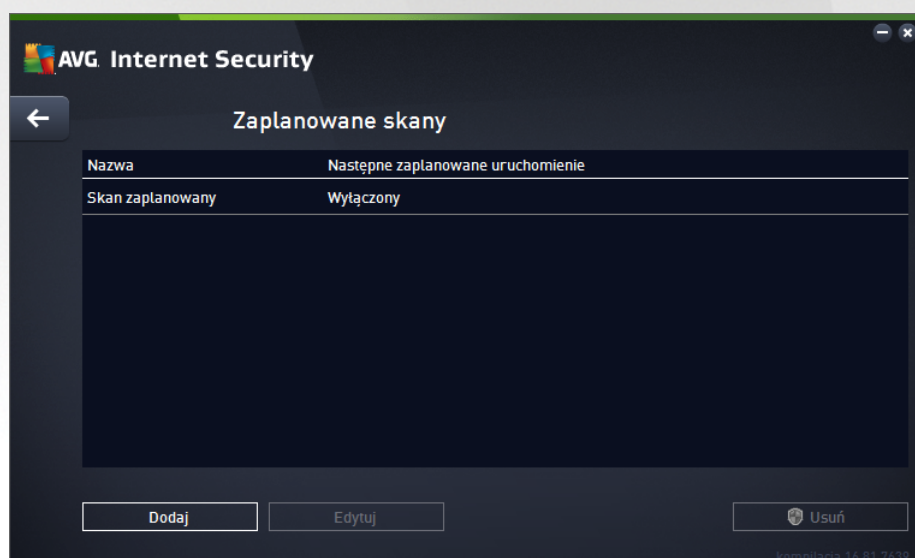


- /SHUTDOWN Zamknij komputer po ukończeniu skanowania
- /THOROUGHSCAN Włącz szczegółowe skanowanie
- /TRASH Przenieś zainfekowane pliki do [Przechowalni wirusów](#)

9.4. Planowanie skanowania

Oprogramowanie **AVG Internet Security** pozwala uruchamiać skanowanie na żądanie (na przykład gdy podejrzewa się infekcję komputera) lub zgodnie z założonym harmonogramem. Stanowczo zaleca się korzystanie 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 wyłączony, pominięty z tego powodu skan zaplanowany jest uruchamiany [po ponownym włączeniu komputera](#).

Harmonogram skanowania można utworzyć lub edytować w oknie **Skany zaplanowane**, dostępnym za pośrednictwem przycisku **Zarządzaj zaplanowanymi skanami** znajdującego się w oknie [Opcje skanowania](#). W nowym oknie **Skan zaplanowany** widoczny będzie przegląd wszystkich zaplanowanych skanów:



W oknie tym można określić własne skanowania. Można tak zrobić przy użyciu przycisku **Dodaj harmonogram skanowania**, aby utworzyć nowy, własny harmonogram. Parametry zaplanowanego skanu można edytować (podobnie jak przy tworzeniu nowego harmonogramu) na trzech kartach:

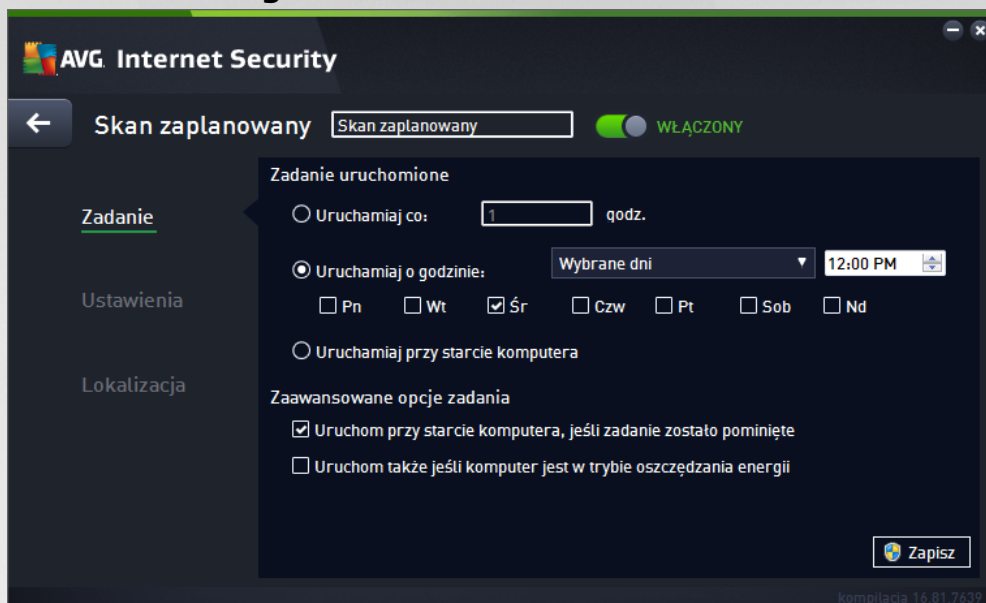
- [Harmonogram](#)
- [Ustawienia](#)
- [Lokalizacja](#)

Na każdej karcie można przełączyć przycisk „sygnalizacji świetlnej” , aby tymczasowo wyłączyć



zaplanowany test, i włączyć go ponownie, gdy znajdzie taka potrzeba.

9.4.1. Harmonogram



W górnej części karty **Harmonogram** znajduje się pole tekstowe umożliwiające nadanie nazwy tworzonemu harmonogramowi skanowania. Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości. Na przykład nazwy typu „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”.


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 danego dnia i o danej godzinie (*Uruchamiaj o określonych godzinach*), a także na skutek wystąpienia zdefiniowanego zdarzenia (*Uruchamiaj przy starcie komputera*).
- **Zaawansowane opcje zadania** — 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 w zasobniku systemowym](#) wyświetlone zostanie odpowiednie powiadomienie. Następnie pojawi się nowa [ikona AVG w zasobniku systemowym](#) (kolorowa, z migającym wiatelkiem), która informuje o uruchomieniu zaplanowanego skanowania. Kliknięcie ikony uruchomionego skanowania AVG prawym przyciskiem myszy pozwala wyświetlić menu kontekstowe, za pomocą którego można wstrzymać lub zatrzymać skanowanie, a także zmienić jego priorytet.

Przyciski dostępne w oknie

- **Zapisz** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do przeglądu [zaplanowanych skanów](#). Oznacza to, że aby skonfigurować parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.



-  — u yj zielonej strzałki w lewym górnym rogu okna dialogowego, aby powrócić do przeglądu [zaplanowanych skanów](#).

9.4.2. Ustawienia



W górnej części karty **Ustawienia** znajduje się pole tekstowe, w którym możesz podać nazwę aktualnie definiowanego zadania skanowania. Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości. Na przykład nazwy typu „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”.

Karta **Ustawienia** zawiera listę parametrów skanowania, które możesz włączyć/wyłączyć. **Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachować predefiniowaną konfigurację** :

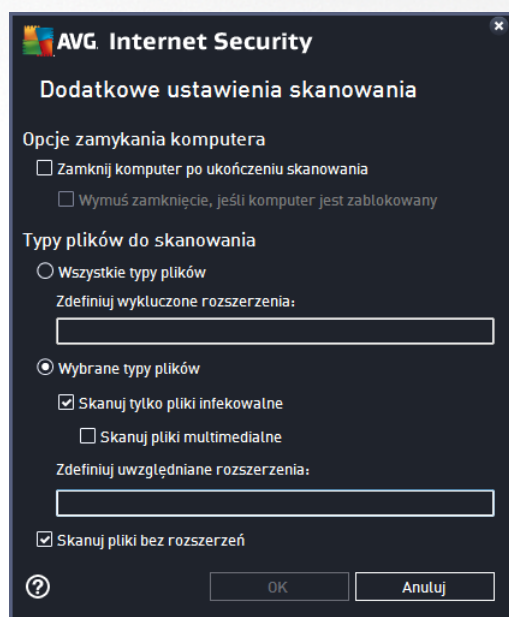
- **Naprawiaj / usuwaj infekcje wirusowe bez potwierdzenia** (domyślnie włączone): Jeśli podczas skanowania zostanie wykryty wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do [Przechowalni wirusów](#).
- **Zgłoś potencjalnie niechciane aplikacje i zagrożenia ze strony oprogramowania szpiegującego** (domyślnie włączone): zaznaczenie tego pola aktywuje skanowanie 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 zwiksza ona poziom ochrony komputera.
- **Zgłoś rozszerzony zestaw potencjalnie niechcianych aplikacji** (domyślnie wyłączone): zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego, czyli programów, które są zupełnie bezpieczne w momencie nabywania ich bezpośrednio od producenta, ale później mogą zostać wykorzystane do szkodliwych celów. To dodatkowy sposób na zapewnienie jeszcze większego bezpieczeństwa Twojemu komputerowi. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego tę domyślnie jest wyłączone.



- **Skanuj w poszukiwaniu ledz cych plików cookie** (domy Inie wyl czone): ten parametr okre la, czy wykrywane maj by pliki cookie; (u ywane w protokole HTTP do uwierzytelniania, ledzenia i przechowywania okre lonych informacji o u ytkownikach, np. ustawie witryn i zawarto ci koszyków w sklepach internetowych).
- **Skanuj wewn trz archiwów** (domy Inie wyl czone): ten parametr okre la, czy skanowanie ma obejmowa wszystkie pliki, nawet te znajduj ce si wewn trz archiwów, np. ZIP, RAR itd.
- **U yj heurystyki** (domy Inie wyl czone): analiza heurystyczna (dynamiczna emulacja kodu skanowanego obiektu w rodowisku maszyny wirtualnej) b dzie jedn z metod wykrywania wirusów w czasie skanowania.
- **Skanuj rodowisko systemu** (domy Inie wyl czone): skanowanie obejmie tak e obszary systemowe komputera.
- **Wl cz szczególowe skanowanie** (domy Inie wyl czone): w okre lonych sytuacjach (gdy zachodzi podejrzenie, e komputer jest zainfekowany) mo na zaznaczy t opcj , aby aktywowa dokladniejsze algorytmy skanowania. W celu uzyskania absolutnej pewno ci b d one skanowa nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Nale y pami ta , e ta metoda skanowania jest do czasochłonna.
- **Skanuj w poszukiwaniu programów typu rootkit** (domy Inie wyl czone): skan Anti-Rootkit sprawdza komputer pod k tem rootkitów, czyli programów i technik pozwalaj cych ukry dziełanie szkodliwego oprogramowania. Wykrycie programu typu rootkit nie jest równoznaczne z tym, e komputer jest zainfekowany. W niektórych przypadkach pewne sterowniki lub elementy zwykłych aplikacji mog omyłkowo zosta zaklasyfikowane jako programy typu rootkit.

Dodatkowe ustawienia skanowania

Link ten otwiera okno dialogowe **Dodatkowe ustawienia skanowania**, w którym mo na okre li nast puj ce parametry:





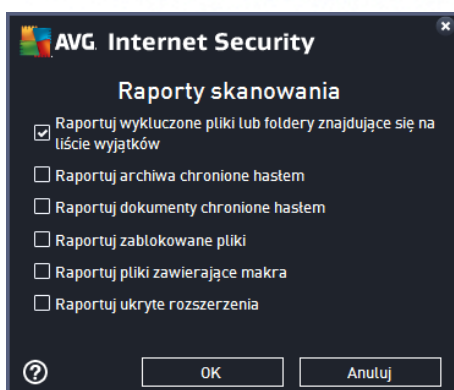
- **Opcje wyłączenia komputera** — określi, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie opcji (*Zamknij komputer po ukończeniu skanowania*) spowoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet wtedy, gdy w danej chwili jest on zablokowany (*Wymuś zamknięcie, jeśli komputer jest zablokowany*).
- **Typy plików do skanowania** — zdecyduj, które z poniższych elementów mają być skanowane:
 - **Wszystkie typy plików** z opcji zdefiniowania typów skanera przez wprowadzenie rozdzielonych przecinkami rozszerzeń, które nie powinny być skanowane.
 - **Wybrane typy plików** — skanowane będą tylko pliki, które mogą zostać zainfekowane (*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 skanowania 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 wybrać pozycję **Skanowanie plików bez rozszerzenia** — ta opcja jest domyślnie wyłączona i zaleca się, aby nie zmieniać tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane łącznie z innymi.

Określ, jak długo ma trwać skanowanie

W tej sekcji można szczegółowo określić czas skanowania w zależności od wykorzystania zasobów systemowych. Domyślna wartość to poziom *Zależy od użytkownika*, co oznacza automatycznie dobrane wykorzystanie zasobów. Jeśli skanowanie ma przebiegać szybciej, poziom wykorzystania zasobów wzrośnie, co może spowolnić działanie innych procesów i aplikacji (*tej opcji można używać wtedy, gdy komputer jest wyłączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przyspieszy jednocześnie czas skanowania.


Ustaw dodatkowe raporty skanowania

Kliknięcie linku **Ustaw dodatkowe raporty skanowania** powoduje otwarcie osobnego okna dialogowego **Raporty skanowania**, w którym można określić szczegółowo raporty, zaznaczając odpowiednie elementy:

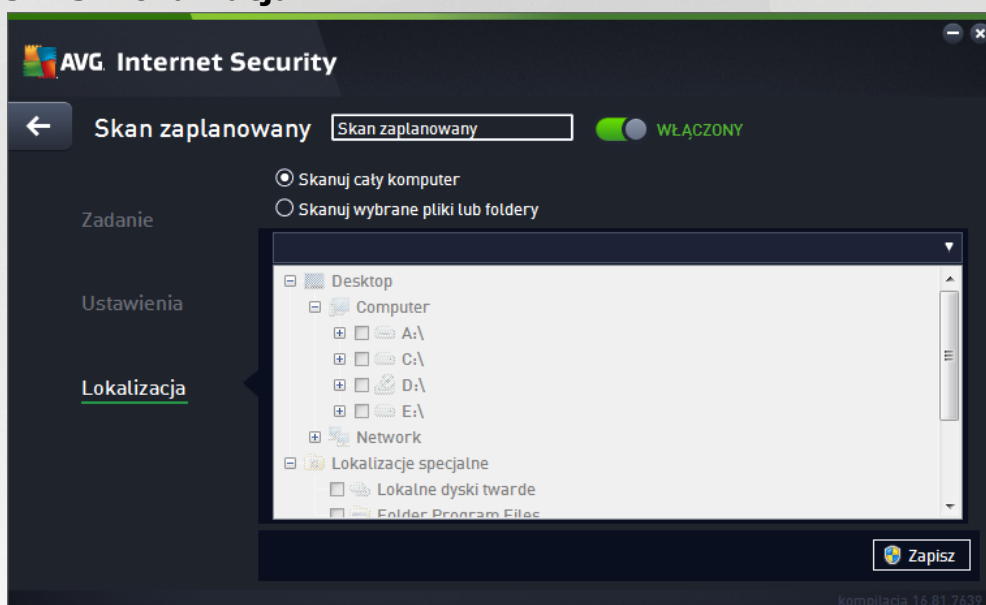




Przyciski dostępne w oknie

- **Zapisz** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do przeglądu [zaplanowanych skanów](#). Oznacza to, że aby skonfigurować parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
-  — umożliwia kliknięcie zielonej strzałki w lewym górnym rogu okna dialogowego, aby powrócić do przeglądu [zaplanowanych skanów](#).

9.4.3. Lokalizacja



Na karcie **Lokalizacja** można określić, czy planowane jest [skanowanie całego komputera](#), czy [skanowanie określonych plików lub folderów](#). Jeżeli zostanie wybrane skanowanie określonych plików lub folderów, w dolnej części tego okna dialogowego zostanie aktywowane drzewo katalogów, które umożliwia wybranie folderów do skanowania (*rozwijaj pozycje, klikaj c znak plusa, dopóki nie znajdziesz folderu, który ma zostać przeskanowany*). Zaznaczaj c więcej niż jedno pole wyboru, aby wybrać kilka folderów. Wybrane foldery zostaną wyświetlone w polu tekstowym u góry okna dialogowego, a historia wybranych skanów będzie przechowywana w rozwijanym menu do późniejszego użytku. Opcjonalnie można wprowadzić pełną ścieżkę do wybranego folderu (*w przypadku kilku ścieżek należy je rozdzielić średnikiem bez dodatkowej spacji*).

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

- **Lokalne dyski twarde** — wszystkie dyski twarde na tym komputerze
- **Folder Program Files**
 - C:\Program Files\
 - w wersji 64-bitowej C:\Program Files (x86)



- **Folder Moje dokumenty**

- w systemie Windows XP: C:\Documents and Settings\Default User\My Documents\
- w systemie Windows Vista/7: C:\Users\user\Documents\

- **Dokumenty udostępnione**


- w systemie Windows XP: C:\Documents and Settings\All Users\Documents\
- w systemie Windows Vista/7: C:\Users\Public\Documents\

- **Folder systemu Windows** — C:\Windows\

- **Inne**

- **Dysk systemowy** — dysk twardy, na którym zainstalowany jest system operacyjny (zazwyczaj C:)
- **Folder systemowy** — C:\Windows\System32\
- **Folder plików tymczasowych** — C:\Documents and Settings\User\Local\ (Windows XP); lub C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- **Folder tymczasowych plików internetowych** — C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); lub C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Przyciski dostępne w oknie

- **Zapisz** — powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do przeglądu [zaplanowanych skanów](#). Oznacza to, że aby skonfigurować parametry testów na wszystkich kartach, należy kliknąć ten przycisk po zakończeniu wprowadzania ustawień.
-  — użyj zielonej strzałki w lewym górnym rogu okna dialogowego, aby powrócić do przeglądu [zaplanowanych skanów](#).



9.5. Wyniki skanowania

Nazwa	Czas rozpocz...	Czas zakończ...	Testowane ob...	Infekcje	Wysol
Skan Anti-Rootkit	6/13/2016, 10:4	6/13/2016, 10:4	23674	0	0
Skanuj cały komputer	6/13/2016, 10:4	6/13/2016, 10:4	4822	0	0

Okno **Przegląd wyników skanowania** wyświetla listę wszystkich przeprowadzonych dotychczas skanów. Tabela podaje następujące informacje o każdym wyniku skanowania:

- **Ikona** — pierwsza kolumna wyświetla ikonę informacyjną podając status skanu:
 - Nie znaleziono infekcji, skanowanie zakończone
 - Nie znaleziono infekcji, skanowanie przerwane przed ukończeniem
 - Znaleziono infekcje, lecz nie wyleczono ich — skanowanie zakończone
 - Znaleziono infekcje, lecz nie wyleczono ich — skanowanie przerwane przed ukończeniem
 - Znaleziono infekcje — wszystkie zostały wyleczone lub usunięte, skanowanie zakończone
 - Znaleziono infekcje — wszystkie zostały wyleczone lub usunięte, skanowanie przerwane przed ukończeniem
- **Nazwa** — ta kolumna zawiera nazwę skanu. Jest to jeden z dwóch [predefiniowanych skanów](#) lub Twój własny [skan zaplanowany](#).
- **Czas rozpoczęcia** — podaje dokładną datę i godzinę uruchomienia skanowania.
- **Czas zakończenia** — podaje dokładną datę i godzinę zakończenia, wstrzymania lub przerwania skanowania.
- **Przetestowane obiekty** — podaje liczbę wszystkich przeskanowanych obiektów.
- **Infekcje** — podaje liczbę usuniętych/wszystkich znalezionych infekcji.
- **Wysoki / redni / Niski** — trzy kolejne kolumny podają liczbę infekcji o wysokim, średnim i niskim




poziomie zagrożenia.

- **Rootkity** — podaje całkowitą liczbę [rootkitów](#) znalezionych podczas skanowania.

Elementy okna

Wyświetl szczegóły — kliknij ten przycisk, aby zobaczyć [szczegóły wybranego skanu](#) (wyróżnionego w tabeli powyżej).


Usuń wyniki — Kliknij ten przycisk, aby usunąć wyniki wybranego skanowania z tabeli.


 — użyj zielonej strzałki w prawym górnym rogu okna, aby wrócić do [głównego interfejsu użytkownika](#) z przeglądem składników.


9.6. Szczegóły wyników skanowania

Aby otworzyć przegląd szczegółowych informacji o wybranym wyniku skanowania, kliknij przycisk **Wyświetl szczegóły** widoczny w oknie [Przejdź do wyników skanowania](#). Nastąpi przekierowanie do tego samego interfejsu opisującego szczegóły wybranego wyniku skanowania. Informacje są rozmieszczone na trzech kartach:

- **Podsumowanie** — podstawowe informacje o skanie: Czy został uruchomiony pomysłnie, czy wykryto zagrożenia i jakie podjęto działania.
- **Szczegóły** — wszystkie informacje o skanowaniu z uwzględnieniem szczegółów na temat każdego znalezionej zagrożenia. Opcja Eksportuj przegląd do pliku umożliwia zapisanie go w pliku csv.
- **Detekcje** — ta karta jest wyświetlana tylko wtedy, gdy podczas skanowania zostały wykryte zagrożenia. Zawiera ona szczegóły dotyczące zagrożenia:

 **Poziom informacyjny:** informacje i ostrzeżenia; nie są to faktyczne zagrożenia. Zazwyczaj są to dokumenty zawierające makra, dokumenty lub archiwa chronione hasłem, zablokowane pliki, itd.

 **redni poziom zagrożenia:** zazwyczaj są to potencjalnie niechciane aplikacje (np. oprogramowanie reklamowe) lub ledzące pliki cookie

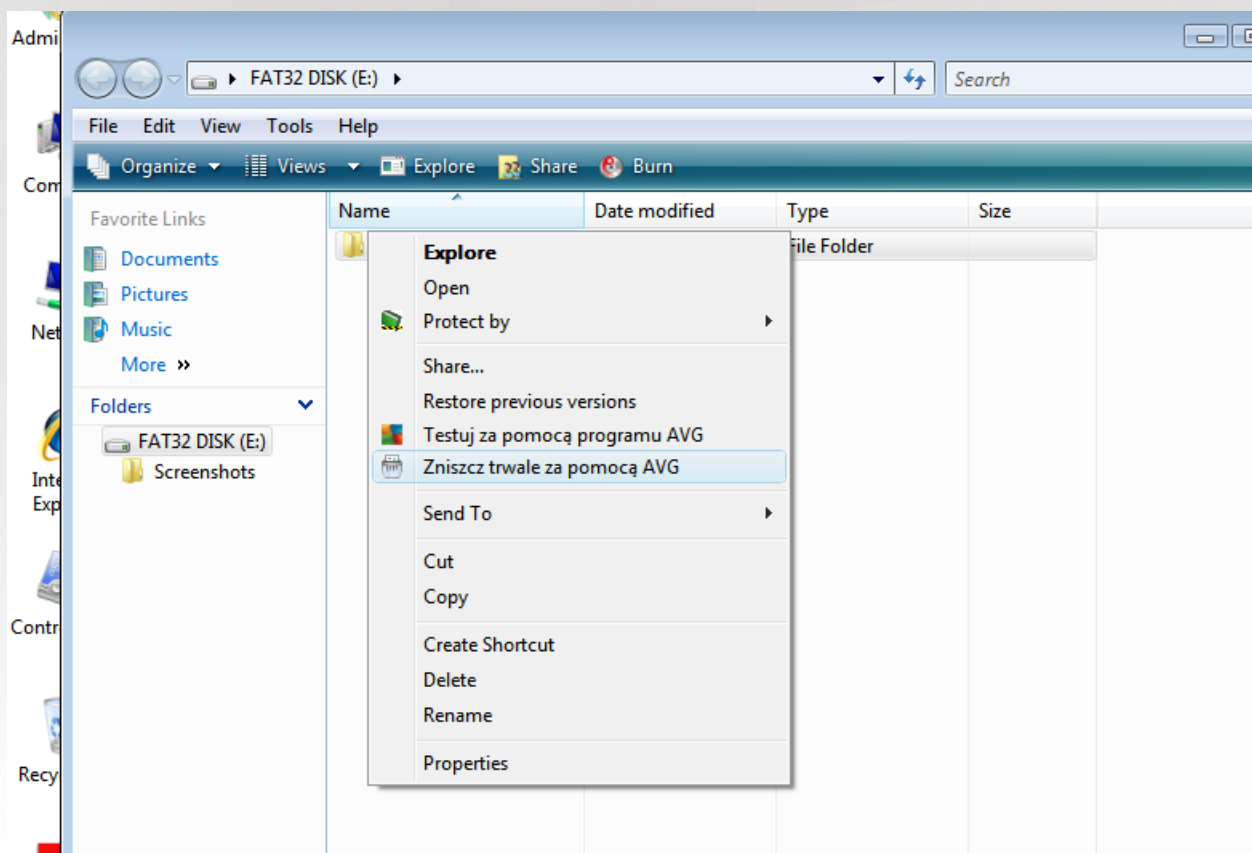
 **Wysoki poziom zagrożenia:** poważne zagrożenia, takie jak wirusy, konie trojańskie, exploity itp. Dotyczy to również obiektów wykrytych przez heurystyczne metody detekcji, czyli zagrożenia, które nie są opisane jeszcze w naszej bazie wirusów.



10. AVG File Shredder

AVG File Shredder służy do usuwania plików w całkowicie bezpieczny sposób, tzn. bez możliwości ich odzyskania nawet za pomocą zaawansowanego oprogramowania przeznaczonego do tych celów.

Aby zniszczyć plik lub folder, kliknij go prawym przyciskiem myszy w menedżerze plików (*takim jak Eksplorator Windows, Total Commander itp.*) i wybierz z menu kontekstowego polecenie **Zniszcz trwale za pomocą AVG**. Pliki z kosza również mogą zostać zniszczone. Jeżeli znajdujący się w danej lokalizacji plik (np. na dysku CD) nie może zostać skutecznie zniszczony, zostaniesz o tym powiadomiony, a jedynie opcja z menu kontekstowego w ogóle nie będzie dostępna.



Pamiętaj: Po zniszczeniu pliku nie można go odzyskać w żaden sposób.



11. Przechowalnia wirusów

Przechowalnia wirusów to bezpieczne środowisko przeznaczone do zarządzania podejrzanymi/zainfekowanymi obiektami, które zostały wykryte podczas testów przeprowadzanych przez program AVG. Po wykryciu zainfekowanego obiektu podczas skanowania i w przypadku braku możliwości automatycznego wyleczenia takiego obiektu przez program AVG użytkownik zostanie poproszony o dokonanie wyboru operacji, które mają zostać wykonane na podejrzanym obiekcie. Zalecanym rozwiązaniem jest przeniesienie obiektu do **Przechowalni wirusów** i tam podjąć dalsze działania. Głównym zadaniem **Przechowalni wirusów** jest przechowywanie wszelkich usuniętych plików przez określony czas, aby umożliwić pewność, że nie były one potrzebne. Jeśli brak danego pliku powoduje problemy, można go wyśłać wraz z pytaniem do analizy lub przywrócić do pierwotnej lokalizacji.

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

- **Data dodania** — podaje datę i godzinę wykrycia podejrzanego pliku i przeniesienia go do Przechowalni wirusów.
- **Zagrożenie** — w przypadku zainstalowania składnika [To samo](#) w ramach oprogramowania **AVG Internet Security** zostanie wyświetlony graficzny identyfikator poziomu zagrożenia: od niegroźnego (trzy zielone kropki) do bardzo niebezpiecznego (trzy czerwone kropki). Podane zostaną również informacje na temat typu infekcji i jej pierwotnej lokalizacji. Link *Więcej informacji* prowadzi do strony ze szczegółowymi informacjami na temat wykrytego zagrożenia w [internetowej encyklopedii wirusów](#).
- **ródło** — określa, który składnik **AVG Internet Security** wykrył dane zagrożenie.
- **Powiadomienia** — w bardzo rzadkich przypadkach w tej kolumnie pojawią się szczegółowe komentarze dotyczące wykrytego zagrożenia.

Przyciski kontrolne

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

- **Przywróć** — przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- **Przywróć jako** — przenosi zainfekowany plik do wybranego folderu.
- **Wyślij do analizy** — ten przycisk staje się aktywny dopiero po zaznaczeniu obiektu na liście wykrytych obiektów powyżej. W takim przypadku użytkownik może wysłać wykryty obiekt do laboratoriów antywirusowych AVG w celu jego dalszej szczegółowej analizy. Należy pamiętać, że ta funkcja powinna przede wszystkim służyć do wysyłania fałszywych wykryć, czyli plików, które zostały wykryte przez oprogramowanie AVG jako zainfekowane lub podejrzone, ale wydają się być nieszkodliwe.
- **Szczegóły** — aby uzyskać szczegółowe informacje o konkretnym zagrożeniu znajdującym się w **Przechowalni wirusów**, podświetl wybraną pozycję na liście i kliknij przycisk **Szczegóły**, który otworzy nowe okno dialogowe z opisem wykrytego zagrożenia.
- **Usu** — całkowicie i nieodwracalnie usuwa zainfekowany plik z **Przechowalni wirusów**.
- **Opróżnij przechowalnię** — usuwa bezpowrotnie całą zawartość **Przechowalni wirusów**. Usunięcie plików z **Przechowalni wirusów** oznacza całkowite i nieodwracalne usunięcie ich z dysku (nie s



one przenoszone do kosza).

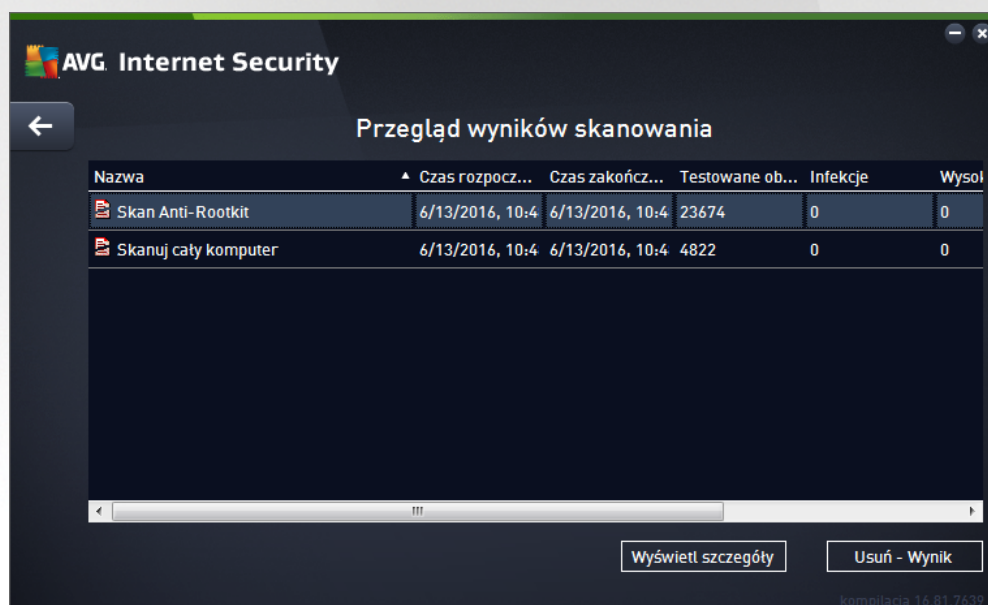


12. Historia

Sekcja **Historia** zawiera informacje o wszystkich przeszłych zdarzeniach (*takich jak aktualizacje, skany, detekcje itd.*) oraz raporty na temat tych zdarzeń. Sekcja ta dostępna jest z poziomu [głównego interfejsu użytkownika](#) przez menu **Opcje / Historia**. Historia wszystkich zapisanych zdarzeń podzielona jest na następujące części:

- [Wyniki skanowania](#)
- [Wyniki narzadzia Ochrona rezydentna](#)
- [Wyniki narzadzia Ochrona poczty email](#)
- [Wyniki narzadzia Ochrona sieci](#)
- [Historia zdarzeń](#)
- [Dziennik Zapory](#)

12.1. Wyniki skanowania




Okno **Przegląd wyników skanowania** jest dostępne za pośrednictwem menu **Opcje / Historia / Wyniki skanowania** w górnej części nawigacyjnej głównego okna **AVG Internet Security**. Okno to zawiera listę wcześniejszych skanowań oraz informacje o ich wynikach:

- **Nazwa** — oznaczenie skanowania; może to być nazwa jednego ze [wstępnie zdefiniowanych skanowań](#) 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 ikona może być widoczna w całości lub „przerwana” — jeżeli ikona jest cała, skanowanie zostało prawidłowo ukończone; 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 skanowania
- **Czas zakończenia** — data i godzina zakończenia skanowania
- **Przetestowano obiektów** — liczba obiektów sprawdzonych podczas skanowania
- **Infekcje** — liczba infekcji wirusowych, które zostały wykryte/usunięte
- **Wysoki / niski** — te kolumny podają liczbę usuniętych/wszystkich infekcji o wysokim i niskim poziomie zagrożenia.
- **Informacja** — informacje dotyczące przebiegu i wyniku skanowania (zwykle o jego zakończeniu lub przerwaniu).
- **Rootkity** — liczba wykrytych [rootkitów](#)

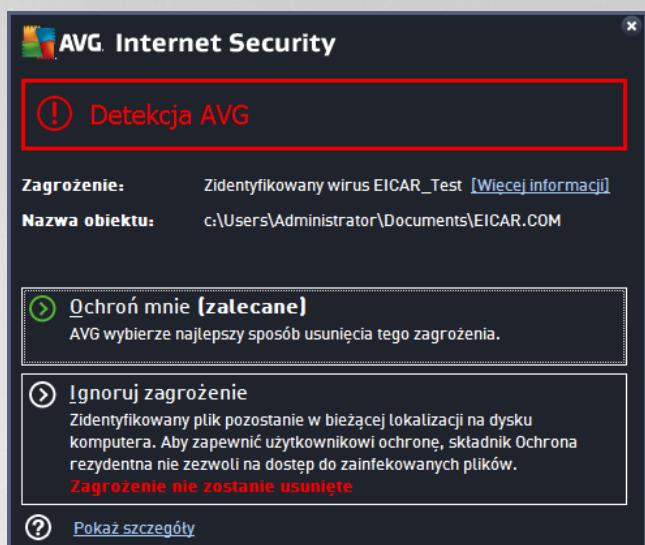
Przyciski kontrolne

Przyciski kontrolne dostępne w oknie **Przebieg 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
- **Usuń wynik** — kliknięcie tego przycisku powoduje usunięcie wybranej pozycji z przeglądu wyników skanowania
-  — aby wrócić do domowego [okna głównego AVG](#) (przebiegu składników), użyj strzałki znajdującej się w lewym górnym rogu tego okna

12.2. Wyniki narzędzia Ochrona rezydentna

Usługa **Ochrona rezydentna** jest częścią składnika **Komputer** odpowiedzialną za skanowanie plików podczas ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego ostrzeżenia:

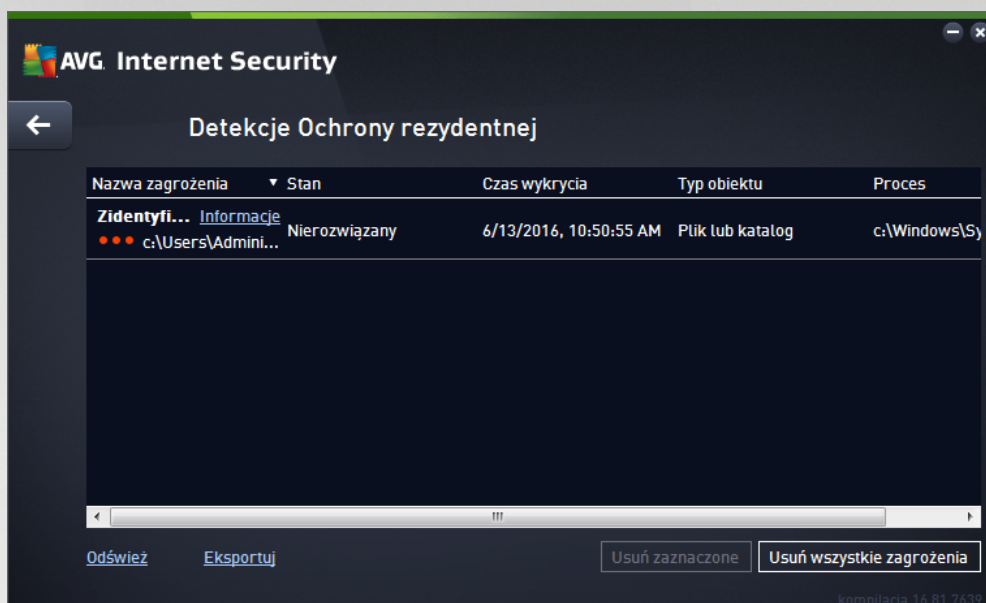


To okno ostrzegawcze podaje informacje o wykrytym obiekcie, który został uznany za infekcję (*Zagrożenie*), a także kilka opisowych faktów dotyczących samej infekcji (*Opis*). Link *Więcej informacji* prowadzi do strony ze szczegółowymi informacjami na temat wykrytego zagrożenia w [internetowej encyklopedii wirusów](#) (jeśli jest dostępna). To samo okno dialogowe zawiera także przegląd dostępnych rozwiązań umożliwiających nieszkodliwienie zagrożenia. Jedną z alternatyw będzie oznaczona jako zalecana. **Ochroni mnie (zalecane). O ile to możliwe, powiniene zawsze trzymać się tego wyboru!**

Uwaga: Może się zdarzyć, że rozmiar wykrytego obiektu przekracza limit wolnego miejsca w Przechowalni wirusów. W takiej sytuacji w przypadku próby przeniesienia zainfekowanego obiektu do Przechowalni wirusów zostanie wysłany komunikat informujący o tym problemie. Istnieje możliwość zmiany rozmiaru Przechowalni wirusów. Można to zrobić, określając dostępną procent rzeczywistego rozmiaru dysku twardego. Aby zwiększyć rozmiar Przechowalni wirusów, przejdź do okna dialogowego [Przechowalnia wirusów](#) w sekcji [Zaawansowane ustawienia AVG](#), korzystając z opcji *Ogranicz rozmiar Przechowalni wirusów*.

W dolnej części tego okna znajduje się link **Pokaż szczegóły**. Kliknij go, aby otworzyć nowe okno zawierające szczegółowe informacje o procesie działającym podczas wykrycia infekcji oraz dane identyfikacyjne tego procesu.

Lista wszystkich detekcji Ochrony rezydentnej dostępna jest w oknie **Zagrożenia wykryte przez Ochronę rezydentną**. To okno dostępne jest przez menu **Opcje / Historia / Zagrożenia wykryte przez Ochronę rezydentną** w górnej części nawigacyjnej [głównego okna AVG Internet Security](#). Okno to zawiera przegląd obiektów wykrytych i ocenionych przez Ochronę rezydentną jako niebezpieczne, które następnie wyleczono lub przeniesiono do [Przechowalni wirusów](#).



Dla każdego wykrytego obiektu podawane są następujące informacje:

- **Nazwa zagrożenia** — opis (czasem także nazwa) wykrytego obiektu oraz jego lokalizacja. Link *Wicej informacji* prowadzi do strony ze szczegółowymi informacjami na temat wykrytego zagrożenia w [internetowej encyklopedii wirusów](#).
- **Status** — działanie podjęte w stosunku do wykrytego obiektu
- **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)

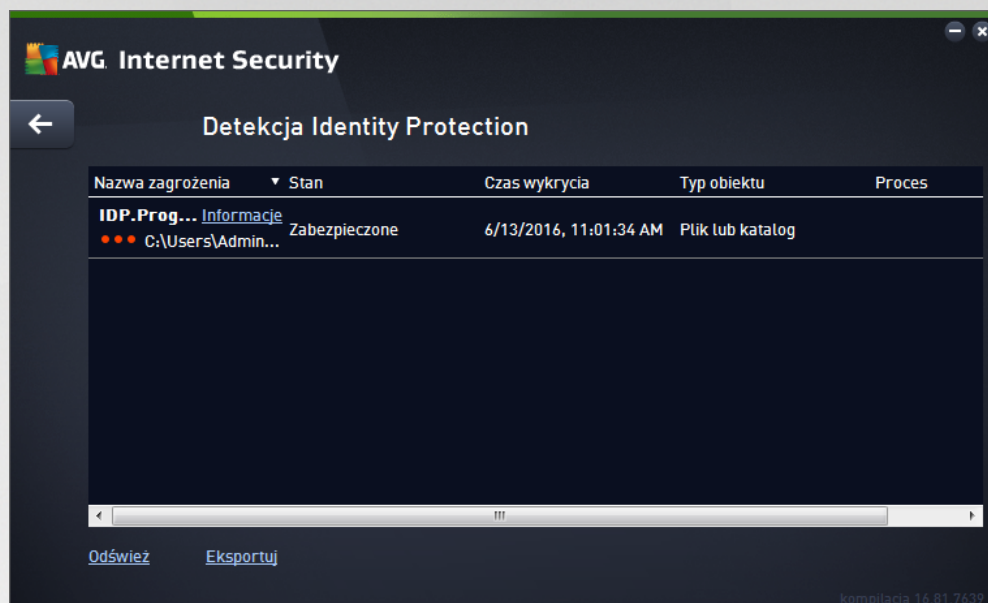
Przyciski kontrolne

- **Odśwież** — pozwala zaktualizować list obiektów wykrytych przez składnik **Ochrona Sieci**
- **Eksportuj** — eksportuje całą listę wykrytych obiektów do pliku
- **Usuń zaznaczone** — umożliwia wybranie przycisku po zaznaczeniu konkretnych pozycji na liście, aby je usunąć.
- **Usuń wszystkie zagrożenia** — umożliwia wybranie przycisku, aby usunąć wszystkie zagrożenia widoczne w tym oknie
- **←** — aby wrócić do domowego [okna głównego AVG](#) (przejrzenia składników), użyj strzałki znajdującej się w lewym górnym rogu tego okna



12.3. Wyniki narzędzia Identity Protection

Okno *Wyniki narz dzia Identity Protection* dostępne jest z poziomu menu *Opcje / Historia / Wyniki narz dzia Identity Protection* znajdującego się w górnej części nawigacyjnej głównego okna **AVG Internet Security**.



To okno dialogowe zawiera listę wszystkich obiektów wykrytych przez składnik [Identity Protection](#). Dla każdego wykrytego obiektu podawane są następujące informacje:

- **Nazwa zagrożenia** — opis (czasem także nazwa) wykrytego obiektu oraz jego lokalizacja. Link *Więcej informacji* prowadzi do strony ze szczegółowymi informacjami na temat wykrytego zagrożenia w [internetowej encyklopedii wirusów](#).
- **Status** — działanie podjęte w stosunku do wykrytego obiektu
- **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 dialogowego, pod listą znajdują się informacje na temat łącznej liczby wykrytych obiektów, które zostały wymienione powyżej. Ponadto, można wyeksportować całą listę obiektów do pliku, (**Eksportuj listę do pliku**) lub usunąć wszystkie jej pozycje (**Opróżnij listę**).

Przyciski kontrolne

W interfejsie składnika *Wyniki Identity Protection* dostępne są następujące przyciski sterujące:

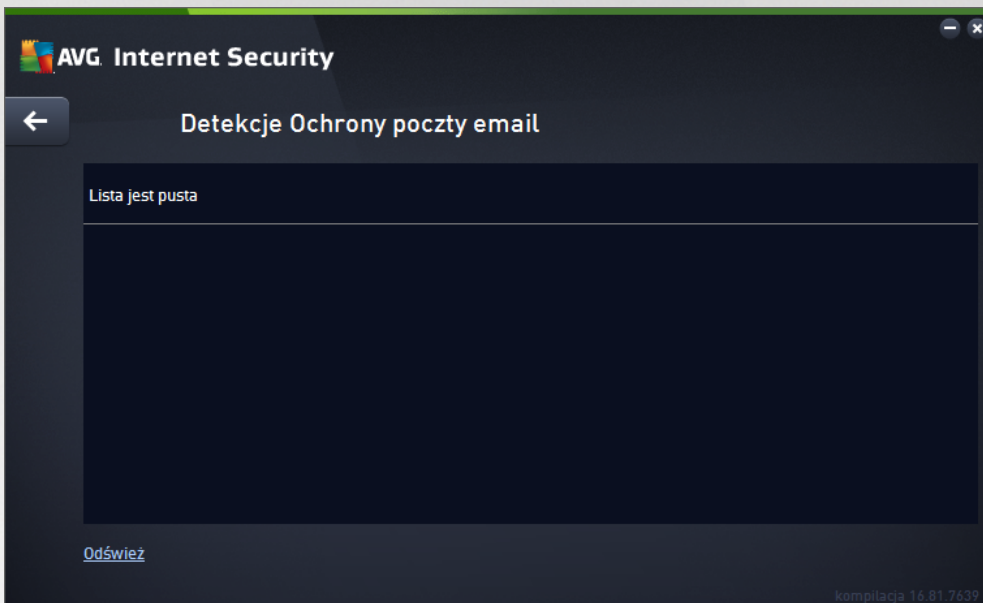
- **Odśwież listę** — aktualizuje listę wykrytych zagrożeń



-  — aby wrócić do domowego [okna głównego AVG](#) (przejdź do składników), użyj strzałki znajdującej się w lewym górnym rogu tego okna

12.4. Wyniki narzędzia Ochrona poczty email

Okno **Wyniki narzędzia Ochrona poczty e-mail** dostępne jest z poziomu menu **Opcje / Historia / Wyniki narzędzia Ochrona poczty e-mail** znajdującego się w górnej części nawigacyjnej głównego okna **AVG Internet Security**.



To okno dialogowe zawiera listę wszystkich obiektów wykrytych przez [Skaner poczty e-mail](#). Dla każdego wykrytego obiektu podawane są następujące informacje:

- **Nazwa detekcji** — opis (a czasem także nazwa) wykrytego obiektu oraz jego źródło
- **Wynik** — działanie podjęte w stosunku do wykrytego obiektu
- **Czas wykrycia** — data i godzina wykrycia podejrzanego obiektu
- **Typ obiektu** — typ wykrytego obiektu
- **Proces** — akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co umożliwiło jego wykrycie)


U dołu okna dialogowego, pod listą znajdują się informacje na temat łącznej liczby wykrytych obiektów, które zostały wymienione powyżej. Ponadto, można wyeksportować całą listę obiektów do pliku, (**Eksportuj listę do pliku**) lub usunąć wszystkie jej pozycje (**Opróżnij listę**).

Przyciski kontrolne

W interfejsie składnika **Skaner poczty Email** dostępne są następujące przyciski sterujące:

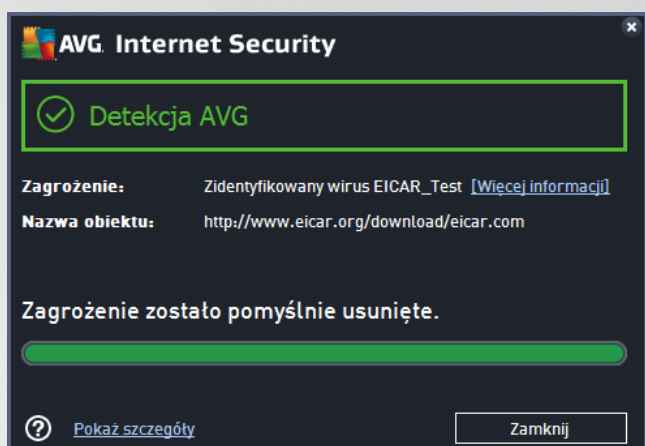
- **Odśwież listę** — aktualizuje listę wykrytych zagrożeń



-  — aby wrócić do domowego okna głównego AVG (przejdź do składników), użyj strzałki znajdującej się w lewym górnym rogu tego okna

12.5. Wyniki narzędzia Ochrona Sieci

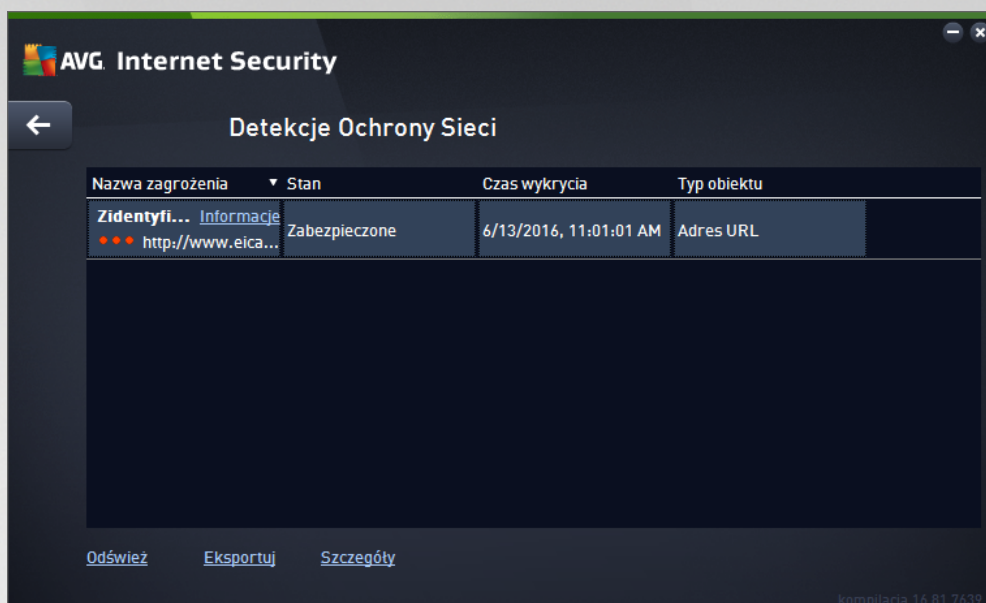
Ochrona Sieci skanuje zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików), jeszcze zanim zostaną wyświetlone w przeglądarce lub pobrane na dysk twardy. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego okna:



To okno ostrzegawcze podaje informacje o wykrytym obiekcie, który został uznany za infekcję (*Zagrożenie*), a także kilka opisowych faktów dotyczących samej infekcji (*Nazwa obiektu*). Link *Więcej informacji* przeniesie Cię do [encyklopedii wirusów online](http://www.eicar.org), która może udzielić szczegółowych informacji o wykrytej infekcji, o ile są one znane. W oknie dialogowym dostępne są następujące przyciski sterujące:

- **Pokaż szczegóły** — kliknięcie tego linku spowoduje otwarcie nowego okna dialogowego, w którym można znaleźć informacje o procesie uruchomionym podczas wykrycia infekcji oraz jego identyfikator.
- **Zamknij** — kliknięcie tego przycisku spowoduje zamknięcie okna ostrzeżenia.

Podejrzana strona nie zostanie otwarta, a wykrycie zagrożenia zostanie odnotowane w **Zagrożeniach wykrytych przez Ochronę Sieci**. Przegląd wykrytych zagrożeń jest dostępny przez menu **Opcje / Historia / Zagrożenia wykryte przez Ochronę rezydentną** w górnej części nawigacyjnej głównego okna **AVG Internet Security**.



Dla każdego wykrytego obiektu podawane są następujące informacje:

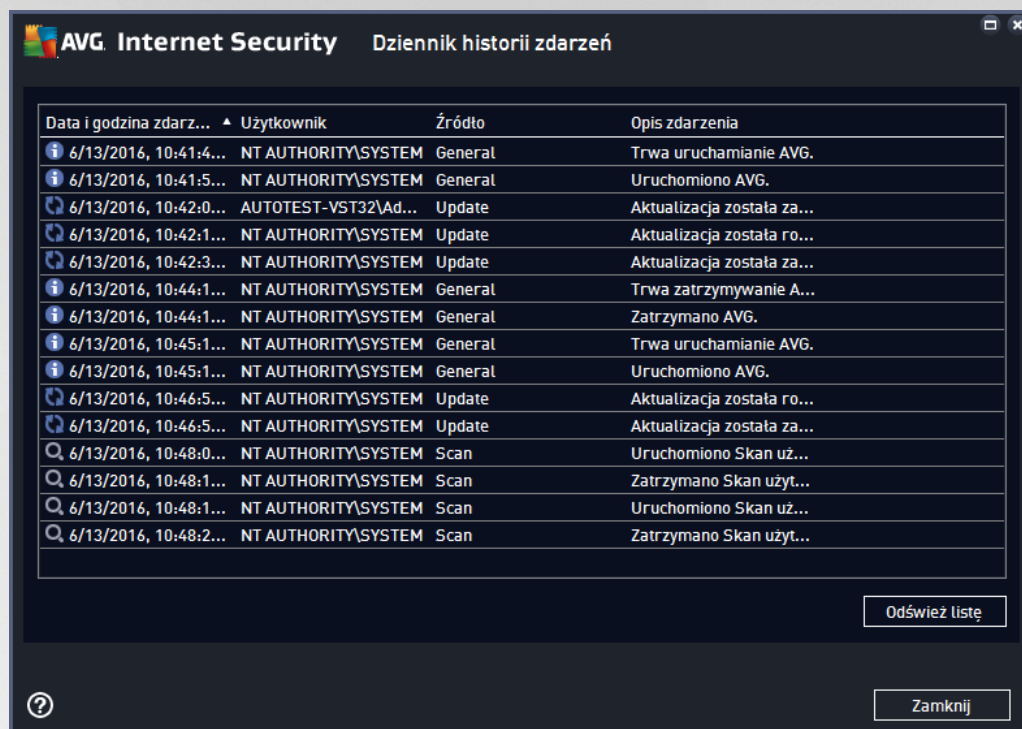
- **Nazwa zagrożenia** — opis (czasem także nazwa) wykrytego obiektu i jego źródło (strona internetowa). Link *Więcej informacji* prowadzi do strony ze szczegółowymi informacjami na temat wykrytego zagrożenia w [internetowej encyklopedii wirusów](#).
- **Status** — działanie podjęte w stosunku do wykrytego obiektu
- **Czas wykrycia** — data i godzina wykrycia i zablokowania zagrożenia
- **Typ obiektu** — typ wykrytego obiektu

Przyciski kontrolne

- **Odśwież** — pozwala zaktualizować listę obiektów wykrytych przez składnik **Ochrona Sieci**
- **Eksportuj** — eksportuje całą listę wykrytych obiektów do pliku
- **←** — aby wrócić do domowego [okna głównego AVG](#) (przejdź do składników), użyj strzałki znajdującej się w lewym górnym rogu tego okna



12.6. Historia zdarzeń



Okno **Historia zdarzeń** dostępne jest przez menu **Opcje / Historia / Historia zdarzeń** w górnym wierszu nawigacji głównego okna programu **AVG Internet Security**. Okno to zawiera podsumowanie najważniejszych zdarzeń, które wystąpiły w czasie działania oprogramowania **AVG Internet Security**. Okno to zawiera wpisy na temat następujących typów zdarzeń: informacje o aktualizacjach systemu AVG; informacje o rozpoczęciu, zakończeniu lub zatrzymaniu skanowania (*w tym czasie automatyczne testy*); informacje o zdarzeniach powiązanych z detekcjami wirusów (*przez Ochronę rezydentną lub skanowanie*) wraz z miejscem ich wystąpienia; a także o innych ważnych zdarzeniach.

Dla każdego zdarzenia wyświetlane są następujące informacje:

- **Data i godzina zdarzenia** określa dokładną datę i godzinę wystąpienia zdarzenia.
- **Użytkownik** określa nazwę użytkownika, który był zalogowany w czasie wystąpienia zdarzenia.
- **Źródło** zawiera informacje o składniku źródłowym lub innej części systemu AVG, która wywołała dane zdarzenie.
- **Opis zdarzenia** przedstawia krótkie podsumowanie zdarzenia.

Przyciski kontrolne

- **Odśwież listę** — powoduje odświeżenie całej listy zdarzeń
- **Zamknij** — kliknij ten przycisk, aby wrócić do głównego okna programu **AVG Internet Security**

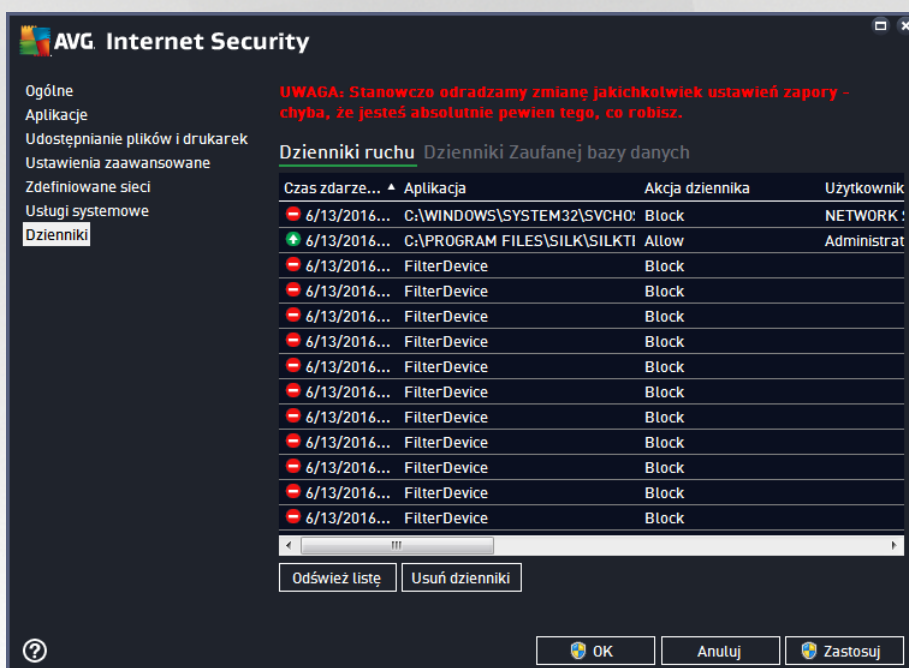


12.7. Dziennik Zapory

To okno konfiguracyjne przeznaczone jest dla ekspertów. Nie zalecamy wprowadzania w nim żadnych zmian bez absolutnej pewności.

Okno dialogowe **Dzienniki** umożliwia przeglądanie listy wszystkich zarejestrowanych działań Zapory, ze szczegółowym opisem odpowiednich parametrów na dwóch kartach:

- **Dzienniki ruchu** — ta karta wyświetla informacje o aktywności wszystkich aplikacji, które próbowały połączyć się z siecią. Każda pozycja zawiera informacje o czasie wystąpienia zdarzenia, nazwie aplikacji, zarejestrowanej akcji, nazwie użytkownika, numerze PID, kierunku ruchu, typie protokołu, numerze portu zdalnego i lokalnego, a także o zdalnym i lokalnym adresie IP.



- **Dzienniki Trusted Database** — *Trusted Database* to wewnętrzna baza danych systemu AVG, która zbiera informacje na temat certyfikowanych i zaufanych aplikacji, dla których komunikacja 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 zezwolić na komunikację sieciową. Najpierw program AVG przeszukuje bazę *Trusted Database*. Jeśli aplikacja znajduje się na liście, dostęp do sieci zostanie jej automatycznie umożliwiony. Dopiero wtedy i pod warunkiem, że w naszej bazie danych nie ma żadnych informacji na temat tej aplikacji, zostanie wyświetlone okno dialogowe z pytaniem, czy dostęp do sieci powinien zostać odblokowany.

Przyciski kontrolne

- **Od wie list** — wszystkie zarejestrowane parametry można uporządkować według wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) — wystarczy kliknąć odpowiedni nagłówek kolumny. Użyj przycisku **Od wie list**, aby zaktualizować wyświetlane informacje.
- **Usu dzienniki** — pozwala usunąć wszystkie wpisy z wykresu.



13. Aktualizacje systemu AVG

Bez regularnych aktualizacji odpowiednie oprogramowanie zabezpieczające nie może zapewnić realnej ochrony przed różnymi typami zagrożeń. Twórcy wirusów nieustannie szukają nowych luk w programach i systemach operacyjnych, które mogliby wykorzystać. Nowe wirusy, szkodliwe oprogramowanie i metody ataków pojawiają się każdego dnia. Z tego powodu dostawcy oprogramowania na bieżąco wydają aktualizacje i poprawki zabezpieczeń, które mają usuwać wykryte luki. Biorąc pod uwagę liczbę nowo powstających zagrożeń internetowych oraz prędkość, z jaką się rozprzestrzeniają, regularna aktualizacja oprogramowania **AVG Internet Security** jest absolutnie niezbędna. Najlepszym rozwiązaniem jest w tym wypadku pozostawienie domyślnych ustawień automatycznej aktualizacji. Przypominamy, że jeśli baza wirusów lokalnego oprogramowania **AVG Internet Security** jest nieaktualna, wykrycie najnowszych zagrożeń może być niemożliwe!

Regularne aktualizacje oprogramowania AVG są kluczowe dla bezpieczeństwa! Jeśli to możliwe, definicje wirusów należy pobierać codziennie. Mniej istotne aktualizacje programu można pobierać co tydzień.

Aby zapewnić maksymalną dostępną ochronę, produkt **AVG Internet Security** domyślnie sprawdza dostępność nowych aktualizacji bazy wirusów co dwie godziny. Aktualizacje systemu AVG nie są publikowane zgodnie z jakimkolwiek harmonogramem – powstają jako reakcja na pojawiające się zagrożenia. Sprawdzanie dostępności aktualizacji jest kluczowym czynnikiem zapewniającym skuteczność bazy wirusów.

Jeśli chcesz natychmiast sprawdzić dostępność nowych plików aktualizacji, użyj szybkiego linku [Aktualizuj teraz](#) dostępnego w głównym interfejsie użytkownika. Link jest widoczny przez cały czas w każdym oknie dialogowym [interfejsu użytkownika](#). Po uruchomieniu tego procesu program AVG sprawdza, czy są dostępne nowe pliki aktualizacji. Jeśli tak, program **AVG Internet Security** rozpocznie ich pobieranie i uruchomi proces aktualizacji. Informacje o wynikach aktualizacji zostaną wyświetlone w wysuwanym oknie nad ikoną AVG w zasobniku systemowym.

Jeśli chcesz zmniejszyć liczbę uruchamianych procesów aktualizacji, możesz ustalić swój własny harmonogram. Stanowczo zalecamy jednak **uruchamianie aktualizacji minimum raz dziennie!** Wspomniana konfiguracja dostępna jest w sekcji [Ustawienia zaawansowane/Harmonogramy](#) w następujących oknach dialogowych:

- [Harmonogram aktualizacji definicji](#)
- [Harmonogram aktualizacji składnika Anti-Spam](#)



14. Często zadawane pytania i pomoc techniczna

Jeśli masz jakiegokolwiek pytania natury technicznej lub handlowej (dotyczące produktów **AVG Internet Security**), istnieje kilka sposobów uzyskania pomocy. Wybierz jedną z poniższych opcji:

- **Uzyskaj Pomoc techniczną** : Bezpośrednio z poziomu aplikacji AVG możesz przejść na dedykowaną stronę pomocy AVG (<http://www.avg.com/>). Wybierz **Pomoc / Uzyskaj Pomoc techniczną** z głównego menu, by zostać przeniesionym na stronę internetową oferującą dostępne formy pomocy. Więcej informacji znajdziesz na wspomnianej wyżej stronie internetowej.
- **Pomoc techniczna (link w menu głównym)**: Menu aplikacji AVG (w górnej części interfejsu użytkownika) zawiera link **Pomoc techniczna**, który otwiera nowe okno, zawierające wszystkie dane potrzebne przy poszukiwaniu pomocy. Znajdziesz tam podstawowe informacje o zainstalowanym systemie AVG (*wersja programu i bazy wirusów*), szczegóły licencji oraz listę przydatnych linków.
- **Rozwiązywanie problemów przy użyciu plików pomocy**: Nowa sekcja **Rozwiązywanie problemów** dostępna jest bezpośrednio w plikach pomocy **AVG Internet Security** (aby otworzyć pomoc, naciśnij klawisz **F1** w dowolnym oknie aplikacji). Zawiera ona listę najczęściej występujących sytuacji, w których użytkownik może poszukiwać pomocy. Wybierz sytuację, która najlepiej opisuje Twój problem, aby otworzyć okno ze szczegółowymi instrukcjami jego rozwiązania.
- **Centrum pomocy technicznej na stronie AVG**: Możesz również poszukać rozwiązania problemu na stronie AVG (<http://www.avg.com/>). W sekcji **Pomoc techniczna** znajduje się tematyczny spis problemów technicznych i związanych ze sprzedażą, uporządkowana sekcja z często zadawanymi pytaniami oraz wszystkie dostępne dane kontaktowe.
- **AVG ThreatLabs**: Specjalna strona AVG (<http://www.avg.com/about-viruses>) poświęcona problemom z wirusami, zapewniająca uporządkowany przegląd informacji związanych z zagrożeniami w sieci. Znajdziesz tam również instrukcje dotyczące usuwania wirusów i oprogramowania szpiegującego, a także porady dotyczące bezpieczeństwa.
- **Forum dyskusyjne**: Możesz także skorzystać z forum użytkowników systemu AVG, znajdziesz tego si pod adresem <http://community.avg.com/>.