AVG Internet Security 2014

Podręcznik użytkownika

Wersja dokumentu 2014.22 (6/19/2014)

Spis treści

1. Wprowadzenie 5

2. Wymagania instalacyjne AVG 6

2.1 Obsługiwane systemy operacyjne 6
2.2 Minimalne i zalecane wymagania sprzętowe 6

3. Proces instalacji systemu AVG 7

3.1 Witamy: Wybór języka 7
3.2 Witamy: Umowa licencyjna 8
3.3 Aktywuj licencję 9
3.4 Wybierz typ instalacji 10
3.5 Opcje niestandardowe 12
3.6 Postęp instalacji 13
3.7 Gratulacje! 14

4. Po instalacji 15

4.1 Rejestracja produktu 15
4.2 Dostęp do interfejsu użytkownika 15
4.3 Skanowanie całego komputera 15
4.4 Test EICAR 15
4.5 Konfiguracja domyślna systemu AVG 16

5. Interfejs użytkownika AVG 17

5.1 Górna sekcja nawigacyjna 18
5.2 Stan bezpieczeństwa 21
5.3 Przegląd składników 22
5.4 Moje aplikacje 23
5.5 Szybkie linki Skanuj / Aktualizuj 24
5.6 Ikona w zasobniku systemowym 24
5.7 Doradca AVG 26
5.8 AVG Accelerator 27

6. Składniki AVG 28

6.1 Ochrona komputera 28
6.2 Ochrona przeglądania sieci 33
6.3 Identity Protection 34
6.4 Ochrona poczty email 36
6.5 Zapora 38

6.6 Składnik Quick Tune ... 41

7. AVG Security Toolbar ... 43

8. AVG Do Not Track ... 45

8.1 Interfejs AVG Do Not Track ... 45
8.2 Informacje o procesach śledzących ... 47
8.3 Blokowanie procesów śledzących ... 48
8.4 Ustawienia AVG Do Not Track ... 48

9. Zaawansowane ustawienia AVG ... 50

9.1 Wygląd ... 50
9.2 Dźwięki ... 53
9.3 Tymczasowo wyłącz ochronę AVG ... 54
9.4 Ochrona komputera ... 55
9.5 Skaner poczty Email ... 60
9.6 Ochrona przeglądania sieci ... 75
9.7 Identity Protection ... 78
9.8 Skany ... 79
9.9 Zaplanowane zadania ... 85
9.10 Aktualizacja ... 94
9.11 Wyjątki ... 98
9.12 Przechowalnia wirusów ... 100
9.13 Ochrona własna AVG ... 101
9.14 Ustawienia prywatności ... 101
9.15 Ignoruj błędny stan ... 104
9.16 Doradca AVG – Znane sieci ... 105

10. Ustawienia Zapory ... 106

10.1 Ogólne ... 106
10.2 Aplikacje ... 108
10.3 Udostępnianie plików i drukarek ... 109
10.4 Ustawienia zaawansowane ... 110
10.5 Zdefiniowane sieci ... 111
10.6 Usługi systemowe ... 112
10.7 Dzienniki ... 114

11. Skanowanie AVG ... 116

11.1 Wstępnie zdefiniowane testy ... 118
11.2 Skan z poziomu eksploratora systemu Windows ... 127

11.3 Skan z poziomu wiersza poleceń 128
11.4 Planowanie skanowania 131
11.5 Wyniki skanowania 138
11.6 Szczegóły wyników skanowania 139

12. AVG File Shredder 141

13. Przechowalnia wirusów 142

14. Historia 144

14.1 Wyniki skanowania 144
14.2 Wyniki narzędzia Ochrona rezydentna 145
14.3 Wyniki Identity Protection 148
14.4 Wyniki narzędzia Ochrona poczty email 149
14.5 Wyniki narzędzia Ochrona sieci 150
14.6 Dziennik historii 152
14.7 Dziennik zapory 153

15. Aktualizacje systemu AVG 155

15.1 Uruchomienie aktualizacji 155
15.2 Poziomy aktualizacji 155

16. FAQ i pomoc techniczna 157

1. Wprowadzenie

Ten podręcznik użytkownika zawiera kompleksową dokumentację użytkownika systemu **AVG Internet Security 2014**.

AVG Internet Security 2014 zapewnia wielowarstwową ochronę w każdej sytuacji, co oznacza, że nie musisz się martwić wirusami, możliwością kradzieży 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 życiem na portalach społecznościowych, a także przeglądać i przeszukiwać sieć, wiedząc, że jesteś chroniony w czasie rzeczywistym.

Możesz skorzystać również z innych źródeł informacji:

- ***Plik pomocy***: Sekcja *Rozwiązywanie problemów* dostępna jest bezpośrednio w plikach pomocy **AVG Internet Security 2014** *(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*** znajdziesz uporządkowaną strukturę tematów opisujących kwestie handlowe i techniczne.

- ***Często zadawane pytania***: Na stronie AVG (*http://www.avg.com/*) opublikowana jest również obszerna sekcja często zadawanych pytań. Można się do niej dostać poprzez menu ***Centrum Pomocy technicznej / FAQ i samouczki*** . Wszystkie pytania podzielone są w czytelny sposób na sekcje: handlową, techniczną i na temat wirusów.

- ***AVG ThreatLabs***: Specjalna strona AVG (*http://www.avgthreatlabs.com/website-safety-reports/*) 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, zlokalizowanego pod adresem http://forums.avg.com.

2. Wymagania instalacyjne AVG

2.1. Obsługiwane systemy operacyjne

System **AVG Internet Security 2014** służy do ochrony stacji roboczych działających pod następującymi systemami operacyjnymi:

- Windows XP Home Edition z dodatkiem SP2
- Windows XP Professional z dodatkiem SP2
- Windows XP Professional x64 Edition z dodatkiem SP1
- Windows Vista (x86 i x64, wszystkie edycje)
- Windows 7 (x86 i x64, wszystkie edycje)
- Windows 8 (x32 i x64)

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

***Uwaga**: Składnik Identity Protection nie jest obsługiwany przez systemy Windows XP x64. Można zainstalować na nim system AVG Internet Security 2014, ale bez składnika Identity Protection.*

2.2. Minimalne i zalecane wymagania sprzętowe

Minimalne wymagania sprzętowe dla systemu **AVG Internet Security 2014**:

- Procesor Intel Pentium 1.5 GHz lub szybszy
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) pamięci RAM
- 1,3 GB wolnej przestrzeni dyskowej *(na potrzeby instalacji)*

Zalecane wymagania sprzętowe dla systemu **AVG Internet Security 2014**:

- Procesor Intel Pentium 1.8 GHz lub szybszy
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) pamięci RAM
- 1,6 GB wolnej przestrzeni dyskowej *(na potrzeby instalacji)*

3. Proces instalacji systemu AVG

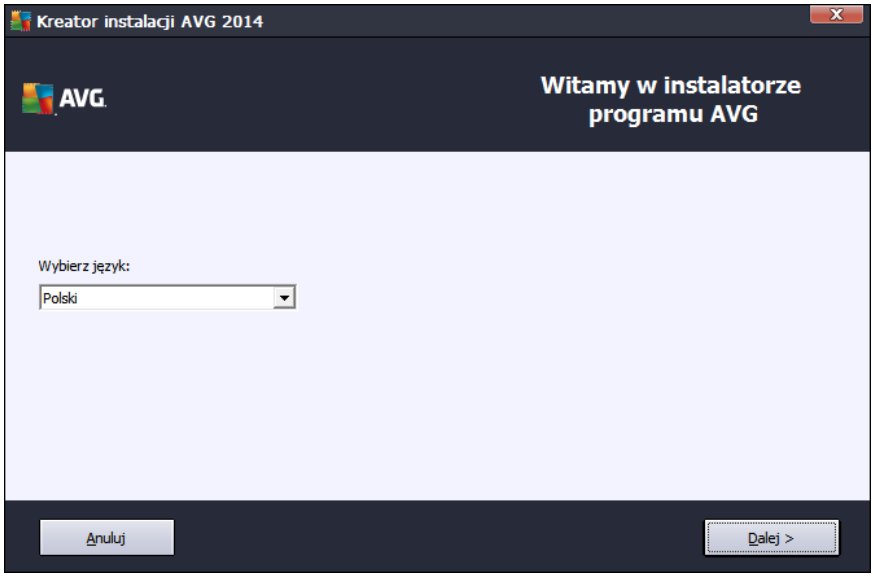
Do zainstalowania systemu **AVG Internet Security 2014** na komputerze konieczny jest najnowszy plik instalacyjny. Aby upewnić się, że instalujesz najnowszą dostępną wersję **AVG Internet Security 2014**, zalecamy pobranie pliku instalacyjnego bezpośrednio z witryny AVG (http://www.avg.com/). Sekcja ***Pomoc / Pobierz*** zawiera pełen zestaw plików instalacyjnych dla wszystkich edycji AVG.

Jeśli nie jesteś pewien, którego pliku potrzebujesz, użyj funkcji ***Wybierz produkt*** znajdującej się u dołu strony. Po udzieleniu odpowiedzi na trzy proste pytania, dowiesz się, czego dokładnie szukasz. Kliknij przycisk ***Kontynuuj***, aby przejść do listy potrzebnych Ci plików.

Po pobraniu i zapisaniu instalatora na dysku, można uruchomić proces instalacji. Instalacja składa się z kilku łatwych w zrozumieniu ekranów. Każdy z nich opisuje krótko, czego dotyczy. Poniżej znajdują się szczegółowe opisy poszczególnych okien:

3.1. Witamy: Wybór języka

Proces instalacji rozpoczyna okno ***Witamy w instalatorze AVG:***

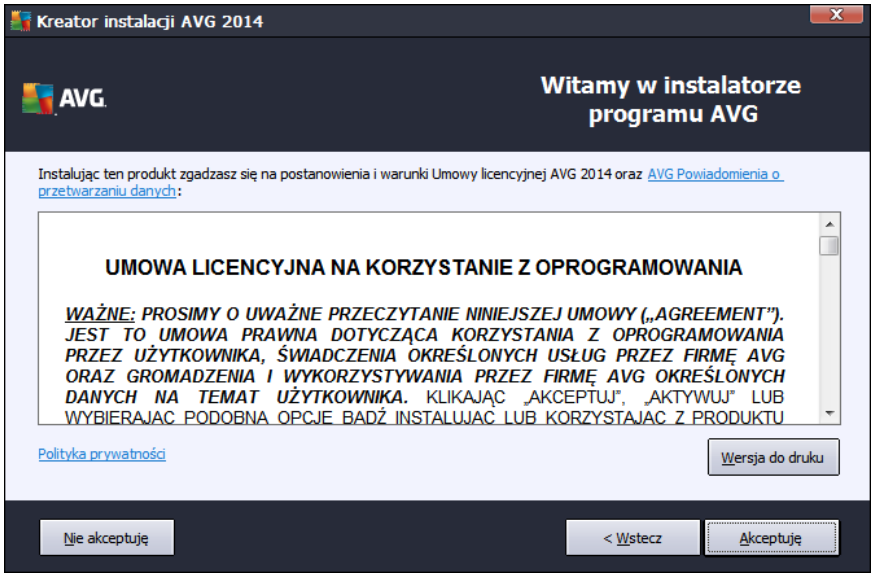


W tym oknie możesz wybrać język, który ma być używany podczas instalacji. Kliknij menu rozwijane, by wyświetlić dostępne języki. Wybierz żądany język, a proces instalacji będzie w nim kontynuowany.

Uwaga: W tym momencie wybierany jest jedynie język instalatora. System AVG Internet Security 2014 zostanie zainstalowany z obsługą wskazanego języka (oraz dodatkowo języka angielskiego, który dostępny jest domyślnie). Możliwa jest jednak instalacja dodatkowych języków i używanie systemu AVG Internet Security 2014 w dowolnym z nich. Jeden z kolejnych ekranów – Opcje niestandardowe – pozwala na wybór zestawu alternatywnych języków.

3.2. Witamy: Umowa licencyjna

Ekran ***Witamy w instalatorze AVG*** wyświetla również pełną treść umowy licencyjnej AVG:



Prosimy o uważne przeczytanie całości tekstu. Aby potwierdzić zapoznanie się z treścią umowy, zrozumienie jej i zaakceptowanie, kliknij przycisk ***Akceptuję***. Jeśli nie zgadzasz się z postanowieniami umowy licencyjnej, kliknij przycisk ***Odrzuć***. Instalacja zostanie natychmiast przerwana.

Porozumienie o przetwarzaniu danych i polityka prywatności firmy AVG

Oprócz umowy licencyjnej możliwe jest również przejrzenie treści ***Porozumienia o przetwarzaniu danych*** i ***Polityki prywatności*** firmy AVG. Wymienione funkcje są wyświetlane w oknie dialogowym w postaci aktywnego hiperłącza, które prowadzi do specjalnej strony internetowej zawierającej szczegółowe informacje. Kliknij odpowiednie łącze, aby przejść do odpowiedniej strony AVG (http://www.avg.com/), zawierającej pełną treść kryjącą się pod danym hasłem.

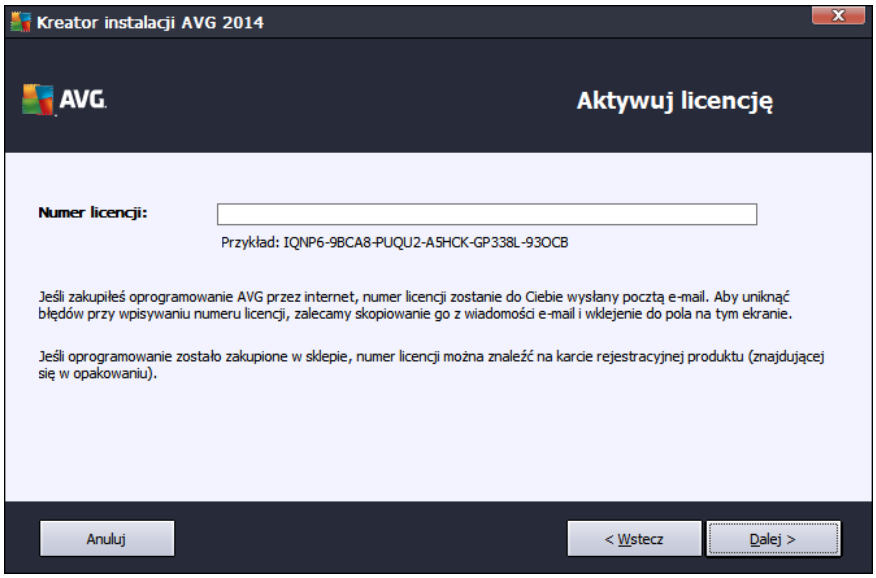
Przyciski kontrolne

W pierwszym oknie instalatora dostępne są tylko dwa przyciski:

- ***Wersja do druku*** – Kliknij ten przycisk, aby wyświetlić pełną, gotową do druku treść umowy licencyjnej AVG w przeglądarce internetowej.
- ***Odrzuć*** – powoduje odrzucenie umowy licencyjnej. Instalacje zostanie natychmiast zakończona. System **AVG Internet Security 2014** nie będzie zainstalowany!
- ***Wstecz*** – powoduje powrót do poprzedniego okna dialogowego.
- ***Akceptuj*** – potwierdza przeczytanie, zrozumienie i akceptację postanowień umowy licencyjnej. Instalacja będzie kontynuowana.

3.3. Aktywuj licencję

W oknie dialogowym ***Aktywuj licencję*** użytkownik jest proszony o wprowadzenie numeru licencji w polu tekstowym:



Gdzie znaleźć numer licencji

Numer sprzedaży można znaleźć na opakowaniu dysku CD z oprogramowaniem **AVG Internet Security 2014**. Numer licencji jest wysyłany za pośrednictwem poczty e-mail po dokonaniu zakupu oprogramowania **AVG Internet Security 2014** online. Ważne jest dokładne wprowadzenie tego numeru. Jeśli 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 wpisywaniu numeru licencji systemu **AVG Internet Security 2014** pozwala uniknąć błędów przy tradycyjnym przepisywaniu. Wykonaj następujące kroki:

- Otwórz wiadomość e-mail zawierającą Twój numer licencji.
- Przytrzymaj wciśnięty lewy przycisk myszy, przeciągając go od początku do końca numeru licencji. Numer powinien zostać podświetlony.
- Przytrzymaj ***Ctrl*** i naciśnij klawisz ***C***. Spowoduje to skopiowanie numeru.
- Umieść kursor w miejscu, w którym chcesz wkleić skopiowany tekst.
- Przytrzymaj ***Ctrl*** i naciśnij klawisz ***V***. Spowoduje to wklejenie numeru w żądanym polu.

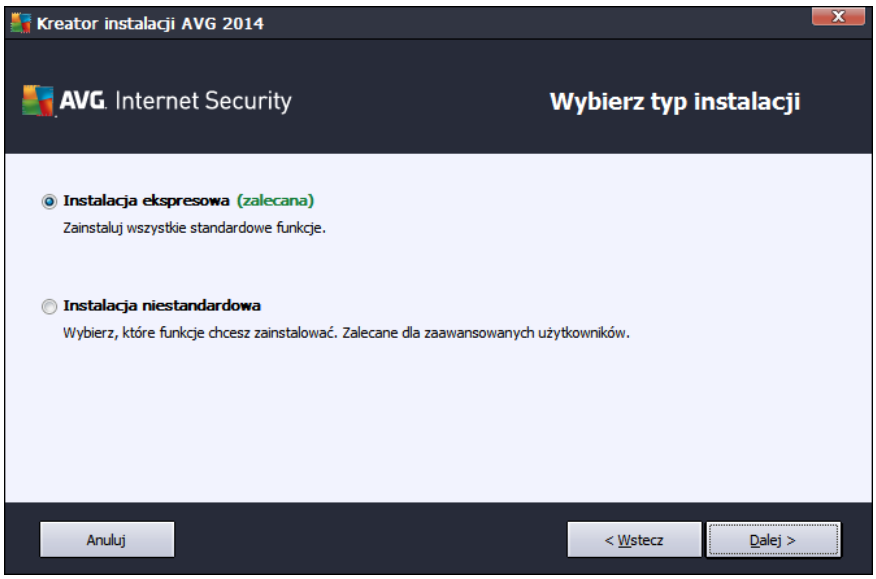
Przyciski kontrolne

Tak jak w przypadku wielu okien instalatora, dostępne są trzy przyciski kontrolne:

- ***Anuluj*** – kończy natychmiastowo proces instalacji; System **AVG Internet Security 2014** nie zostanie zainstalowany!
- ***Wstecz*** – powoduje powrót do poprzedniego okna dialogowego.
- ***Dalej*** – kontynuuje instalację, przechodząc do kolejnego kroku.

3.4. Wybierz typ instalacji

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



Instalacja ekspresowa

Dla większości użytkowników stanowczo zalecane jest skorzystanie ze standardowej instalacji ***Ekspresowej***. W ten sposób zainstalujesz **AVG Internet Security 2014** w pełni automatyczny sposób z domyślnymi ustawieniami producenta programu, w tym Pasek narzędzi AVG Security Toolbar. Taka konfiguracja zapewnia maksymalne bezpieczeństwo oraz optymalne wykorzystanie zasobów. Jeśli w przyszłości zajdzie potrzeba zmiany konfiguracji, można będzie to zrobić bezpośrednio z poziomu aplikacji **AVG Internet Security 2014**.

Kliknij przycisk ***Dalej***, aby przejść do następnego okna instalatora.

Instalacja niestandardowa

Opcję ***Instalacja niestandardowa*** powinni wybierać tylko doświadczeni użytkownicy, którzy mają uzasadnione powody, aby nie instalować systemu **AVG Internet Security 2014** z ustawieniami domyślnymi (np. po to, aby dostosować go do specyficznych wymagań systemowych). Gdy

wybierzesz tę opcję, w oknie dialogowym zostanie aktywowanych kilka nowych opcji:

- ***Zainstaluj pasek narzędzi AVG Toolbar, aby zwiększyć ochronę w internecie*** – Jeśli domyślne ustawienia nie zostaną zmienione, składnik ten zostanie automatycznie zainstalowany w domyślnej przeglądarce internetowej (*obecnie obsługiwane przeglądarki to Microsoft Internet Explorer w wersji 6.0 lub nowszej i Mozilla Firefox w wersji 3.0 lub nowszej*), aby zapewnić kompleksową ochronę podczas surfowania po internecie. Nie gwarantujemy działania naszego paska narzędzi w innych przeglądarkach (jeżeli używasz jednej z alternatywnych przeglądarek, np. Avant Browser, może wystąpić jej nieprzewidziane zachowanie.

- ***Ustaw i zachowaj AVG Secure Search jako domyślną stronę startową i stronę nowej karty*** – pozostaw to pole zaznaczone, aby potwierdzić, że chcesz otwierać domyślną przeglądarkę internetową i wszystkie jej karty z AVG Secure Search jako stroną startową.

- ***Ustaw i zachowaj AVG Secure Search jako domyślną wyszukiwarkę*** – pozostaw to pole zaznaczone , aby potwierdzić, że chcesz użyć wyszukiwarki AVG Secure Search, która ściśle współpracuje z technologią Link Scanner Surf Shield w celu zapewnienia Ci maksymalnego bezpieczeństwa online.

- ***Folder docelowy*** – W tym miejscu musisz podać lokalizację instalacji programu **AVG Internet Security 2014**. Domyślnie program **AVG Internet Security 2014** jest instalowany w folderze Program Files zlokalizowanym na dysku C:, zgodnie z wartością wyświetlaną w polu tekstowym okna dialogowego. Aby zmienić tę lokalizację, kliknij przycisk ***Przeglądaj*** i w wyświetlonym oknie wybierz odpowiedni folder. Aby przywrócić domyślną lokalizację (wstępnie ustawioną przez dostawcę oprogramowania), należy użyć przycisku ***Domyślne***.

Następnie kliknij przycisk ***Dalej***, aby przejść do okna Opcje niestandardowe.

Przyciski kontrolne

Tak jak w przypadku wielu okien instalatora, dostępne są trzy przyciski kontrolne:

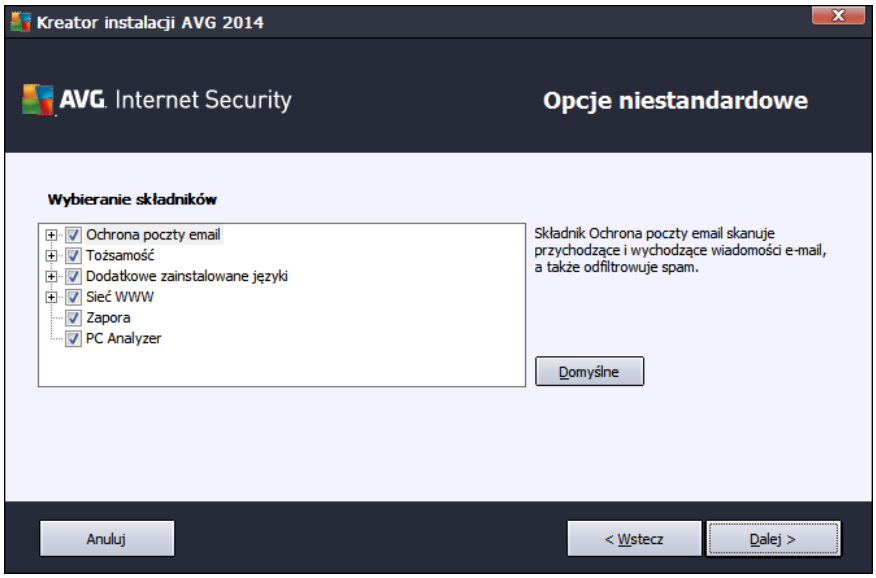
- ***Anuluj*** – kończy natychmiastowo proces instalacji; System **AVG Internet Security 2014** nie zostanie zainstalowany!

- ***Wstecz*** – powoduje powrót do poprzedniego okna dialogowego.

- ***Dalej*** – kontynuuje instalację, przechodząc do kolejnego kroku.

3.5. Opcje niestandardowe

Okno dialogowe ***Opcje niestandardowe*** umożliwia skonfigurowanie szczegółowych parametrów instalacji:



Sekcja ***Wybór składników*** zawiera przegląd wszystkich możliwych do zainstalowania składników systemu **AVG Internet Security 2014**. Jeśli ustawienia domyślne nie są dla Ciebie odpowiednie, można dodać lub usunąć wybrane składniki. ***Wybierać można jednak tylko składniki dostępne w zakupionej edycji systemu AVG!*** Po zaznaczeniu dowolnej pozycji na liście ***Wybór składników*** po prawej stronie zostanie wyświetlony krótki opis odpowiedniego składnika. Szczegółowe informacje o funkcjach poszczególnych składników zawiera rozdział Przegląd składników. Aby przywrócić domyślną konfigurację wstępnie ustawioną przez dostawcę oprogramowania, należy użyć przycisku ***Domyślne***.

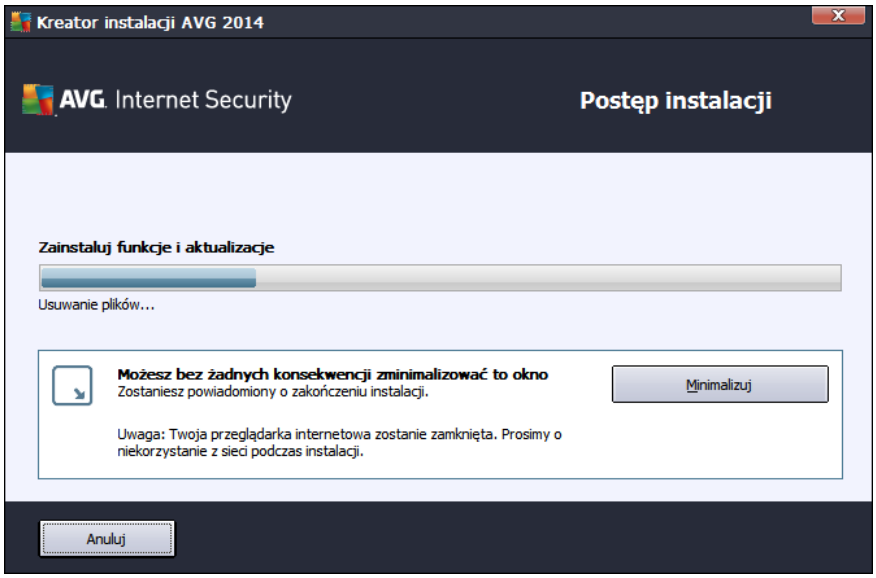
Przyciski kontrolne

Tak jak w przypadku wielu okien instalatora, dostępne są trzy przyciski kontrolne:

- ***Anuluj*** – kończy natychmiastowo proces instalacji; System **AVG Internet Security 2014** nie zostanie zainstalowany!
- ***Wstecz*** – powoduje powrót do poprzedniego okna dialogowego.
- ***Dalej*** – kontynuuje instalację, przechodząc do kolejnego kroku.

3.6. Postęp instalacji

Okno dialogowe ***Postęp instalacji*** zawiera jedynie informacje o postępie procesu instalacji i nie wymaga żadnych działań ze strony użytkownika:



Po zakończeniu instalacji nastąpi przekierowanie do następnego okna dialogowego.

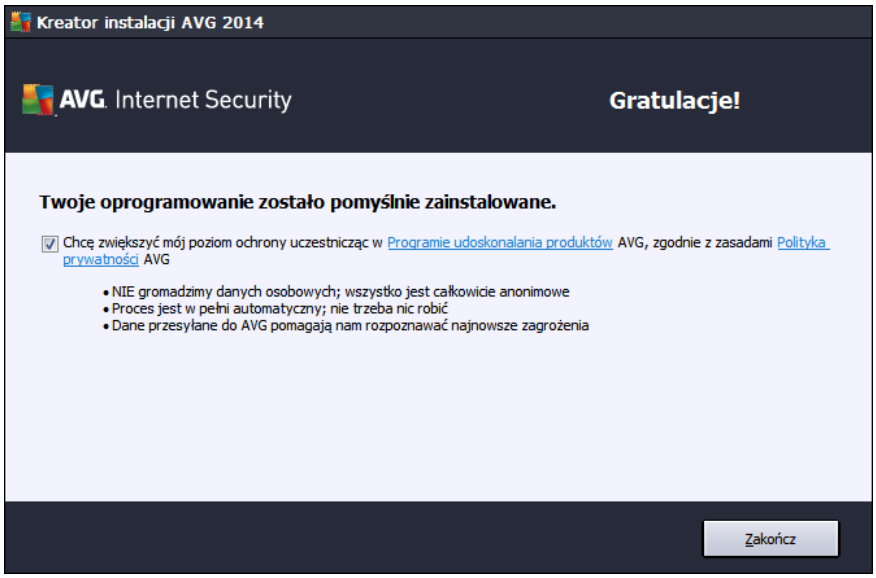
Przyciski kontrolne

To okno zawiera dwa przyciski kontrolne:

- ***Minimalizuj*** – Proces instalacji może potrwać kilka minut. Kliknięcie tego przycisku zminimalizuje okno do postaci ikony widocznej na pasku systemowym. Okno pojawi się ponownie po zakończeniu instalacji.
- ***Anuluj*** – Ten przycisk powinien być używany tylko w przypadku konieczności zatrzymania procesu instalacji. Prosimy pamiętać, że wówczas system **AVG Internet Security 2014** nie zostanie zainstalowany!

3.7. Gratulacje!

Okno ***Gratulujemy*** potwierdza, że produkt **AVG Internet Security 2014** został w pełni zainstalowany i skonfigurowany:



Program udoskonalania produktów i Polityka prywatności

To okno pozwala zdecydować, czy chcesz ***brać udział w Programie udoskonalania produktów (*** *Szczegóły znajdują się w rozdziale Zaawansowane ustawienia AVG / Program udoskonalania produktów AVG*), który pozwala nam zbierać anonimowe informacje o wykrytych zagrożeniach, podnosząc dzięki temu ogólny poziom bezpieczeństwa w internecie. Wszystkie dane traktowane są jako poufne, zgodnie z Polityką prywatności AVG; kliknij link ***Polityka prywatności***, by zostać przekierowanym na stronę internetową AVG (http://www.avg.com/) zawierającą pełną treść Polityki prywatności AVG. Jeśli się zgadzasz, pozostaw tę opcję zaznaczoną *(domyślnie jest ona zaznaczona)*.

Aby zakończyć proces instalacji, kliknij przycisk ***Zakończ***.

4. Po instalacji

4.1. Rejestracja produktu

Po ukończeniu instalacji **AVG Internet Security 2014** 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 stronę rejestracji najprościej jest przejść z poziomu interfejsu użytkownika systemu **AVG Internet Security 2014**. Wybierz z górnej nawigacji pozycję Opcje / Zarejestruj teraz. Zostaniesz wówczas przeniesiony na stronę ***Rejestracja*** (*http://www.avg.com/*). Tam znajdziesz dalsze wskazówki.

4.2. Dostęp do interfejsu użytkownika

Dostęp do interfejsu użytkownika AVG można uzyskać na kilka sposobów:

- klikając dwukrotnie ikonę AVG na pasku zadań,
- klikając dwukrotnie ikonę AVG na pulpicie,
- z menu ***Start / Wszystkie Programs / AVG / AVG 2014***

4.3. Skanowanie całego komputera

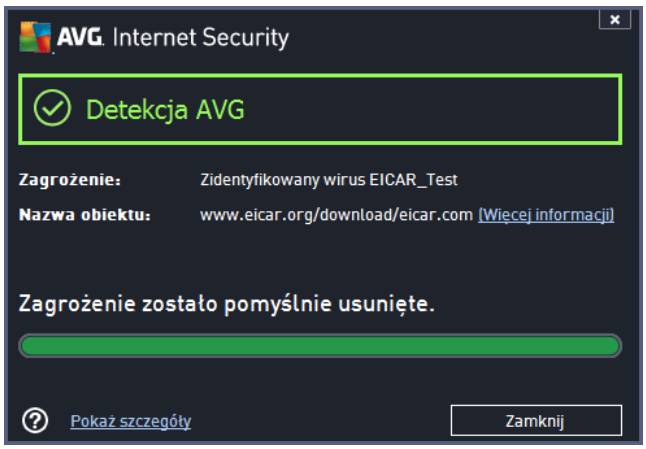
Istnieje pewne ryzyko, że wirus dostał się do komputera przed zainstalowaniem systemu **AVG Internet Security 2014**. Z tego powodu należy uruchomić test Skan całego komputera, aby upewnić się, że jest on w pełni bezpieczny. Pierwsze skanowanie może chwilę potrwać *(około godziny)*, lecz zalecamy uruchomienie go, by zyskać pewność, że komputer nie jest zainfekowany przez wirusy. Instrukcje dotyczące uruchamiania testu Skan całego komputera zawiera rozdział Skanowanie AVG.

4.4. Test EICAR

Aby potwierdzić, że system **AVG Internet Security 2014** został zainstalowany poprawnie, można przeprowadzić test EICAR.

Test EICAR jest standardową i całkowicie bezpieczną metodą służącą do sprawdzania prawidłowości działania systemu antywirusowego. Można go bezpiecznie rozpowszechniać, ponieważ nie jest prawdziwym wirusem i nie zawiera żadnych fragmentów złośliwego kodu. Większość produktów rozpoznaje go jako wirusa (*chociaż zwykle zgłasza go pod jednoznaczną 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* i zapisać go na dysku twardym komputera. Zaraz po tym jak potwierdzisz pobranie pliku testowego, Twój system **AVG Internet Security 2014** powinien zareagować ostrzeżeniem. Pojawienie się komunikatu potwierdza, że oprogramowanie AVG jest prawidłowo zainstalowane na komputerze.



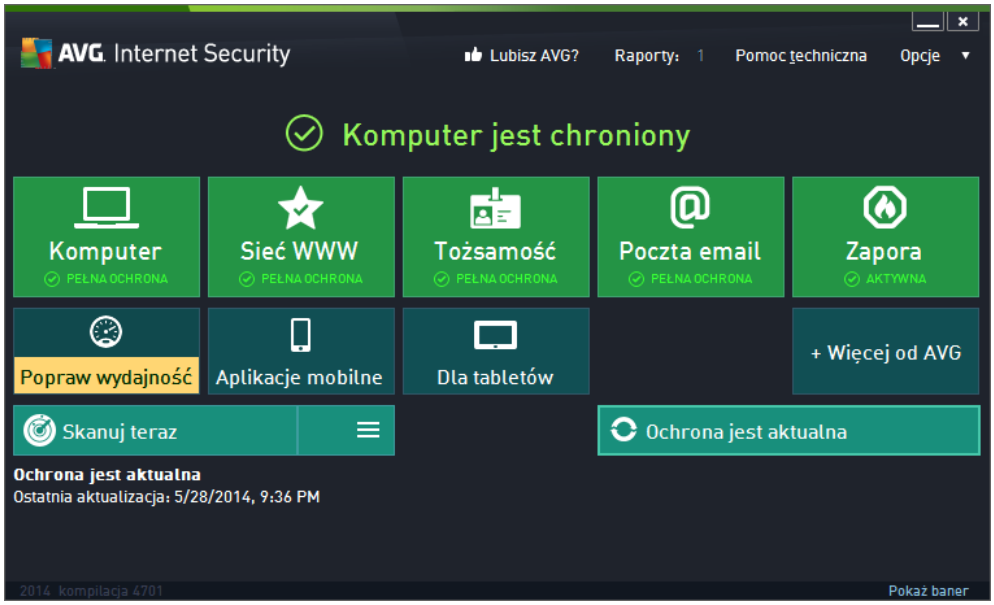
Jeśli system AVG nie rozpozna pliku testowego EICAR jako wirusa, należy ponownie sprawdzić jego konfigurację!

4.5. Konfiguracja domyślna systemu AVG

Konfiguracja domyślna (*ustawienia stosowane zaraz po instalacji*) systemu **AVG Internet Security 2014** jest wstępnie definiowana przez producenta i ma na celu zapewnienie optymalnej wydajności wszystkich składników oraz funkcji. ***Konfigurację systemu AVG należy zmieniać tylko w uzasadnionych przypadkach! Wszelkie zmiany powinny być wprowadzane wyłącznie przez doświadczonych użytkowników.*** Jeśli chcesz precyzyjnie dopasować konfigurację systemu AVG do swoich potrzeb, użyj Ustawień zaawansowanych AVG, *wybierając z menu głównego Ustawienia zaawansowane* i edytując opcje w nowo otwartym oknie Ustawienia zaawansowane AVG.

5. Interfejs użytkownika AVG

Otwarcie systemu **AVG Internet Security 2014** powoduje wyświetlenie jego okna głównego:



Okno główne jest podzielone na kilka sekcji:

- ***Górna nawigacja*** składa się z czterech linków umieszczonych w górnej sekcji głównego okna *(Polub AVG, Raporty, Pomoc, Opcje).* Szczegóły >>
- ***Informacje o stanie bezpieczeństwa*** to podstawowe informacje o obecnym stanie Twojego systemu **AVG Internet Security 2014**. Szczegóły >>
- ***Przegląd zainstalowanych składników*** znajduje się w poziomej linii bloków w środkowej sekcji okna głównego. Składniki widoczne są pod postacią jasnozielonych bloków, oznaczonych ikonami odpowiednich składników i zawierających informację o ich stanie. Szczegóły >>
- ***Moje aplikacje*** przedstawione są na pasku widocznym w dolnej części okna głównego i wyświetlają przegląd dodatkowych aplikacji **AVG Internet Security 2014**, które już zostały zainstalowane, lub których instalację zalecamy. Szczegóły >>
- ***Szybkie linki Skanuj / Aktualizuj*** umieszczone są w dolnej linii bloków na głównym ekranie. Przyciski te dają natychmiastowy dostęp do najważniejszych i najczęściej używanych funkcji AVG. Szczegóły >>

Poza głównym oknem **AVG Internet Security 2014** istnieje jeszcze jeden element, którego możesz użyć, by uzyskać dostęp do aplikacji:

- ***Ikona w zasobniku systemowym*** znajduje się w prawym dolnym rogu ekranu *(w zasobniku systemowym),* i wskazuje obecny stan systemu **AVG Internet Security 2014**. Szczegóły >>

5.1. Górna sekcja nawigacyjna

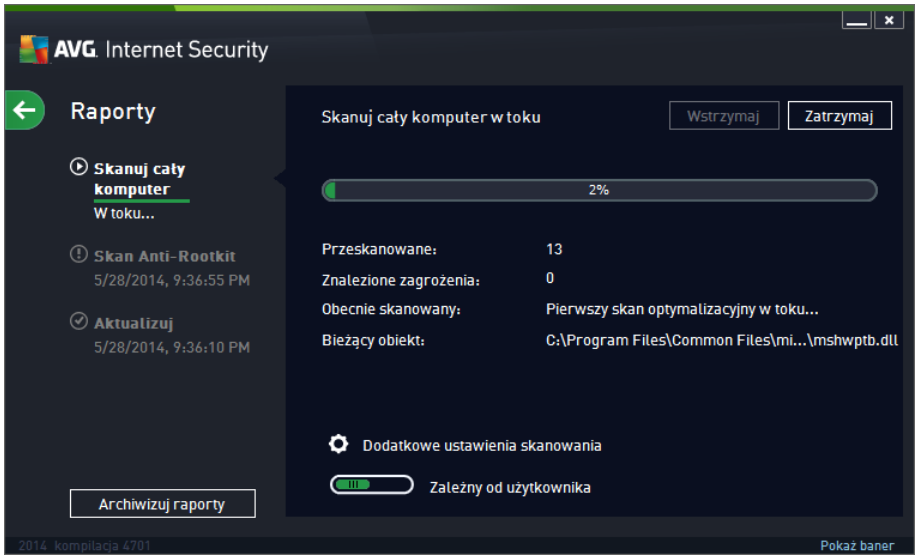
Górna sekcja nawigacyjna składa się z kilku aktywnych linków ułożonych w linii w górnej sekcji głównego okna. Nawigacja możliwa jest dzięki następującym przyciskom:

5.1.1. Dołącz do nas na Facebooku

Kliknij link, by połączyć się ze społecznością AVG w serwisie Facebook i dzielić najnowszymi informacjami, wiadomościami i poradami dotyczącymi AVG, by zapewnić sobie maksymalną ochronę.

5.1.2. Raporty

Otwiera nowe okno ***Raporty*** zawierające przegląd wszystkich raportów dotyczących poprzednio uruchomionych procesów skanowania i aktualizacji. Jeśli skanowanie lub aktualizacja jest w toku, obok tekstu ***Raporty*** w górnej części nawigacyjnej głównego interfejsu użytkownika wyświetlona będzie ikona obracającego się okręgu. Kliknij ją, aby przejść do okna obrazującego postęp uruchomionego procesu:



5.1.3. Pomoc

Otwiera nowe okno podzielone na cztery karty, które pozwolą Ci znaleźć wszystkie informacje o Twoim systemie **AVG Internet Security 2014**:

- ***Licencja i Pomoc techniczna*** – Ta karta dostarcza informacji 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, by otworzyć nowe okno ***Aktywuj oprogramowanie AVG***. Wprowadzenie w nim nowego numeru licencji umożliwia zastąpienie numeru handlowego *(używanego podczas instalacji AVG Internet Security 2014)*, lub zmianę licencji *(np. przy uaktualnieniu do bogatszej wersji systemu AVG)*.

    - *Kopiuj do schowka* – Użyj tego linku, by skopiować numer licencji, a następnie wkleić go w żądanym miejscu. W ten sposób będziesz pewien, że numer licencji został wpisany poprawnie.

    - *Odnów teraz* – Zalecamy odnowienie licencji programu **AVG Internet Security 2014** z wyprzedzeniem, co najmniej na miesiąc przed wygaśnięciem aktualnej. Zostaniesz powiadomiony o zbliżającej się dacie wygaśnięcia licencji. Kliknij ten link, by przejść do witryby AVG *(http://www.avg.com/)*, na której znajdziesz szczegółowe informacje o stanie swojej licencji, jej dacie wygaśnięcia i ofercie odnowienia/uaktualnienia.

- ***Produkt*** – Ta karta zawiera przegląd **AVG Internet Security 2014** najważniejszych informacji technicznych o produkcie, zainstalowanych składnikach, zainstalowanej ochronie poczty e-mail oraz samym systemie.

- ***Program*** – Na tej karcie możesz znaleźć informacje o wersji programu oraz o użytych bibliotekach innych producentów.

- ***Umowa licencyjna*** – Ta karta cytuje pełną treść umowy licencyjnej, którą zawarłeś z firmą

AVG Technologies.

5.1.4. Opcje

Funkcje obsługi systemu **AVG Internet Security 2014** dostępne są w sekcji ***Opcje***. Kliknij strzałkę, by otworzyć menu rozwijane:

- ***Skanuj komputer*** uruchamia skanowanie całego komputera.
- ***Skanuj wybrany folder...*** – przełącza do interfejsu skanera systemu AVG i umożliwia wskazanie plików oraz folderów, które mają zostać przeskanowane.
- ***Skanuj plik...*** – Pozwala przetestować na żądanie pojedynczy plik. Wybranie tej opcji spowoduje otwarcie nowego okna, przedstawiającego drzewiastą strukturę katalogów. Wskaż żądany plik i potwierdź rozpoczęcie skanowania.
- ***Aktualizuj*** – Automatycznie uruchamia proces aktualizacji systemu **AVG Internet Security 2014**.
- ***Aktualizuj z katalogu...*** – uruchamia proces aktualizacji korzystając z pliku zlokalizowanego w określonym folderze na dysku lokalnym. Jednak ta opcja jest zalecana do użytku jedynie w sytuacjach awaryjnych, np. gdy nie ma połączenia z internetem (komputer został zainfekowany i odłączony od internetu, komputer jest podłączony do sieci bez dostępu do internetu itp.). W nowo otwartym oknie należy wskazać folder, w którym został wcześniej zapisany plik aktualizacyjny, a następnie uruchomić proces aktualizacji.
- ***Przechowalnia wirusów*** – Otwiera interfejs Przechowalni wirusów, do której program AVG przenosi wszystkie niemożliwe do wyleczenia infekcje. W czasie tej kwarantanny zainfekowane pliki są izolowane i nie zagrażają bezpieczeństwu komputera, a jednocześnie istnieje możliwość ich naprawy w przyszłości.
- ***Historia*** – Rozwija dalsze opcje podmenu:
  - *Wyniki skanowania* – Otwiera okno zawierające przegląd wyników skanowania.
  - *Zagrożenia wykryte przez Ochronę rezydentną* – Otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez Ochronę Rezydentną.
  - *Zagrożenia wykryte przez Identity Protection* – Otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez składnik Identity.
  - *Zagrożenia wykryte przez Ochronę poczty email* – Otwiera okno zawierające przegląd załączników uznanych przez Ochronę poczty e-mail za niebezpieczne.
  - *Zagrożenia wykryte przez Ochronę Sieci* – Otwiera okno dialogowe zawierające przegląd zagrożeń wykrytych przez składnik Ochrona Sieci
  - *Dziennik historii zdarzeń* – Otwiera interfejs dziennika historii z przeglądem wszystkich zarejestrowanych akcji **AVG Internet Security 2014**.
  - *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 2014**. Na ogół zaleca się zachowanie domyślnych ustawień zdefiniowanych przez producenta oprogramowania AVG.

- ***Ustawienia Zapory...*** – Otwiera okno zaawansowanej konfiguracji składnika Zapora AVG.

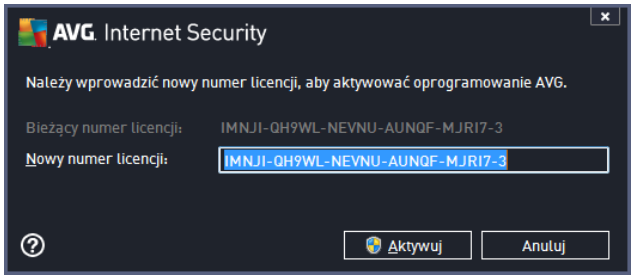
- ***Spis treści*** – Otwiera pliki pomocy systemu AVG.

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

- ***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 sprzedaży (*użytego do zainstalowania programu AVG*) lub starego numeru licencji (*na przykład podczas uaktualnienia do nowego produktu AVG*). W przypadku korzystania z próbnej wersji systemu **AVG Internet Security 2014**, ostatnie dwie pozycje to ***Kup teraz*** i ***Aktywuj***. Umożliwiają one uaktualnienie programu do jego pełnej wersji. W przypadku systemu **AVG Internet Security 2014** zainstalowanego z numerem sprzedaży, te pozycje to ***Zarejestruj*** i ***Aktywuj***:



- ***Zarejestruj teraz / MyAccount*** – Jest linkiem do strony rejestracyjnej oprogramowania AVG (*http://www.avg.com/*). Należy tam podać swoje dane rejestracyjne – jedynie klientom, którzy zarejestrowali swój produkt AVG, przysługuje bezpłatna pomoc techniczna.

- ***AVG – Informacje*** – Otwiera nowe okno zawierające cztery karty z informacjami o zakupionej licencji i dostępnej pomocy, produkcie oraz programie, a także pełny tekst umowy licencyjnej. *(To samo okno dialogowe można otworzyć, klikając łącze Pomoc techniczna w głównym panelu nawigacji).*

5.2. Stan bezpieczeństwa

Obszar ***Informacje o stanie bezpieczeństwa*** znajduje się w górnej części głównego okna **AVG Internet Security 2014**. Znajdziesz tam informacje o bieżącym stanie bezpieczeństwa systemu **AVG Internet Security 2014**. W obszarze tym mogą być wyświetlane następujące ikony:

– zielona ikona wskazuje, że system ***AVG Internet Security 2014 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 2014** nie wystąpił jednak żaden błąd krytyczny, a użytkownik prawdopodobnie wyłączył z jakiegoś powodu jeden ze składników. Wciąż jesteś chroniony!. Należy jednak sprawdzić ustawienia składnika, który zgłasza problem! Błędnie skonfigurowany składnik będzie oznaczony pomarańczowym paskiem w głównym interfejsie użytkownika.

Żółta ikona pojawia się również wtedy, gdy z jakiegoś powodu zdecydowałeś się ignorować błędny stan któregoś ze składników. Opcja ***Ignoruj błędny stan*** dostepna jest w gałęzi Ustawienia zaawansowane / Ignoruj błędny stan. Masz możliwość potwierdzić, że zdajesz sobie sprawę z błędnego stanu składnika, ale z pewnych powodów chcesz pozostawić system **AVG Internet Security 2014** w tym stanie i nie chcesz być o tym ostrzegany. W pewnych sytuacjach użycie tej opcji może być pomocne, jednak zalecamy wyłączenie opcji ***Ignorowania błędnego stanu*** tak szybko, jak to będzie możliwe!

Oprócz tego, żółta ikona będzie wyświetlana, gdy Twój system **AVG Internet Security 2014** wymaga restartu komputera (***Wymagany restart***). Prosimy o zwrócenie uwagi na to ostrzeżenie i ponowne uruchomienie komputera.

 – pomarańczowa ikona wskazuje na krytyczny stan systemu ***AVG Internet Security 2014***! Co najmniej jeden składnik nie działa poprawnie, a system **AVG Internet Security 2014** nie może chronić Twojego komputera. Należy natychmiast usunąć zgłoszony problem! Jeśli nie jest to możliwe, należy skontaktować się z zespołem Pomocy technicznej AVG.

Jeżeli system AVG Internet Security 2014 wykryje, że nie działa z optymalną wydajnością, obok informacji o stanie pojawi się przycisk "Kliknij, by naprawić problem" (lub "Kliknij, by naprawić wszystko", jeśli problem dotyczy kilku składników). Kliknij ten przycisk, by rozpocząć automatyczny proces sprawdzenia i naprawy programu. Jest to prosty sposób na osiągnięcie optymalnej wydajności systemu AVG Internet Security 2014 oraz maksymalnego poziomu bezpieczeństwa.

Stanowczo zaleca się reagowanie na zmiany ***Stanu bezpieczeństwa*** i natychmiastowe rozwiązywanie ewentualnych problemów. Brak reakcji naraża komputer na poważne zagrożenia!

Uwaga: *Informacje o stanie systemu AVG Internet Security 2014 można również uzyskać w dowolnym momencie z poziomu ikony na pasku zadań.*

5.3. Przegląd składników

Przegląd zainstalowanych składników znajduje się w poziomej linii bloków w środkowej sekcji okna głównego. Składniki wyświetlane są pod postacią jasnozielonych bloków oznaczonych ikonami odpowiednich składników. Każdy blok zawiera również informację 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 błędu, zostaniesz o tym ostrzeżony poprzez tekst w kolorze pomarańczowym. ***Zalecamy wówczas zwrócenie szczególnej uwagi na ustawienia danego składnika!***

Umieść kursor myszy nad składnikiem, by wyświetlić krótki tekst w dolnej części okna głównego.

Tekst ten stanowi wprowadzenie do funkcjonalności danego składnika. Informuje on również o bieżącym stanie składnika, a także wskazuje, która z funkcji składnika nie jest poprawnie skonfigurowana.

Lista zainstalowanych składników

Sekcja ***Przegląd składników*** systemu **AVG Internet Security 2014** zawiera informacje o następujących składnikach:

- ***Komputer*** – Ten składnik świadczy dwie usługi: ***Ochronę antywirusową*** wykrywa wirusy, oprogramowanie szpiegujące, robaki, konie trojańskie, niepożądane pliki wykonywalne lub biblioteki i chroni Cię przed szkodliwym oprogramowaniem reklamowym, oraz ***Anti-Rootkit*** skanuje aplikacje, sterowniki i biblioteki w poszukiwaniu rootkitów. Szczegóły >>
- ***Przeglądanie Sieci*** – chroni Cię przed zagrożeniami internetowymi w czasie gdy przeglądasz strony WWW. Szczegóły >>
- ***Identity*** – 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, blokując wirusy, próby phishingu i inne zagrożenia.Szczegóły >>
- ***Zapora*** – kontroluje całą komunikację na wszystkich portach sieciowych, chroniąc komputer przed atakami oraz blokując wszelkich intruzów. Szczegóły >>

Dostępne akcje

- ***Umieść kursor nad ikoną dowolnego składnika***, aby go zaznaczyć. W dolnej części interfejsu użytkownika zostanie wówczas wyświetlony opis jego podstawowych funkcji.
- ***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*** *(linijka zielonych bloków pod zbiorem składników)* znajduje się przegląd dodatkowych aplikacji AVG, które są już zainstalowane, lub których instalacja jest zalecana. Bloki te są wyświetlane zależnie od Twojego systemu i mogą reprezentować następujące aplikacje:

- ***Ochrona mobilna*** to aplikacja chroniąca Twój telefon komórkowy przed wirusami i złośliwym oprogramowaniem. Daje również możliwość zdalnego śledzenia swojego telefonu, jeśli kiedykolwiek go utracisz.
- ***LiveKive*** ma w założeniu tworzyć kopie zapasowe ważnych danych na naszych bezpiecznych serwerach. LiveKive automatycznie tworzy kopie zapasowe wszystkich Twoich plików, zdjęć i muzyki w jednym bezpiecznym miejscu, pozwalając Ci dzielić się nimi z rodziną i przyjaciółmi oraz korzystać z nich na urządzeniach typu iPhone i Android.

- ***Funkcja Family Safety*** pozwala chronić dzieci przed nieodpowiednią zawartością stron internetowych i wynikami wyszukiwania oraz umożliwia tworzenie raportów dotyczących ich aktywności online. AVG Family Safety rejestruje sekwencje klawiszy, aby monitorować aktywność Twojego dziecka w pokojach czatowych lub w sieciach społecznościowych. W przypadku wykrycia słów, fraz lub specyficznego tonu, który może wskazywać na agresję lub próbę manipulacji Twoim dzieckiem, zostaniesz o tym powiadomiony poprzez SMS lub e-mail. Możesz ustawić odpowiedni poziom ochrony dla każdego dziecka i monitorować je oddzielnie przy użyciu unikatowych kont.

- ***PC Tuneup*** jest zaawansowanym narzędziem analizującym stan systemu pod kątem zwiększenia wydajności Twojego komputera.

- ***MultiMi*** sprowadza w jedno, bezpieczne miejsce wszystkie Twoje konta poczty e-mail i sieci społecznościowych, ułatwiając kontakt z rodziną i przyjaciółmi, przeglądanie internetu oraz dzielenie się zdjęciami, filmami i plikami. MultiMi zawiera w sobie usługę LinkScanner, która chroni Cię przed stale wzrastającą liczbą zagrożeń internetowych, analizując strony kryjące się za wszystkimi linkami, które spotykasz przeglądając internet.

- ***AVG Toolbar*** jest dostępny bezpośrednio z poziomu przeglądarki internetowej, by zapewnić Ci maksymalne bezpieczeństwo podczas przeglądania internetu.

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

5.5. Szybkie linki Skanuj / Aktualizuj

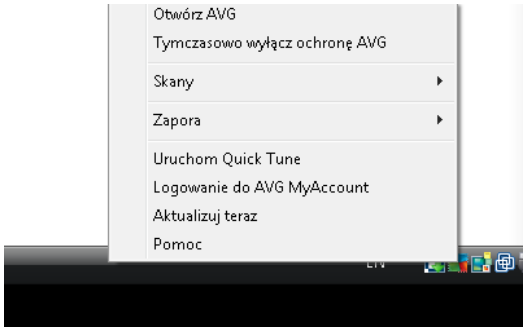
Szybkie linki znajdują się w dolnej części interfejsu użytkownika **AVG Internet Security 2014**. Pozwalają one uzyskać natychmiastowy dostęp do najważniejszych i najczęściej używanych funkcji aplikacji, czyli skanowania i aktualizacji. Szybkie linki dostępne są z poziomu dowolnego okna interfejsu:

- ***Skanuj teraz*** – Przycisk ten jest graficznie podzielony na dwie sekcje. Użyj linku ***Skanuj teraz***, by natychmiastowo uruchomić Skanowanie całego komputera i obserwować jego postęp oraz wyniki w otwartym oknie Raporty. Przycisk ***Opcje*** otwiera okno ***Opcje skanowania***, które pozwala zarządzać zaplanowanymi skanami oraz edytować parametry Skanu całego komputer / Skanu określonych plików lub folderów. *(Szczegóły można znaleźć w rozdziale Skanowanie AVG)*

- ***Aktualizuj teraz*** – Użyj tego przycisku, by natychmiastowo uruchomić aktualizację produktu. Zostaniesz poinformowany o wynikach aktualizacji za pomocą wysuwanego okna 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 systemu **AVG Internet Security 2014**. Ikona ta jest zawsze widoczna, niezależnie od tego, czy Interfejs użytkownika **AVG Internet Security 2014** jest otwarty czy zamknięty:



Ikona AVG na pasku zadań

- Jeśli ikona na pasku zadań jest kolorowa i nie zawiera żadnych dodatków, oznacza to, że wszystkie składniki systemu **AVG Internet Security 2014** są aktywne i w pełni funkcjonalne. Może ona być kolorowa także wtedy, gdy system AVG zasygnalizował błędy, 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 co najmniej jeden składnik jest w stanie błędu. Prosimy o baczne obserwowanie takich sytuacji oraz o podjęcie próby przywrócenia poprawnej konfiguracji odpowiednich składników. W tym celu wystarczy kliknąć dwukrotnie ikonę, co spowoduje otwarcie interfejsu użytkownika AVG. Szczegóły na temat błędnego stanu systemu można znaleźć w sekcji Informacje o stanie bezpieczeństwa.

- Kolorowej ikonie na pasku zadań może również 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 **AVG Internet Security 2014**.

Informacje ikony na pasku zadań

Ikona AVG w obszarze powiadomień informuje także o bieżących czynnościach podejmowanych przez Twój system **AVG Internet Security 2014**, a także o potencjalnych zmianach jego stanu (*np. o automatycznym uruchomieniu zaplanowanego skanu lub aktualizacji, przełączeniu profilu Zapory, zmianie stanu składnika, wystąpieniu błędu itp.*) poprzez wyskakujące okienka otwierane w obszarze powiadomień.

Akcje dostępne z poziomu ikony na pasku zadań

Ikona AVG na pasku zadań może być używana jako szybki sposób na uruchomienie interfejsu użytkownika **AVG Internet Security 2014** (wystarczy dwukrotne kliknięcie). Kliknięcie ikony prawym przyciskiem myszy otwiera menu kontekstowe zawierające następujące opcje:

- ***Otwórz AVG*** – kliknij, aby otworzyć interfejs użytkownika programu **AVG Internet Security 2014**.

- ***Tymczasowo wyłącz ochronę AVG*** – Ta opcja pozwala Ci natychmiastowo wyłączyć wszelką ochronę zapewnianą przez system **AVG Internet Security 2014**. Pamiętaj, że tej opcji nie powinno się używać, chyba że jest to absolutnie konieczne! W większości przypadków nie jest konieczne wyłączanie systemu **AVG Internet Security 2014** przed instalowaniem nowego oprogramowania lub sterowników, nawet jeśli instalator lub kreator sugeruje uprzednie zamknięcie działających programów i aplikacji. Jeśli jednak tymczasowe wyłączenie systemu **AVG Internet Security 2014** jest konieczne, należy go 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 otwiera menu kontekstowe zawierające predefiniowane skany (*Skan całego komputera*, *Skan wybranych plików/folderów*) i umożliwia natychmiastowe uruchomienie dowolnego z nich.

- ***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. Ponadto dostępne są następujące akcje: *Ustaw priorytet dla wszystkich skanów, Wstrzymaj wszystkie skanowania* lub *Zatrzymaj wszystkie skanowania*.

- ***Uruchom Quick Tune*** – kliknij, aby uruchomić składnik Quick Tune.

- ***Zaloguj się na konto AVG MyAccount*** – Otwiera stronę główną AVG MyAccount, umożliwiającą zarządzanie subskrypcjami Twoimi produktów, zakup dodatkowej ochrony, pobranie plików instalacyjnych, sprawdzenie przeszłych zamówień i faktur, a także zarządzanie danymi osobowymi.

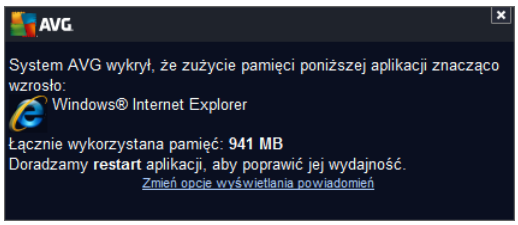
- ***Aktualizuj teraz*** – uruchamia natychmiastową aktualizację.

- ***Pomoc*** – otwiera plik pomocy na stronie startowej.

5.7. Doradca AVG

Doradca AVG został stworzony po to, by wykrywać problemy (które mogą spowalniać Twój komputer lub stwarzać zagrożenia) oraz proponować ich rozwiązania. Gdy komputer zaczyna nagla zwalniać *(dotyczy to zarówno przeglądania internetu, jak i ogólnej wydajności)*, dokładna przyczyna ani skuteczne rozwiązanie nie zawsze są znane. Właśnie w takim momencie może pomóc ***Doradca AVG***: w obszarze powiadomień wyświetli on powiadomienie z informacją o ewentualnym problemie i sposobie jego rozwiązania. ***Doradca AVG*** stale monitoruje wszystkie działające na Twoim komputerze procesy pod kątem możliwych problemów, by w razie potrzeby doradzić ich rozwiązanie.

Doradca AVG widoczny jest w postaci powiadomienia wysuwanego nad paskiem systemowym:



Doradca AVG monituruje między innymi:

- ***Stan aktualnie otwartych przeglądarek internetowych***. Przeglądarki internetowe potrafią przeciążyć pamięć operacyjną (szczególnie wtedy, gdy wiele okien lub kart pozostaje otwartych przez dłuższy czas), spowalniając tym samym Twój komputer. Najczęstszym rozwiązaniem jest w tym przypadku ponowne uruchomienie przeglądarki.

- ***Otwarte połączenia peer-to-peer***. Protokoły P2P wykorzystywane przy współdzieleniu plików często pozostawiają wiele otwartych połączeń, które mogą zużywać dostępne pasmo. W rezultacie zaobserwujesz znacznie wolniejsze ładowanie stron podczas przeglądania internetu.

- ***Nieznana sieć o znajomej nazwie***. Dotyczy to zazwyczaj jedynie użytkowników, którzy korzystają z różnych sieci na swoich komputerach przenośnych: jeśli nieznana sieć będzie miała podobną nazwę do dobrze znanej *(np. "Dom" lub "MojeWiFi")*, możesz przez przypadek połączyć się z potencjalnie niebezpieczną siecią. ***Doradca AVG*** może Cię przed tym uchronić, ostrzegając, że pod zaufaną nazwą kryje się nieznana sieć. Oczywiście jeśli stwierdzisz, że nowa sieć jest bezpieczna, możesz zachować ją na prowadzonej przez ***Doradcę AVG*** liście znanych sieci, aby w przyszłości nie była już ona raportowana.

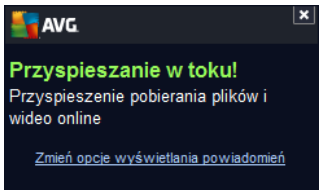
W każdej z tych sytuacji ***Doradca AVG*** ostrzeże Cię przed nadchodzącym problemem i wyświetli ikonę oraz nazwę procesu, którego on dotyczy. ***Doradca AVG*** sugeruje również kroki, które należy podjąć, by uniknąć problemu.

Obsługiwane przeglądarki internetowe

Funkcja ta współpracuje z następującymi przeglądarkami: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

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



6. Składniki AVG

6.1. Ochrona komputera

Składnik ***Komputer*** świadczy dwie podstawowe usługi dotyczące bezpieczeństwa: ***AntiVirus*** i ***Data Safe***:

- ***AntiVirus*** składa się z silnika skanującego, który chroni wszystkie pliki, obszary komputera oraz urządzenia wymienne *(dyski flash, itd)* poszukując 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, nieznany wirus, jeśli zawiera on pewne cechy znane z istniejących wirusów. **AVG Internet Security 2014** jest również w stanie analizować i wykrywać wykonywalne aplikacje i biblioteki DLL, które mogą być potencjalne niepożądane w Twoim systemie *(różne rodzaje oprogramowania szpiegującego, reklamowego itd)*. 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.

- ***Funkcja Data Safe*** pozwala na tworzenie wirtualnych sejfów służących do przechowywania ważnych lub poufnych danych. Zawartość sejfów funkcji Data Safe jest szyfrowana wybranym przez użytkownika hasłem, tak aby nikt nie mógł jej zobaczyć bez autoryzacji.

Elementy okna

Aby przełączyć się między dwoma sekcjami okna, możesz po prostu kliknąć gdziekolwiek w obszarze odpowiedniego panelu. Panel zostanie wówczas podświetlony jasnoniebieskim kolorem. W obu sekcjach okna znajdują się następujące przyciski kontrolne: Ich działanie jest takie samo,

niezależnie od funkcji, do której należą *(AntiVirus lub File Vaults)*:

 ***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 AntiVirus jest aktywna i w pełni funkcjonalna. Kolor czerwony reprezentuje stan ***Wyłączony***, co oznacza, że usługa jest nieaktywna. Jeśli nie posiadasz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli z pewnych powodów zechcesz wyłączyć usługę, zostaniesz natychmiast ostrzeżony o możliwym ryzyku poprzez czerwony znak ***Ostrzeżenia*** oraz informację o chwilowym braku pełnej ochrony. ***Prosimy pamiętać o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!***

 ***Ustawienia*** – Kliknij ten przycisk, by zostać przeniesionym do interfejsu Ustawień zaawansowanych. Dokładniej, zostanie otworzone odpowiednie okno, w którym będziesz mógł skonfigurować wybraną usługę, np. AntiVirus. W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład **AVG Internet Security 2014**, lecz polecamy to jedynie doświadczonym użytkownikom!

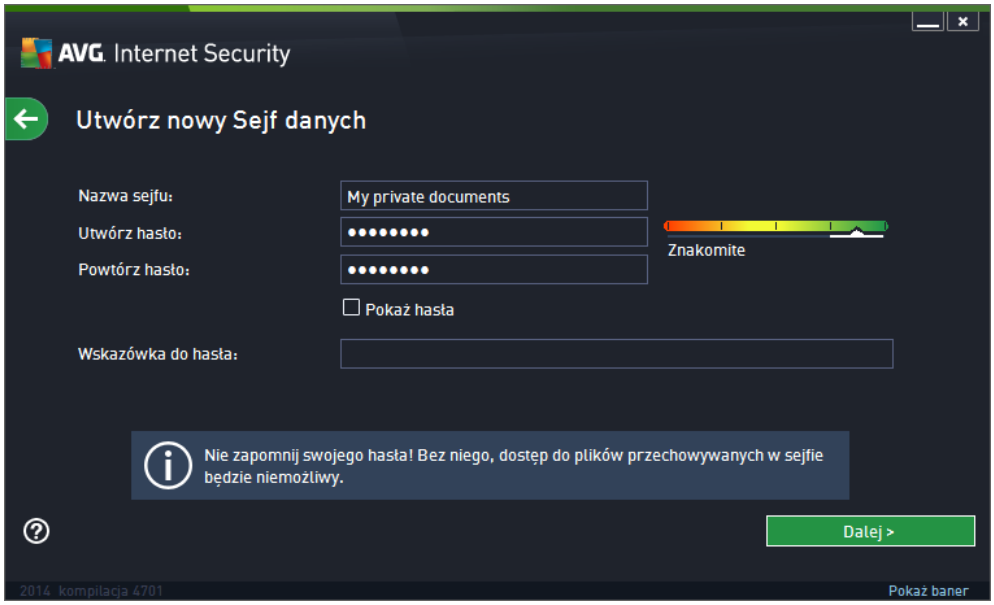
 ***Statystyki*** – Kliknij ten przycisk, by zostać przeniesionym do dedykowanej strony AVG (*http://www.avg.com/*). Znajdziesz na niej statystyczne podsumowanie wszystkich działań systemu **AVG Internet Security 2014** prowadzonych na Twoim komputerze w ostatnim okresie, oraz od momentu instalacji.

 ***Szczegóły*** – Kliknij ten przycisk, aby w dolnej części okna wyświetlić krótki opis wybranej usługi.

 – Użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do głównego interfejsu użytkownika z przeglądem składników.

Tworzenie własnego sejfu danych

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



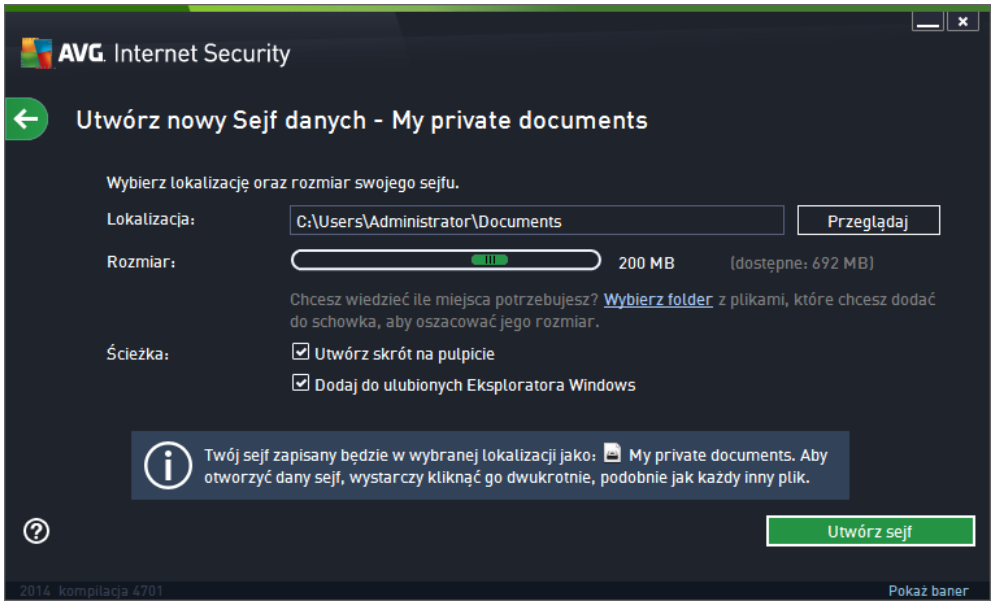
Po pierwsze, należy określić nazwę sejfu i utworzyć silne hasło:

- ***Nazwa sejfu*** – Aby utworzyć nowy sejf danych, należy najpierw wybrać odpowiednią nazwę sejfu, aby go rozpoznać. Jeśli korzystasz z tego samego komputera, co reszta członków rodziny, możesz podać zarówno swoje imię, jak również wskazówkę zawartości sejfu, na przykład *Wiadomości e-mail taty*.

- ***Utwórz hasło/Powtórz hasło*** – Wymyśl hasło dla swojego sejfu danych i wpisz je w odpowiednie pola tekstowe. Wskaźnik graficzny znajdujący się po prawej stronie informuje użytkownika, czy hasło jest słabe *(stosunkowo łatwe do złamania przy pomocy specjalnych narzędzi)* czy też silne. Zalecamy stosowanie haseł o przynajmniej średnim stopniu bezpieczeństwa. Możesz sprawić, iż Twoje hasło będzie silniejsze, poprzez stosowanie dużych liter, cyfr i innych znaków takich jak kropki, myślniki, itp. Jeżeli chcesz mieć pewność, że wprowadzasz prawidłowe hasło, możesz zaznaczyć pole ***Pokaż hasło*** *(oczywiście, jeśli nikt inny nie patrzy wtedy na Twój monitor)*.

- ***Wskazówka do hasła*** – Zalecamy także utworzenie pomocnej wskazówki do hasła, która pozwoli Ci je sobie przypomnieć. Należy pamiętać, że funkcja Data Safe chroni Twoje pliki i umożliwia do nich dostęp wyłącznie przy pomocy hasła; nie można tego obejść, więc jeśli zapomnisz swojego hasła, nie będziesz mógł odzyskać 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:

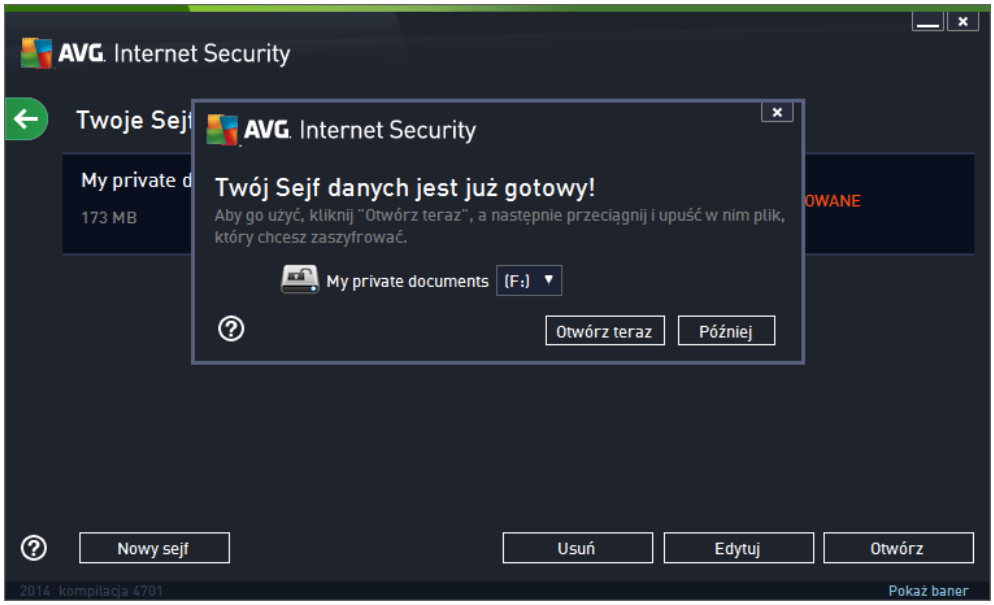
- ***Lokalizacja*** określa, gdzie dany sejf zostanie umieszczony. Wybierz odpowiednie miejsce na swoim dysku twardym lub pozostaw lokalizację domyślną, czyli folder *Dokumenty*. Pamiętaj, że po utworzeniu sejfu danych, jego lokalizacja nie może zostać zmieniona.

- ***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)*, czy też zbyt duża *(zabierająca niepotrzebnie za dużo miejsca na dysku)*. Jeśli 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. Jednakże, rozmiar ten może zostać później zmieniony w zależności od potrzeb użytkownika.

- ***Dostęp*** – pola wyboru w tej sekcji umożliwiają tworzenie wygodnych skrótów do sejfów danych.

Korzystanie z Sejfu danych

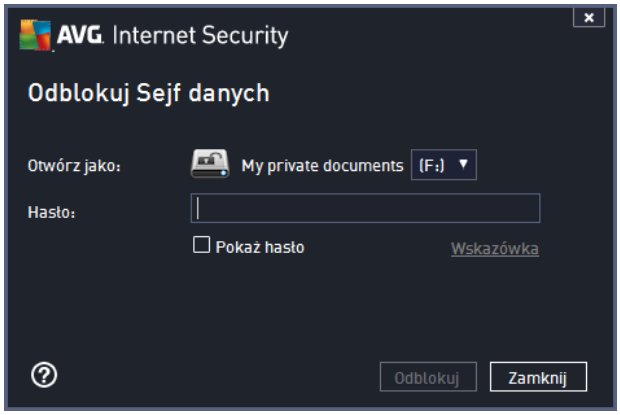
Gdy zakończysz konfigurowanie ustawień, kliknij przycisk ***Utwórz sejf***. Zostanie otwarte nowe okno dialogowe ***Twój Sejf danych jest już gotowy***, informujące o dostępności sejfu do przechowywania w nim danych. W tej chwili sejf jest otwarty i możesz się do niego od razu dostać. Przy kolejnych 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 dowolną literę z menu rozwijanego (*do wyboru będą tylko aktualnie nie używane dyski*). Zazwyczaj niedozwolone są litery takie jak: C *(przypisana jest ona 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:



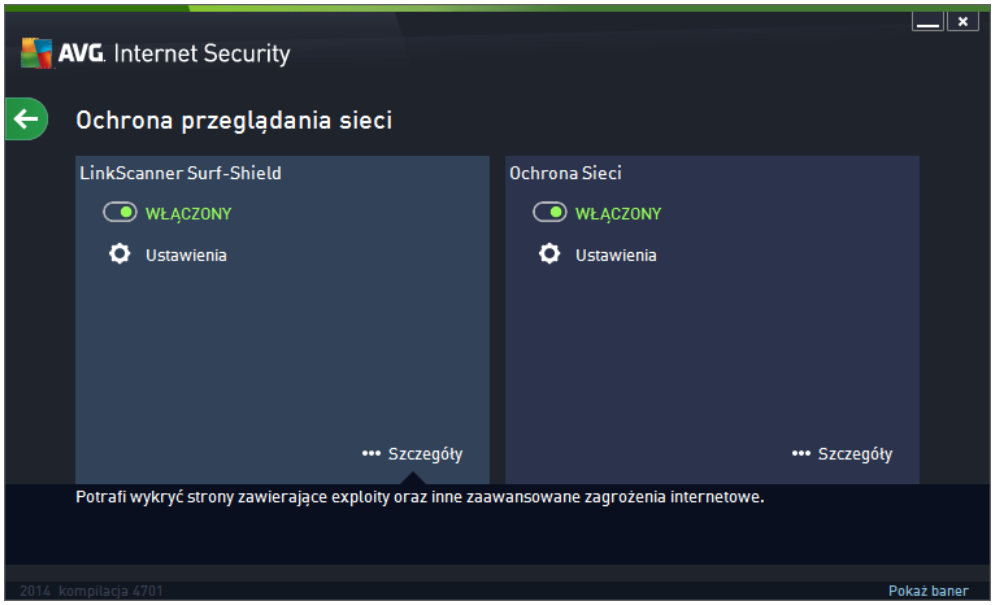
Wpisz hasło w polu tekstowym, aby dokonać autoryzacji, a następnie kliknij przycisk ***Odblokuj***. Jeśli potrzebujesz pomocy w przypomnieniu sobie hasła, kliknij opcję ***Wskazówka***, aby wyświetlić podpowiedź dotyczącą hasła utworzoną podczas tworzenia sejfu danych. Nowy sejf danych będzie widoczny w przeglądzie Twoich sejfów danych jako ODBLOKOWANY i możliwe będzie dodawanie do niego plików oraz ich usuwanie.

6.2. Ochrona przeglądania sieci

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

- ***LinkScanner Surf-Shield*** to funkcja zapewniająca ochronę przed rosnącą liczbą zagrożeń internetowych. Zagrożenia te mogę być ukryte na stronie internetowej każdego typu (od stron rządowych przez witryny dużych i znanych marek, a kończąc na stronach małych firm). Rzadko kiedy pozostają tam dłużej niż 24 godziny. Składnik LinkScanner zapewnia nadzwyczaj skuteczną ochronę, skanując wszystkie łącza znajdujące się na każdej przeglądanej stronie. Robi to dokładnie wtedy, gdy ma to największe znaczenie – zanim zdecydujesz się je kliknąć. ***Funkcja LinkScanner Surf-Shield nie jest przeznaczona dla platform serwerowych!***

- ***Ochrona Sieci*** to rodzaj programu rezydentnego, zapewniającego ochronę w czasie rzeczywistym. Składnik ten skanuje zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików), jeszcze zanim zostaną załadowane przez przeglądarkę lub pobrane na dysk twardy. Ochrona Sieci wykrywa strony zawierające niebezpieczny kod javascript i blokuje ich ładowanie. Ponadto, identyfikuje szkodliwe oprogramowanie zawarte na stronach WWW i w razie podejrzeń zatrzymuje pobieranie, aby nie dopuścić do infekcji komputera. Ta zaawansowana funkcja ochrony blokuje szkodliwą zawartość dowolnej otwieranej witryny internetowej, zapobiegając pobraniu jej na komputer. Gdy jest ona włączona, kliknięcie jakiegokolwiek linku lub wpisanie adresu URL prowadzącego do niebezpiecznej witryny spowoduje automatyczne zablokowanie strony, dzięki czemu komputer nie zostanie nieświadomie zainfekowany. Warto zapamiętać, że infekcja może przedostać się na Twój komputer z zainfekowanej witryny nawet podczas zwykłych odwiedzin na stronie internetowej. ***Ochrona Sieci nie jest przeznaczona dla platform serwerowych!***



Elementy okna

Aby przełaczyć się między dwoma sekcjami okna, możesz po prostu kliknąć gdziekolwiek w obszarze odpowiedniego panelu. Panel zostanie wówczas podświetlony jasnoniebieskim kolorem.

W obu sekcjach okna znajdują się następujące przyciski kontrolne: Ich funkcjonalność jest identyczna, niezależnie od usługi, której dotyczą *(LinkScanner Surf-Shield lub Ochrona Sieci)*:

 ***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 LinkScanner Surf-Shield / Ochrona Sieci jest aktywna i w pełni funkcjonalna. Kolor czerwony reprezentuje stan ***Wyłączony***, co oznacza, że usługa nie jest aktywna. Jeśli nie posiadasz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli z pewnych powodów zechcesz wyłączyć usługę, zostaniesz natychmiast ostrzeżony o możliwym ryzyku poprzez czerwony znak ***Ostrzeżenia*** oraz informację o chwilowym braku pełnej ochrony. ***Prosimy pamiętać o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!***

 ***Ustawienia*** – Kliknij ten przycisk, by zostać przeniesionym do interfejsu Ustawień zaawansowanych. Dokładniej, zostanie otworzone odpowiednie okno, w którym będziesz mógł skonfigurować wybraną usługę, tj. LinkScanner Surf-Shield lub Ochrona Sieci. W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład **AVG Internet Security 2014**, lecz polecamy to jedynie doświadczonym użytkownikom!

 ***Szczegóły*** – Kliknij ten przycisk, aby w dolnej części okna wyświetlić krótki opis wybranej usługi.

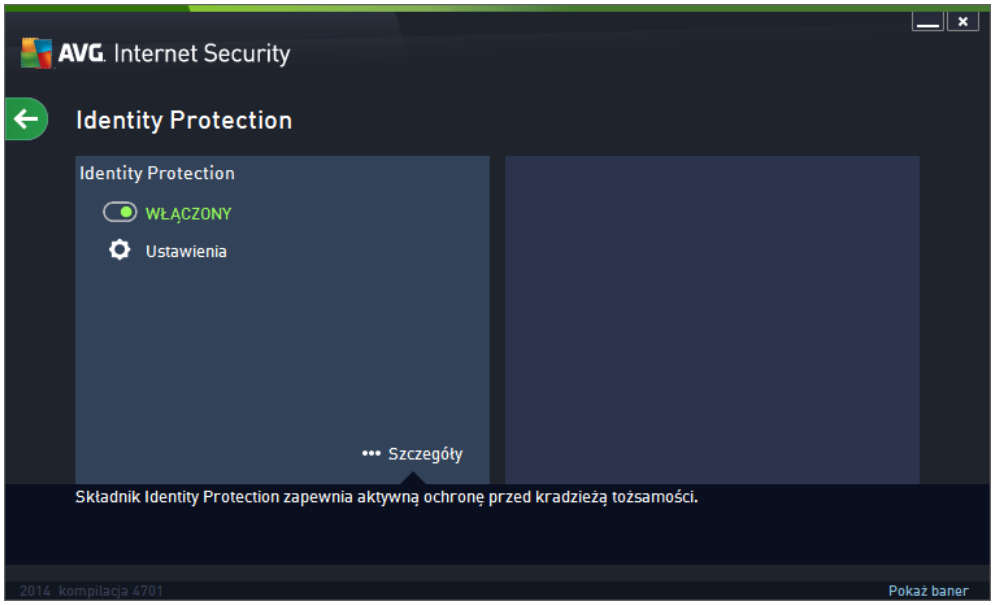
 – Użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do głównego interfejsu użytkownika z przeglądem składników.

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, zapewniając ochronę przed wszystkimi jego rodzajami (*jak np. programami szpiegującymi, botami, kradzieżami tożsamości itp.*), używając technologii behawioralnych. Identity Protection to usługa, której głównym zadaniem jest zapobieganie kradzieżom tożsamości (w wyniku kradzieży haseł, rachunków bankowych, numerów kart kredytowych i innych cennych danych) przez szkodliwe oprogramowanie (*malware*). Zapewnia poprawne działanie wszystkich programów uruchomionych na Twoim komputerze i w sieci lokalnej. Identity Protection wykrywa i blokuje podejrzane zachowanie (dzięki stałemu nadzorowi), a także chroni komputer przed nowym szkodliwym oprogramowaniem. Składnik Identity Protection zapewnia komputerowi ochronę w czasie rzeczywistym przeciw nowym, a nawet nieznanym zagrożeniom. Monitoruje 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 w komputerze pojawi się nieznany kod programu, jest on natychmiast obserwowany i monitorowany pod kątem szkodliwego zachowania. Jeśli dany plik zostanie uznany za szkodliwy, składnik Identity Protection przeniesie jego kod do Przechowalni wirusów i cofnie wszelkie zmiany wprowadzone w systemie

(ingerencje w inne programy, 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 tym oknie możesz znaleźć 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 posiadasz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli z pewnych powodów zechcesz wyłączyć usługę, zostaniesz natychmiast ostrzeżony o możliwym ryzyku poprzez czerwony znak ***Ostrzeżenia*** oraz informację o chwilowym braku pełnej ochrony. ***Prosimy pamiętać o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!***

Ustawienia – Kliknij ten przycisk, by zostać przeniesionym do interfejsu Ustawień zaawansowanych. Dokładniej, zostanie otworzone odpowiednie okno, w którym będziesz mógł skonfigurować wybraną usługę, tj. Identity Protection. W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład **AVG Internet Security 2014**, lecz polecamy to jedynie doświadczonym użytkownikom!

Szczegóły – Kliknij ten przycisk, aby w dolnej części okna wyświetlić krótki opis wybranej usługi.

– Użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do głównego interfejsu

użytkownika z przeglądem składników.

Niestety, produkt **AVG Internet Security 2014** nie zawiera usługi Identity Alert. Jeśli interesuje Cię ochrona tego typu, kliknij przycisk ***Uaktualnij, aby aktywować***. Nastąpi przeniesienie do specjalnej strony umożliwiającej zakup licencji Identity Alert.

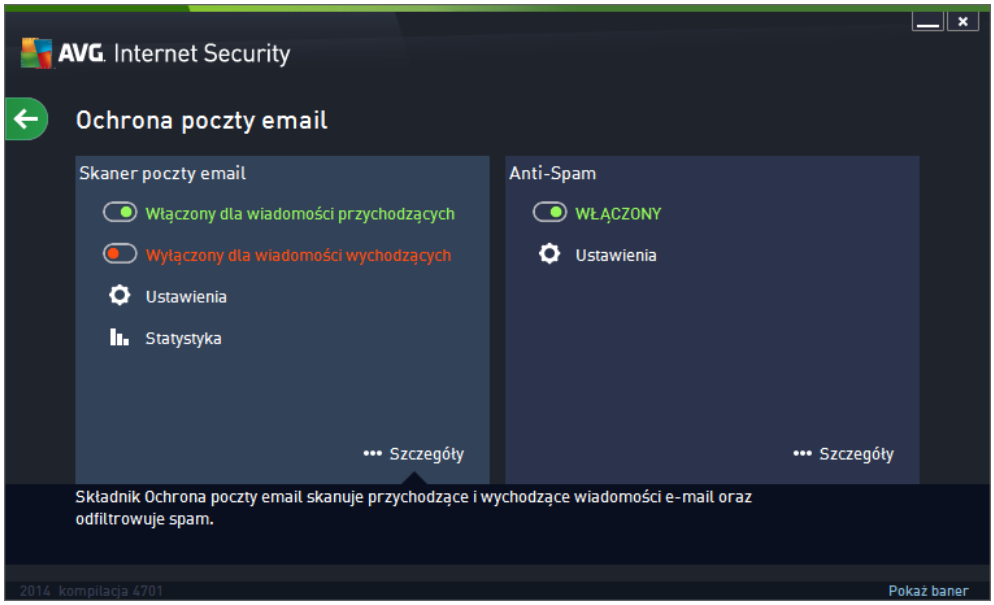
Przypominamy, że nawet w przypadku edycji AVG Premium Security usługa Identity Alert jest obecnie dostępna jedynie na wybranych obszarach: w Stanach Zjednoczonych, Wielkiej Brytanii, Kanadzie i Irlandii.

6.4. Ochrona poczty email

Składnik ***Ochrona poczty e-mail*** świadczy następujące usługi zabezpieczające: ***Skaner poczty e-mail*** i ***Anti-Spam***:

- ***Skaner poczty email***: Poczta e-mail to od dawna częste źródło wirusów i koni trojańskich. Wyłudzenia danych i spam powodują, że stała się ona jeszcze większym zagrożeniem. Darmowe konta pocztowe są szczególnie narażone na otrzymywanie szkodliwych wiadomości e-mail, *gdyż rzadko korzystają z technologii antyspamowych*, a domowi użytkownicy najczęściej używają właśnie takich kont. Dodatkowo odwiedzają oni nieznane witryny i wpisują w formularzach dane osobowe (*takie jak adres e-mail*), co powoduje, że w jeszcze większym stopniu narażają się na ataki za pośrednictwem poczty e-mail. Firmy na ogół używają komercyjnych kont pocztowych które, w celu ograniczenia ryzyka, korzystają z filtrów antyspamowych itp. Składnik Ochrona poczty email jest odpowiedzialny za skanowanie wszystkich wiadomości e-mail, zarówno wysyłanych, jak i otrzymywanych. Każdy wirus wykryty w wiadomości jest natychmiast przenoszony do Przechowalni. Skaner poczty może odfiltrowywać określone typy załączników i dodawać do wiadomości tekst certyfikujący brak infekcji. ***Skaner poczty Email 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 do wielu skrzynek pocztowych, zapychając je. Spamem nie jest korespondencja seryjna rozsyłana do odbiorców po wyrażeniu przez nich zgody.)*. Składnik Anti-Spam może modyfikować temat wiadomości e-mail (*wykrytej jako SPAM*), dodając do niego specjalny ciąg tekstowy. Dzięki temu możliwe jest łatwe filtrowanie 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 do wykrywania spamu korzysta z regularnie aktualizowanej bazy danych. Można także użyć zdefiniowanych serwerów RBL (*publicznych baz adresów znanych nadawców spamu*) lub ręcznie dodać adresy do białej listy (*nigdy nieoznaczanej jako spam*) lub czarnej listy (*zawsze oznaczanej jako spam)*.



Elementy okna

Aby przełaczyć się między dwoma sekcjami okna, możesz po prostu kliknąć gdziekolwiek w obszarze odpowiedniego panelu. Panel zostanie wówczas podświetlony jasnoniebieskim kolorem. W obu sekcjach okna znajdują się następujące przyciski kontrolne: Ich funkcjonalność jest taka sama, niezależnie od tego, do której usługi się odnoszą *(Skaner poczty email lub Anti-Spam)*:

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 jest aktywna i w pełni funkcjonalna. Kolor czerwony reprezentuje stan ***Wyłączony***, co oznacza, że usługa jest nieaktywna. Jeśli nie posiadasz poważnego powodu do wyłączenia usługi, stanowczo zalecamy pozostawienie domyślnych wartości wszystkich ustawień dotyczących bezpieczeństwa. Ustawienia domyślne zapewniają optymalną wydajność aplikacji oraz maksymalne bezpieczeństwo. Jeśli z pewnych powodów zechcesz wyłączyć usługę, zostaniesz natychmiast ostrzeżony o możliwym ryzyku poprzez czerwony znak ***Ostrzeżenia*** oraz informację o chwilowym braku pełnej ochrony. ***Prosimy pamiętać o ponownym aktywowaniu usługi tak szybko, jak to będzie możliwe!***

W sekcji Skanera poczty Email można znaleźć dwa przyciski przypominające sygnalizację świetlną. Dzięki temu możesz osobno określić, czy chcesz, aby Skaner poczty email sprawdzał wiadomości przychodzące, wychodzące, czy wszystkie. Domyślnie skanowane są tylko wiadomości przychodzące, a wiadomości wychodzące są pomijane, ze względu na niskie ryzyko infekcji.

Ustawienia – Kliknij ten przycisk, by zostać przeniesionym do interfejsu Ustawień zaawansowanych. Dokładniej, zostanie otworzone odpowiednie okno, w którym będziesz mógł skonfigurować wybraną usługę, tj. Skaner poczty e-mail lub Anti-Spam. W interfejsie Ustawień zaawansowanych można edytować konfigurację wszystkich usług zabezpieczających wchodzących w skład **AVG Internet Security 2014**, lecz polecamy to jedynie doświadczonym użytkownikom!

Statystyki – Kliknij ten przycisk, by zostać przeniesionym do dedykowanej strony AVG (http://www.avg.com/). Znajdziesz na niej statystyczne podsumowanie wszystkich działań systemu **AVG Internet Security 2014** prowadzonych na Twoim komputerze w ostatnim okresie, oraz od momentu instalacji.

Szczegóły – Kliknij ten przycisk, aby w dolnej części okna wyświetlić krótki opis wybranej usługi.

– Użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do głównego interfejsu użytkownika z przeglądem składników.

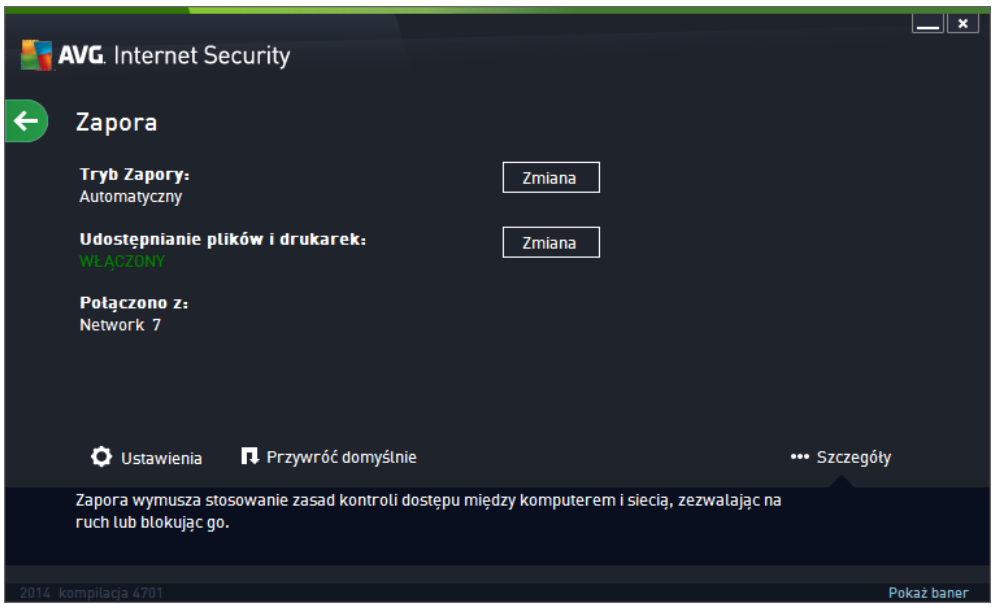
6.5. Zapora

Zapora internetowa to system, który wymusza stosowanie zasad kontroli dostępu między dwoma lub większą liczbą sieci, blokując lub umożliwiając przepływ danych. Zapora składa się z zestawu reguł, które sterują komunikacją na każdym indywidualnym porcie sieciowym, chroniąc w ten sposób sieć lokalną przed atakami, których źródło znajduje się na zewnątrz (zazwyczaj w internecie). Komunikacja jest oceniana (w oparciu o zdefiniowane reguły), a następnie akceptowana lub blokowana. Jeśli Zapora wykryje próbę ataku, blokuje ją i nie pozwala intruzowi przejąć kontroli nad komputerem. Konfiguracja Zapory pozwala blokować lub dopuszczać komunikację wewnętrzną lub zewnętrzną *(zarówno wychodzącą, jak i przychodzącą)* na konkretnych portach i dla zdefiniowanych programów. Zapora może np. akceptować tylko ruch WWW, z którego korzysta program Microsoft Internet Explorer. Próba transmisji danych WWW przez jakąkolwiek inną przeglądarkę będzie w takim przypadku blokowana. Zapora chroni również Twoje dane osobowe – nikt nie uzyska ich bez Twojej wyraźnej zgody. Decyduje też o tym, jak wymieniane są dane z innymi komputerami w sieci lokalnej lub internecie. Zapora w środowisku komercyjnym chroni również pojedyncze komputery przed atakami przeprowadzanymi z wnętrza tej samej sieci.

W systemie **AVG Internet Security 2014**, ***Zapora*** kontroluje cały ruch na każdym porcie sieciowym komputera. Na podstawie zdefiniowanych reguł Zapora *ocenia uruchomione aplikacje (chcące nawiązać połączenie z siecią lokalną lub internetem) 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 nieznana *(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!

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



Uwaga: *Po zainstalowaniu programu AVG Internet Security 2014 składnik Zapory może wymagać ponownego uruchomienia komputera. W takim przypadku zostanie wyświetlone okno dialogowe składnika z informacją o konieczności ponownego uruchomienia. W wyświetlonym oknie dialogowym znajduje się przycisk* ***Uruchom ponownie teraz****. Do czasu ponownego uruchomienia składnik Zapory 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 w oparciu o środowisko i tryb pracy komputera. Każda z opcji wymaga innego poziomu zabezpieczeń, 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 będziesz proszony o podejmowanie jakichkolwiek decyzji. Zapora zezwoli na połączenia wszystkich znanych aplikacji, tworząc jednocześnie reguły umożliwiające im nawiązywanie połączeń w przyszłości. Dla innych aplikacji, Zapora zdecyduje, czy pozwolić na komunikację, na podstawie analizy behawioralnej aplikacji. W takich przypadkach nie utworzy ona jednak reguły, więc aplikacja będzie sprawdzana przy każdorazowej próbie połączenia. Tryb automatyczny nie narzuca się i jest polecany większości użytkowników.

- ***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. Zalecane tylko dla użytkowników zaawansowanych.

- ***Blokuj dostęp do internetu*** – Połączenie z internetem będzie całkowicie zablokowane, nie będzie można dostać się do internetu, a także nikt z zewnątrz nie będzie mógł się dostać do komputera. Tylko do stosowania wyjątkowego i tymczasowego.

- ***Wyłącz Zaporę (niezalecane)*** – wyłączenie Zapory zezwoli na cały ruch przychodzący i

wychodzący do i z komputera. W rezultacie stanie się on podatny na ataki hakerów. Prosimy o stosowanie tej opcji ze rozwagą.

Należy zwrócić uwagę na specyficzny, automatyczny tryb pracy Zapory. Tryb ten jest aktywowany w tle za każdym razem, gdy składnik Komputer lub Identity Protection zostanie wyłączony, co naraża Twój komputer na zwiększone niebezpieczeństwo. W takim przypadku Zapora zezwoli automatycznie jedynie na ruch sieciowy znanych i absolutnie bezpiecznych aplikacji. We wszystkich pozostałych przypadkach będziesz pytany o decyzję. Służy to zrównoważeniu ryzyka spowodowanego wyłączonymi składnikami i jest sposobem na zachowanie bezpieczeństwa Twojego komputera.

Elementy okna

W tym oknie jest wyświetlany przegląd informacji o bieżącym stanie składnika Zapora:

- ***Tryb Zapory*** – Informuje o obecnie wybranym trybie Zapory. Użyj przycisku ***Zmień*** znajdującego się obok podanej informacji, aby przejść do interfejsu Ustawień Zapory i zmienić bieżący tryb na inny *(opis i zalecenia dotyczące profili Zapory znajdują się w poprzednim akapicie)*.

- ***Udostępnianie plików i drukarek*** – Informuje Cię o tym, czy udostępnianie plików i drukarek *(w obu kierunkach)* jest obecnie dozwolone. 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 obiektów jest pożądane jedynie w sieciach uważanych za bezpieczne *(np. w domu, w pracy lub w szkole)*. Jeśli jednak połączony jesteś z siecią publiczną *(jak np. Wi-Fi na lotnisku lub w kawiarence internetowej)*, najprawdopodobniej nie chcesz czegokolwiek udostępniać.

- ***Połączony z*** – Podaje nazwę sieci, z którą jesteś obecnie połączony. W systemie Windows XP nazwa sieci odpowiada nazwie wybranej dla danej sieci podczas pierwszego połączenia z nią. W systemie Windows Vista i nowszych, nazwa sieci pobierana jest automatycznie z Centrum Sieci i Udostępniania.

To okno zawiera następujące przyciski:

Zmień – Ten przycisk umożliwia zmianę stanu odpowiedniego parametru. Szczegóły dotyczące zmiany parametrów znajdują się w powyższym akapicie.

Ustawienia – Kliknij ten przycisk, by zostać przeniesionym do interfejsu Ustawień Zapory, który umożliwia edycję pełnej konfiguracji Zapory. Wszelkie zmiany konfiguracji powinny być wprowadzane wyłącznie przez doświadczonych użytkowników!

Przywróć domyślne – ten przycisk umożliwia nadpisanie bieżącej konfiguracji Zapory i przywrócenie konfiguracji domyślnej (na podstawie automatycznego wykrywania).

Szczegóły – Kliknij ten przycisk, aby w dolnej części okna wyświetlić krótki opis wybranej usługi.

– Użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do głównego interfejsu

użytkownika z przeglądem składników.

6.6. Składnik Quick Tune

Składnik ***Quick Tune*** stanowi zaawansowane narzędzie przeznaczone do prowadzania szczegółowej analizy i modyfikacji ustawień systemu, aby zwiększyć szybkość i efektywność działania komputera. Uruchamiane jest ono z głównego interfejsu użytkownika poprzez opcję ***Popraw wydajność*** :

Przeanalizowane i naprawione mogą zostać problemy z następujących kategorii: błędy rejestru, pliki-śmieci, fragmentacja i błędne skróty:

- ***Błędy rejestru*** – określa liczbę błędów rejestru systemu Windows, które mogą powodować wolniejsze działanie komputera lub wyświetlanie komunikatów o błędach.
- ***Pliki-śmieci*** – określa liczbę zbędnych plików, które zajmują miejsce na dysku. Zazwyczaj są to różnego rodzaju pliki tymczasowe oraz pliki znajdujące się w Koszu.
- ***Fragmentacja*** – umożliwia obliczenie procentowego stopnia fragmentacji danych na dysku twardym (po upływie dłuższego czasu wiele plików może ulec rozproszeniu po różnych sektorach dysku fizycznego).
- ***Błędne skróty*** – wykrywa niedziałające skróty prowadzące do nieistniejących lokalizacji itd.

Aby uruchomić analizę systemu, kliknij przycisk ***Analizuj teraz***. Postęp analizy oraz jej wyniki będzie można obserwować bezpośrednio na wykresie:

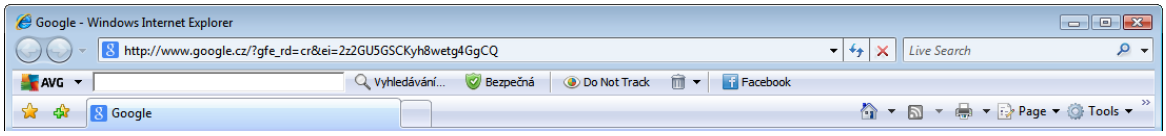
Podgląd wyników zawiera ilość wykrytych problemów systemowych, sklasyfikowanych według odpowiednich kategorii. Wyniki analizy będą również wyświetlane w postaci graficznej na osi w kolumnie ***Poziom zagrożenia***.

Przyciski kontrolne

- ***Analizuj teraz*** (*wyświetlany przed uruchomieniem analizy*) – kliknięcie tego przycisku umożliwia uruchomienie natychmiastowej analizy komputera.
- ***Napraw teraz*** *(wyświetlany po zakończeniu analizy*) – kliknięcie tego przycisku powoduje rozpoczęcie naprawy wszystkich wykrytych błędów. Przegląd wyników zostanie wyświetlony zaraz po ukończeniu tego procesu.
- ***Anuluj*** – użyj tego przycisku, by zakończyć bieżącą analizę lub powrócić do domyślnego okna AVG (*Przeglądu składników*) po jej zakończeniu.

7. AVG Security Toolbar

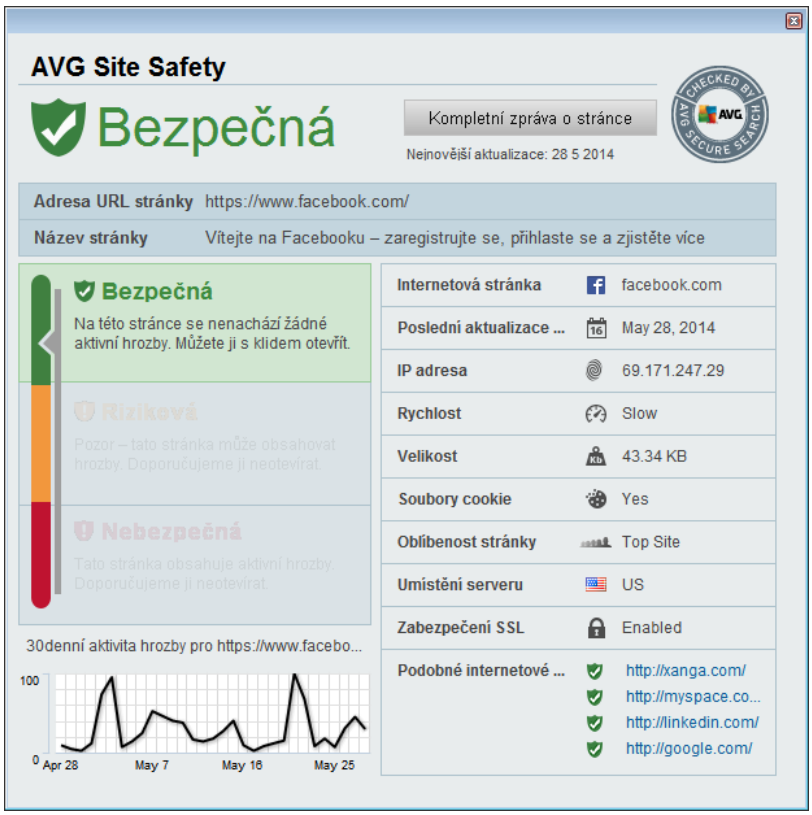
AVG Security Toolbar to narzędzie ściśle współpracujące z funkcją Surf-Shield składnika LinkScanner. Jego zadaniem jest zapewnienie maksymalnego bezpieczeństwa podczas przeglądania internetu. Proces instalacji systemu **AVG Internet Security 2014** pozwala Ci zdecydować, czy chcesz zainstalować ***AVG Security Toolbar***. ***AVG Security Toolbar*** dostępny jest bezpośrednio z poziomu przeglądarki internetowej. Obecnie obsługiwane przeglądarki to: Internet Explorer (*wersja 6.0 i nowsze*), oraz Mozilla Firefox (*wersja 3.0 i nowsze*). Nie gwarantujemy działania naszego paska narzędzi w innych przeglądarkach *(jeżeli używasz jednej z alternatywnych przeglądarek, np. Avant Browser, może wystąpić jej nieprzewidziane zachowanie).*



AVG Security Toolbar składa się z następujących elementów:

- ***Logo AVG*** wraz z menu rozwijanym:
  - ***Obecny poziom zagrożenia*** – otwiera stronę internetową laboratorium wirusów, która zawiera graficzną reprezentację obecnego poziomu zagrożeń w sieci.
  - ***Laboratoria AVG Threat Labs*** – otwiera stronę internetową ***AVG Threat Labs*** *(pod adresem http://www.avgthreatlabs.com)*, na której znaleźć można informacje na temat zabezpieczeń witryn internetowych oraz ogólnego poziomu bezpieczeństwa w sieci.
  - ***Toolbar – Pomoc*** – otwiera podręcznik online opisujący wszystkie funkcje paska ***AVG Security Toolbar***.
  - ***Prześlij opinię o produkcie*** – otwiera formularz internetowy, który pozwoli Ci wyrazić swoją opinię o ***AVG Security Toolbar***.
  - ***Umowa licencyjna użytkownika końcowego*** – powoduje otwarcie strony AVG, na której dostępny jest pełny tekst umowy licencyjnej związanej z użytkowaniem programu **AVG Internet Security 2014**.
  - ***Polityka prywatności*** – powoduje otwarcie strony AVG, na której znaleźć można pełny tekst Polityki prywatności AVG.
  - ***Odinstaluj AVG Security Toolbar*** – otwiera stronę internetową zawierającą szczegółowe instrukcje wyłączenia paska ***AVG Security Toolbar*** w każdej z obsługiwanych przeglądarek.
  - ***Informacje...*** – otwiera okno zawierające szczegóły dotyczące zainstalowanej wersji paska ***AVG Security Toolbar***.
- ***Pole wyszukiwania*** – szukaj informacji przy użyciu paska ***AVG Security Toolbar***, aby mieć pewność, że wszystkie wyświetlone wyniki są w stu procentach bezpieczne. Wprowadź słowo lub frazę i kliknij przycisk ***Szukaj*** *(lub użyj klawisza Enter)*.
- ***Bezpieczeństwo strony*** – ten przycisk otwiera nowe okno informujące o aktualnym

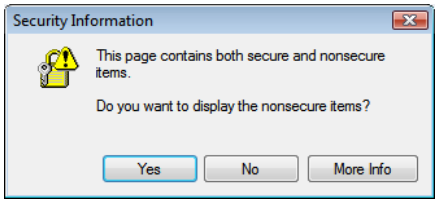
poziomie bezpieczeństwa odwiedzanej przez Ciebie strony (*Bezpieczna*). Ten krótki przegląd można rozwinąć, aby wyświetlić w nim szczegóły wszystkich operacji związanych z bezpieczeństwem danej witryny (*Pełny raport strony*):



- ***Do Not Track*** – usługa DNT pozwala Ci zidentyfikować witryny internetowe, które gromadzą dane o Twojej aktywności online, a także je zablokować. Szczegóły >>

- ***Usuń*** – przycisk z ikoną kosza otwiera menu zawierające opcje umożliwiające usunięcie historii przeglądania, pobierania, formularzy online i wyszukiwania.

- ***Pogoda*** – Przycisk otwierający nowe okno, które zawiera informacje o bieżącej pogodzie (w miejscu Twojego pobytu) oraz prognozie na najbliższe 2 dni. Informacje te są na bieżąco aktualizowane (co 3-6 godzin). Okno pogody umożliwia również ręczną zmianę bieżącej lokalizacji oraz wybór między stopniami Celsjusza a Fahrenheita.



- ***Facebook*** – Przycisk pozwalający na bezpośrednie połączenie z portalem Facebook z poziomu paska ***AVG Security Toolbar***

- Skróty umożliwiające szybki dostęp do aplikacji takich jak: ***Kalkulator***, ***Notatnik***, ***Eksplorator Windows***.

8. AVG Do Not Track

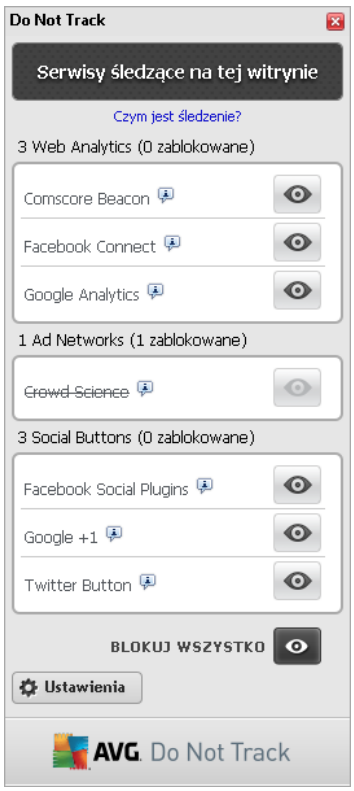
AVG Do Not Track pozwala Ci zidentyfikować witryny internetowe, które zbierają dane o Twojej aktywności online. Funkcja ***AVG Do Not Track,*** będąca częścią paska narzędzi AVG Security Toolbar, wskazuje strony internetowe lub reklamodawców, którzy gromadzą dane o Twojej aktywności online, a także pozwala Ci zdecydować, które z nich chcesz zablokować.

- ***AVG Do Not Track*** dostarcza szczegółowych informacji o polityce prywatności każdego serwisu, a także podaje bezpośredni link umożliwiający rezygnacje z usług danego reklamodawcy, o ile to możliwe.
- Dodatkowo, ***AVG Do Not Track*** obsługuje protokół W3C DNT, za pomocą którego może automatycznie powiadamiać odwiedzane witryny o braku Twojej zgody na śledzenie aktywności. Powiadamianie W3C DNT jest domyślnie włączone, lecz w dowolnym momencie można zmienić to ustawienie.
- ***Dla AVG Do Not Track*** obowiązują następujące warunki korzystania z usługi.
- ***Funkcja AVG Do Not Track*** jest domyślnie włączona, ale w dowolnym momencie możesz ją wyłączyć. Stosowne instrukcje można znaleźć w temacie FAQ Wyłączanie funkcji AVG Do Not Track.
- Więcej informacji na temat ***AVG Do Not Track*** można znaleźć na naszej stronie internetowej.

Obecnie funkcja ***AVG Do Not Track*** obsługiwana jest przez przeglądarki Mozilla Firefox, Chrome i Internet Explorer.

8.1. Interfejs AVG Do Not Track

Gdy przeglądasz internet, funkcja ***AVG Do Not Track*** ostrzeże Cię, gdy tylko wykryje jakąkolwiek aktywność polegającą na gromadzeniu Twoich danych. W takim wypadku ikona ***AVG Do Not Track*** znajdująca się na pasku AVG Security Toolbar zmienia swój wygląd; pojawia się obok niej niewielka liczba oznaczająca liczbę wykrytych serwisów gromadzących dane:  Kliknij ikonę, by wyświetlić następujące okno:



Wszystkie wykryte serwisy gromadzące dane widoczne są w przeglądzie ***Serwisy śledzące obecne na tej witrynie***. ***AVG Do Not Track*** rozróżnia trzy kategorie narzędzi gromadzących dane o użytkownikach:

- ***Web analytics*** *(domyślnie dozwolone)*: Serwisy używane do podniesienia wydajności i atrakcyjności danej witryny. W tej kategorii znajdują się usługi takie jak: Google Analytics, Omniture, czy Yahoo Analytics. Nie zalecamy blokowania ich działalności, ponieważ może to zakłócić funkcjonowanie witryny.

- ***Ad networks*** *(niektóre domyślnie zablokowane)*: Serwisy pośrednio lub bezpośrednio zbierające lub udostępniające dane o Twojej aktywności online na wielu stronach internetowych, w celu wyświetlania spersonalizowanych reklam (w przeciwieństwie do reklam kontekstowych). Szczegółowe zasady działania każdej sieci reklamowej dostępne są na jej stronach internetowych. Niektóre z sieci reklamowych są domyślnie zablokowane.

- ***Social buttons*** *(domyślnie dozwolone)*: Elementy ułatwiające korzystanie z sieci społecznościowych. Przyciski społecznościowe znajdujące się na odwiedzanych przez Ciebie stronach ładowane są z serwerów sieci społecznościowych. Podczas gdy jesteś zalogowany, mogą one zbierać dane o Twojej aktywności online. Przykładowe przyciski społecznościowe to: wtyczki społecznościowe Facebook, przycisk Twitter, Google +1.

Uwaga: *W zależności od tego jakie usługi działają w tle na danej witrynie, niektóre z opisanych wyżej sekcji interfejsu AVG Do Not Track mogą nie być widoczne.*

Elementy okna

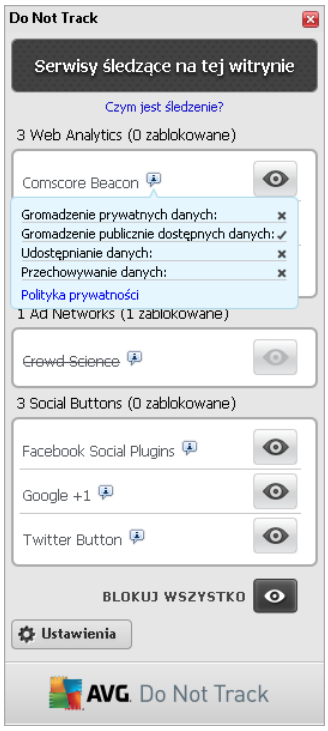
- ***Czym jest śledzenie?*** – Kliknij ten link, znajdujący się w górnej części okna, by przejść na specjalną stronę internetową, szczegółowo wyjaśniającą założenia serwisów śledzących i podającą opisy poszczególnych typów śledzenia.

- ***Blokuj wszystko*** – Kliknij przycisk widoczny w dolnej części okna, aby zaznaczyć, że nie życzysz sobie jakiegokolwiek gromadzenia danych *(szczegóły można znaleźć w rozdziale Blokowanie procesów śledzących).*

- ***Ustawienia Do Not Track*** – Kliknij przycisk znajdujący się w dolnej części okna, by przejść na specjalną stronę internetową umożliwiającą edycję różnych parametrów funkcji ***AVG Do Not Track*** *(więcej szczegółów znajduje się w rozdziale Ustawienia AVG Do Not Track)*

8.2. Informacje o procesach śledzących

Lista wykrytych procesów śledzących podaje jedynie ich nazwy. Aby podjąć świadomą decyzję o zablokowaniu lub zezwoleniu na działanie któregoś z nich, możesz potrzebować dodatkowych informacji. Umieść kursor nad odpowiednią pozycją na liście. Pojawi się wówczas okno informujące o szczegółach danego procesu śledzącego. Dowiesz się, czy proces śledzący gromadzi Twoje prywatne dane, czy jedynie inne, ogólnodostępne informacje; czy zebrane dane będą udostępniane innym podmiotom; a także czy zostaną one zachowane do wykorzystania w przyszłości:



W dolnej części okna znajduje się również link ***Polityka prywatności***, który przeniesie Cię na stronę omawiającą politykę prywatności danego serwisu.

8.3. Blokowanie procesów śledzących

Dzięki listom Ad Networks / Social Buttons / Web Analytics, masz możliwość kontrolowania, które z nich powinny zostać zablokowane. Możesz zrobić to na dwa sposoby:

- ***Blokuj wszystko*** – Kliknij ten przycisk widoczny w dolnej części okna, by zaznaczyć, że nie życzysz sobie aktywności żadnych serwisów gromadzących Twoje dane. *(Ostrzegamy jednak, że takie działanie może zakłócić funkcjonowanie witryn internetowych, które korzystały z danej usługi!)*

-  – Jeśli jednak nie chcesz zablokować jednocześnie wszystkich serwisów, możesz indywidualnie określić, które z nich mają być dozwolone. Możesz zezwolić na działanie niektórych wykrytych systemów *(np. systemów analiz – kategoria Web Analytics):* używają one zebranych danych w celu optymalizacji danej witryny, pomagając w ten sposób stworzyć środowisko przyjaźniejsze dla wszystkich użytkowników internetu. Jednocześnie możesz jednak zablokować aktywność procesów śledzących zaklasyfikowanych jako sieci reklamowe (kategoria Ad Networks). Wystarczy kliknąć ikonę  znajdującą się obok odpowiedniego procesu śledzącego *(jego nazwa zostanie przekreślona)*, by zablokować go lub odblokować ponownie.

8.4. Ustawienia AVG Do Not Track

Okno ***Opcje Do Not Track*** zawiera następującą konfigurację:

- ***Funkcja Do Not Track jest włączona*** – Domyślnie usługa DNT jest aktywna *(włączona)*. Aby wyłączyć tę usługę, ustaw przełącznik w pozycji OFF.

- W centralnej części okna widoczna jest lista znanych serwisów gromadzących dane, zaklasyfikowanych jako sieci reklamowe (Ad Networks). Domyślnie funkcja ***Do Not Track*** blokuje niektóre elementy z listy Ad Networks automatycznie, a pozostałe zależnie od Twojej decyzji. Aby to zrobić, kliknij przycisk ***Blokuj wszystko*** znajdujący się pod listą. Możesz także użyć przycisku ***Domyślne***, aby anulować wszelkie zmiany i powrócić do pierwotnej konfiguracji.

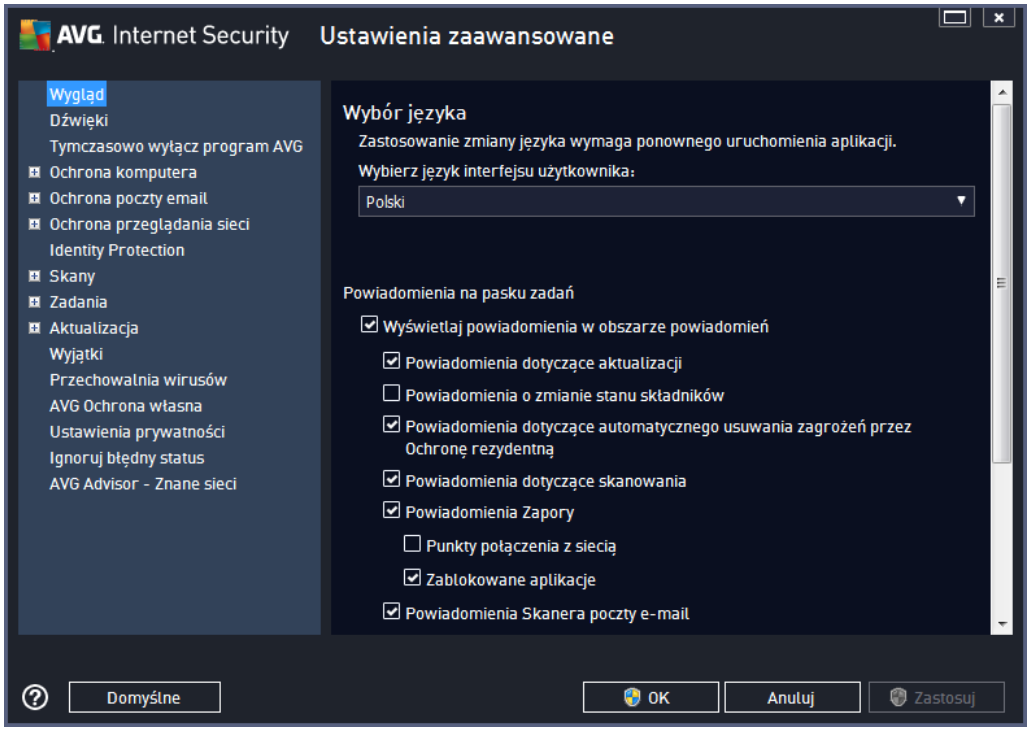
- ***Powiadamiaj witryny...*** – W tej sekcji możesz włączyć/wyłączyć opcję ***Powiadamiaj witryny o braku zgody na śledzenie*** *(domyślnie włączona).* Pozostaw tę opcję włączoną, aby funkcja ***Do Not Track*** informowała wykryte serwisy śledzące, że nie życzysz sobie śledzenia.

9. Zaawansowane ustawienia AVG

Opcje zaawansowanej konfiguracji systemu **AVG Internet Security 2014** 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 części którego*) konfiguracja ma zostać zmieniona, powoduje przejście do odpowiedniego okna z prawej strony.

9.1. Wygląd

Pierwszy element w drzewie nawigacji, ***Wygląd***, odnosi się do ogólnych ustawień interfejsu użytkownika **AVG Internet Security 2014** oraz kilku podstawowych opcji sterujących zachowaniem aplikacji:



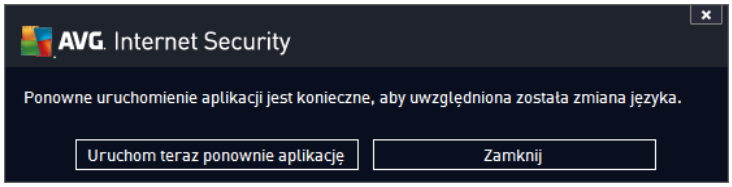
Wybór języka

W sekcji ***Wybór języka*** z rozwijanego menu można wybrać język aplikacji. Wybrany język będzie używany w całym interfejsie użytkownika **AVG Internet Security 2014**. Menu rozwijane zawiera tylko języki wybrane podczas instalacji i język angielski (*instalowany domyślnie*). Przełączenie aplikacji **AVG Internet Security 2014** na inny język wymaga ponownego uruchomienia interfejsu użytkownika. Wykonaj następujące kroki:

- Wybierz żądany język z menu rozwijanego
- Potwierdź wybór, klikając przycisk ***Zastosuj*** button *(prawy dolny róg okna)*
- Kliknij przycisk ***OK***, aby potwierdzić.

- Pojawi się wówczas komunikat informujący o konieczności restartu aplikacji **AVG Internet Security 2014**

- Kliknij przycisk ***Uruchom AVG ponownie***, aby zgodzić się na restart programu i poczekać kilka sekund na zastosowanie zmian:



Powiadomienia w zasobniku systemowym

W tym obszarze można wyłączyć wyświetlane w dymkach powiadomienia dotyczące stanu aplikacji **AVG Internet Security 2014**. Domyślnie wszystkie powiadomienia są wyświetlane. Stanowczo nie zaleca się zmiany tego ustawienia bez uzasadnionej przyczyny! Powiadomienia informują m.in. o rozpoczęciu testu lub aktualizacji, oraz o zmianie stanu któregokolwiek ze składników **AVG Internet Security 2014**. Z reguły warto zwracać na nie uwagę.

Jeśli jednak z jakiegoś powodu zdecydujesz, że nie chcesz być w ten sposób informowany, lub że interesują Cię tylko niektóre powiadomienia *(związane z konkretnym składnikiem AVG Internet Security 2014)*, możesz zdefiniować swoje preferencje poprzez zaznaczenie odpowiednich pól:

- ***Wyświetlaj powiadomienia w obszarze powiadomień*** *(domyślnie włączone)* – będą wyświetlane wszystkie powiadomienia. Odznaczenie tej opcji powoduje całkowite wyłączenie wszystkich powiadomień. Po włączeniu tej opcji można bardziej szczegółowo określić, jakie powiadomienia mają być wyświetlane:

  - ***Powiadomienia dotyczące aktualizacji*** *(domyślnie włączone)* – zdecyduj, czy powinny być wyświetlane informacje dotyczące uruchamiania, postępu i wyników aktualizacji **AVG Internet Security 2014**.

  - ***Powiadomienia o zmianach stanu składników*** *(domyślnie wyłączone)* – wyświetlane będą powiadomienia o włączeniu/wyłączeniu, oraz o ewentualnych problemach dotyczących składników. W przypadku zgłoszenia błędnego stanu składnika, funkcja ta zareaguje zmieniając kolory ikony na pasku zadań, co będzie wskazywało na problemy z którymś ze składników systemu **AVG Internet Security 2014**.

  - ***Powiadomienia dotyczące automatycznego usuwania zagrożeń przez Ochronę rezydentną*** *(domyślnie włączone)* – wyświetlane będą informacje dotyczące zapisywania, kopiowania i otwierania plików (*ta konfiguracja jest dostępna tylko wtedy, gdy jest włączona opcja automatycznego leczenia Ochrony rezydentnej*).

  - ***Powiadomienia dotyczące skanowania*** *(domyślnie włączone)* – wyświetlane będą informacje dotyczące automatycznego rozpoczęcia, postępu i zakończenia zaplanowanego skanowania.

  - ***Powiadomienia dotyczące Zapory*** *(domyślnie włączone)* – wyświetlane będą informacje dotyczące stanu i działań Zapory, np. ostrzeżenia o włączeniu/wyłączeniu

składnika, możliwym blokowaniu połączeń, itd. Ta opcja posiada dwa kolejne pola wyboru *(szczegółowy opis związanych z nimi funkcji można znaleźć w rozdziale Zapora niniejszego dokumentu)*:

– ***Punkty połączenia z siecią*** *(domyślnie wyłączone)* – przy łączeniu z siecią Zapora poinformuje Cię, czy zna sieć i czy włączone jest udostępnianie plików i drukarek.

– ***Zablokowane aplikacje*** *(domyślnie włączone)* – gdy nieznana lub podejrzana aplikacja próbuje połączyć się z siecią, Zapora zablokuje próbę połączenia i wyświetli powiadomienie. Jest to przydatna funkcja, dzięki której będziesz zawsze poinformowany, więc nie zalecamy wyłączania jej.

- ***Powiadomienia Skanera poczty email*** *(domyślnie włączone)* – wyświetlane będą informacje o skanowaniu wszystkich wiadomości przychodzących i wychodzących.

- ***Powiadomienia dotyczące statystyk*** *(domyślnie włączone)* – pozostaw to pole zaznaczone, aby być regularnie powiadamianym o dotychczasowych statystykach bezpieczeństwa.

- ***Powiadomienia dotyczące składnika AVG Accelerator*** *(domyślnie włączone)* – wyświetlane będą powiadomienia o aktywności składnika ***AVG Accelerator***. ***AVG Accelerator*** to usługa pozwalająca na płynniejsze odtwarzanie filmów online i łatwiejsze pobieranie dodatkowych plików.

- ***Powiadomienia dotyczące przyspieszenia czasu startu systemu*** *(domyślnie wyłączone)* – zdecyduj, czy chcesz być informowany o przyspieszeniu czasu rozruchu systemu.

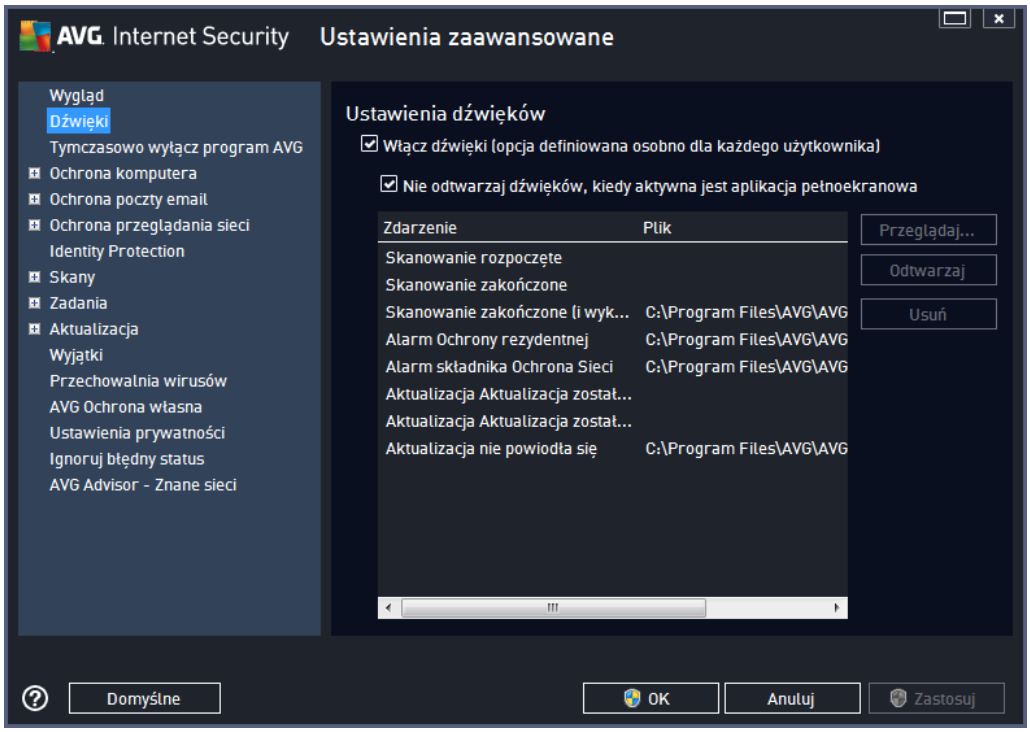
- ***Powiadomienia Doradcy AVG*** *(domyślnie włączone)* – zdecyduj, czy chcesz wyświetlać informacje o aktywności Doradcy AVG w rozwijanym panelu nad zasobnikiem systemowym.

Tryb gry

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

9.2. Dźwięki

W oknie dialogowym ***Ustawienia dźwięków*** można określić, czy oprogramowanie **AVG Internet Security 2014** ma informować o określonych czynnościach za pomocą dźwięków:



Ustawienia obowiązują wyłącznie dla bieżącego konta użytkownika, co oznacza, że każdy użytkownik komputera może mieć własne ustawienia dźwięków. Jeżeli zgadzasz się na powiadomienia dźwiękowa, 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)*.

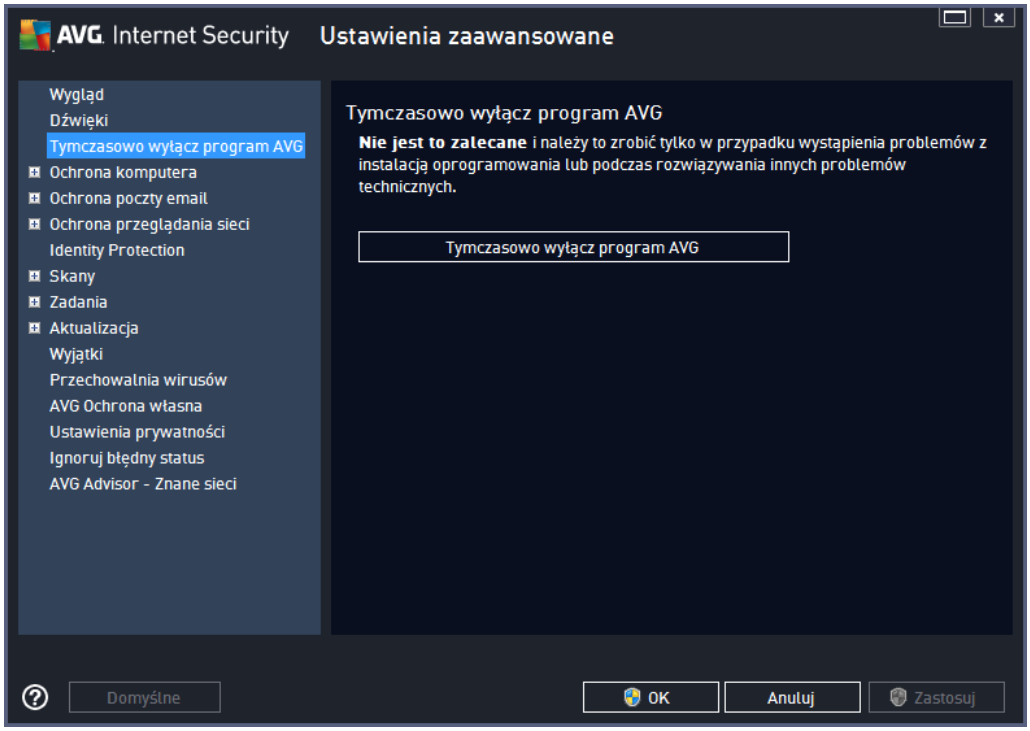
Przyciski kontrolne

- ***Przeglądaj...*** – po wybraniu konkretnego zdarzenia z listy, użyj przycisku ***Przeglądaj***, aby wskazać żądany plik dźwiękowy. *(Przypominamy, że obecnie obsługiwane są tylko pliki *.wav!)*
- ***Odtwórz*** – Aby odsłuchać wybranego dźwięku, wskaż na liście żądane zdarzenie i kliknij przycisk ***Odtwórz***.
- ***Usuń*** – Użyj przycisku ***Usuń***, aby usunąć dźwięk przypisany do danego zdarzenia.

9.3. Tymczasowo wyłącz ochronę AVG

W oknie dialogowym ***Tymczasowo wyłącz ochronę AVG*** można wyłączyć całą ochronę zapewnianą przez system **AVG Internet Security 2014**.

Pamiętaj, że tej opcji nie powinno się używać, chyba że jest to absolutnie konieczne!

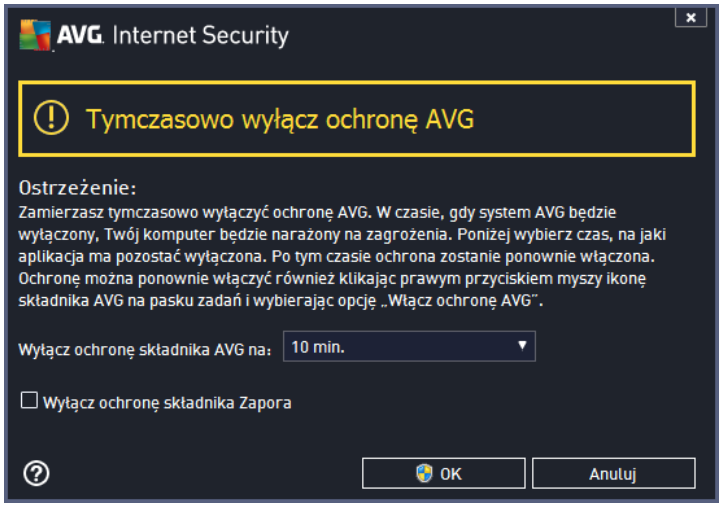


W większości przypadków ***nie jest konieczne*** wyłączanie systemu **AVG Internet Security 2014** przed instalowaniem nowego oprogramowania lub sterowników, nawet jeśli instalator lub kreator sugeruje uprzednie zamknięcie działających programów i aplikacji. Jeżeli jednak napotkasz problemy przy instalacji, spróbuj najpierw wyłączyć Ochronę rezydentną (pole *Włącz Ochronę rezydentną*) first. Jeśli jednak tymczasowe wyłączenie systemu **AVG Internet Security 2014** jest konieczne, należy go 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.

Jak wyłaczyć ochronę AVG

Zaznacz pole ***Tymczasowo wyłącz ochronę AVG***, a następnie potwierdź swoją decyzję, klikając przycisk ***Zastosuj.*** Określ w nowo otwartym oknie ***Tymczasowo wyłącz ochronę AVG*** na jak długo chcesz wyłączyć system **AVG Internet Security 2014**. Domyślnie ochrona pozostanie nieaktywna przez 10 minut, co powinno wystarczyć na wykonanie przeciętnego zadania, np. instalację nowego oprogramowania itp. Możesz zdecydować się na dłuższy okres, jednak nie zalecamy tej opcji, chyba, że jest absolutnie niezbędna. Po upłynięciu żądanego czasu, wszystkie wyłączone składniki zostaną automatycznie aktywowane ponownie. Możesz wyłączyć ochronę AVG aż do następnego restartu komputera. Osobna opcja umożliwiająca wyłączenie ***Zapory***

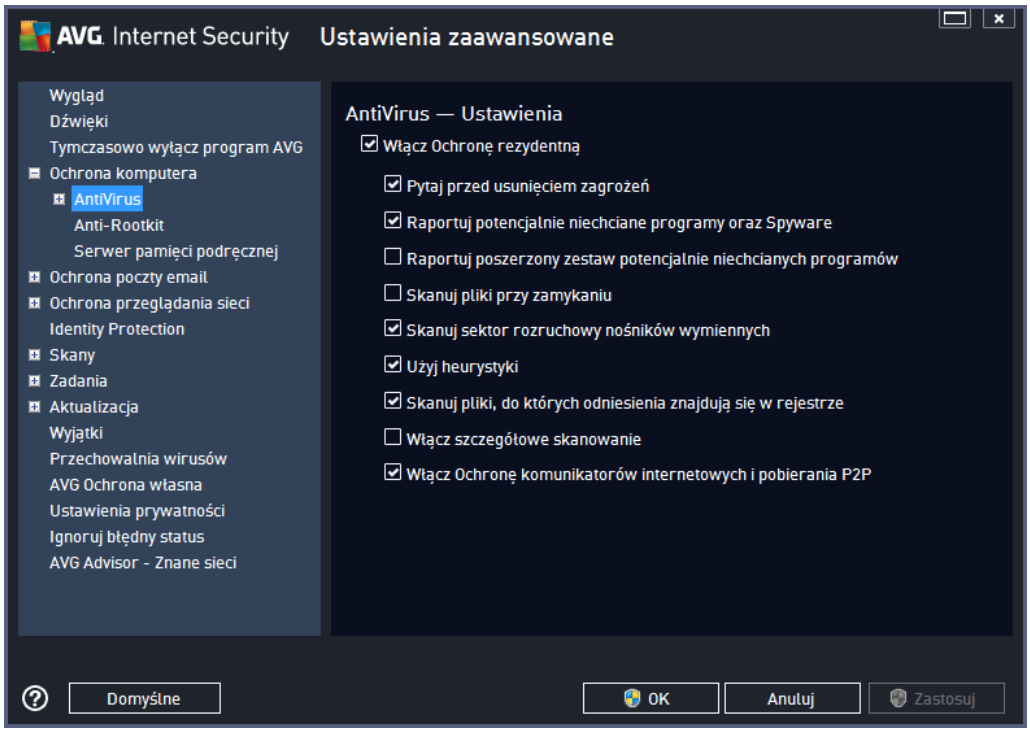
dostępna jest w oknie ***Tymczasowo wyłącz ochronę AVG***. Aby to zrobić, zaznacz pole ***Wyłącz Zaporę***.



9.4. Ochrona komputera

9.4.1. AntiVirus

AntiVirus oraz ***Ochrona rezydentna*** stale chronią Twój komputer przed wszystkimi znanymi typami wirusów, oprogramowania szpiegującego i złośliwego oprogramowania *(włączając w to tak zwane uśpione 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*). Ponadto, można aktywować tylko wybrane funkcje składnika Ochrona rezydentna:

- ***Pytaj przed usunięciem zagrożeń*** (*domyślnie włączone*) – zaznacz to pole, aby zyskać pewność, że Ochrona rezydentna nie podejmie żadnych działań w sposób automatyczny; każdorazowo wyświetlone zostanie okno opisujące wykryte zagrożenie i umożliwiające Ci podjęcie decyzji. Jeśli pozostawisz to pole niezaznaczone, **AVG Internet Security 2014** automatycznie wyleczy infekcję, a jeśli to nie będzie możliwe – przeniesie obiekt do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy i spyware*** (*opcja domyślnie włączona*) – zaznaczenie tego pola umożliwi 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 wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja 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 Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też 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*** (*opcja domyślnie włączona*).

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) – przy skanowaniu będzie używana analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku maszyny wirtualnej*).

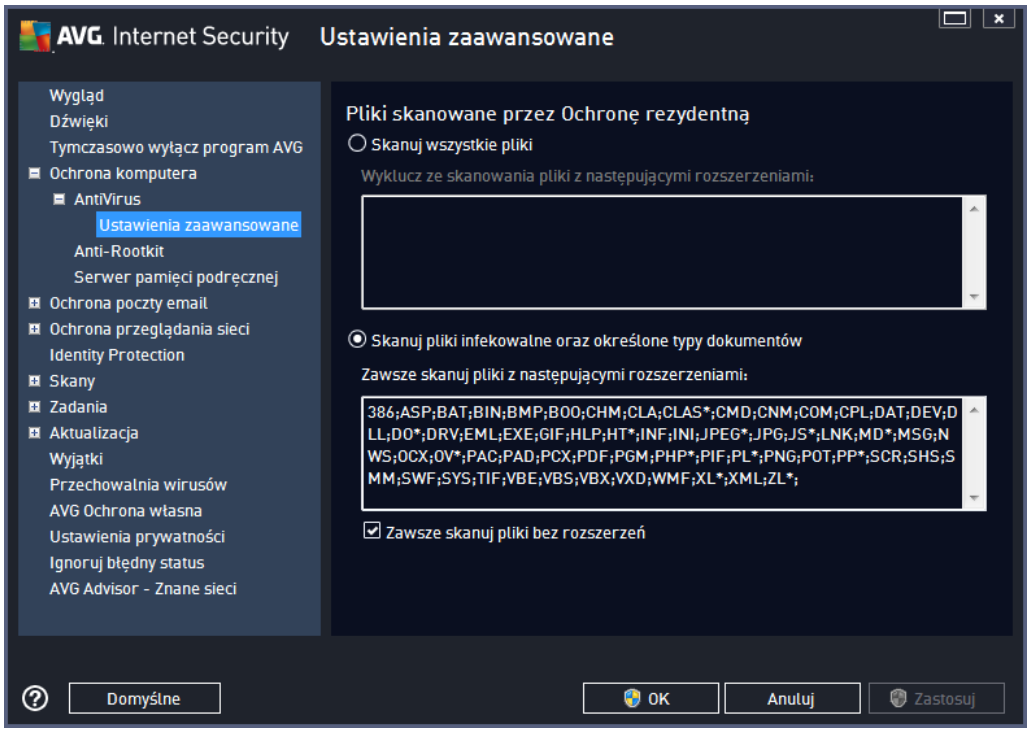
- ***Skanuj pliki, do których odniesienia znajdują się w rejestrze*** (*opcja domyślnie włączona*) – ten parametr określa, że system AVG będzie skanować wszystkie pliki wykonywalne dodane do rejestru w sekcji autostartu.

- ***Włącz szczegółowe skanowanie*** (*opcja domyślnie wyłączona*) – w określonych sytuacjach (*w stanie wyjątkowej konieczności*) można zaznaczyć tę opcję, aby aktywować algorytmy bardziej szczegółowego skanowania, które będą dogłębnie sprawdzać wszystkie obiekty mogące stwarzać zagrożenie. Należy pamiętać, że ta metoda skanowania jest 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, ...*) i danych pobranych z sieci Peer-to-Peer *(sieci umożliwiających nawiązywanie bezpośrednich połączeń między klientami, bez udziału serwera, co może być potencjalnie niebezpieczne; zazwyczaj używanych do wymiany*

muzyki).

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

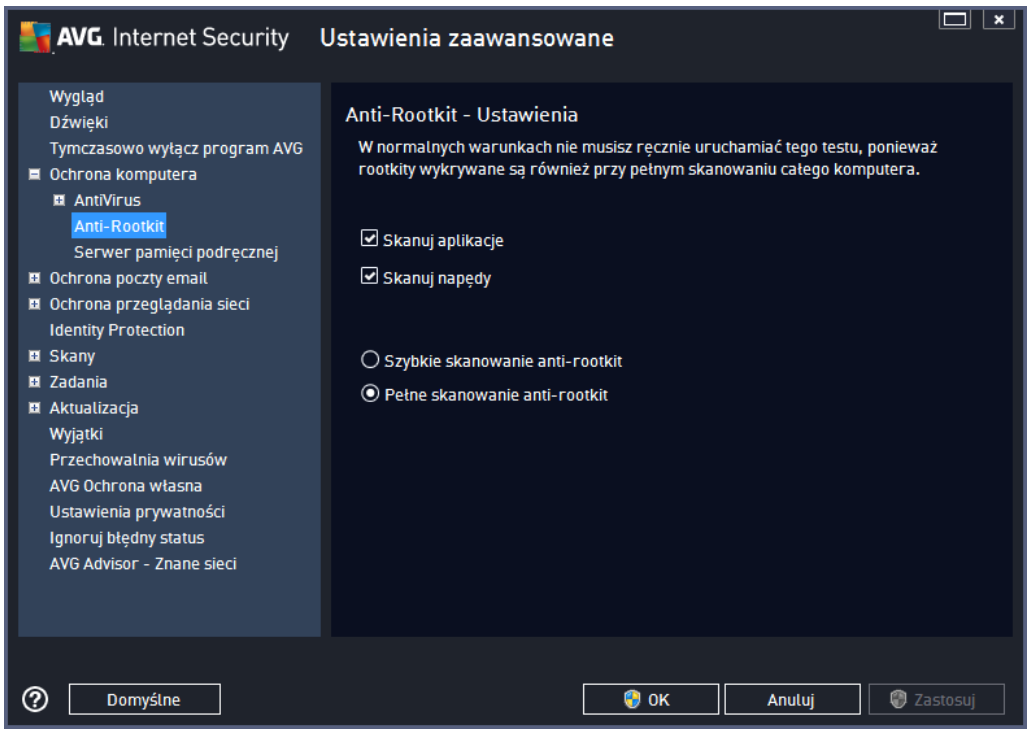


Zaznacz odpowiednie pole, w zależności od tego, czy chcesz skanować ***wszystkie pliki*** czy ***tylko pliki infekowalne i niektóre typy dokumentów***. Aby przyspieszyć skanowanie a jednocześnie zapewnić maksymalną ochronę, zalecamy zachowanie ustawień domyślnych. Dzięki temu skanowane będą tylko pliki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

Zaznaczenie opcji ***Skanuj również pliki bez rozszerzeń*** (*domyślnie włączone*) gwarantuje, że Ochrona rezydentna będzie skanowała także pliki bez rozszerzeń i pliki nieznanych formatów. Nie zaleca się wyłączania tej opcji, ponieważ pliki bez rozszerzeń są podejrzane.

9.4.2. Anti-Rootkit

W oknie ***Ustawienia Anti-Rootkit*** możesz edytować konfigurację funkcji ***Anti-Rootkit*** oraz parametry skanowania w poszukiwaniu programów typu rootkit. Test Anti-Rootkit jest domyślną częścią Skanu całego komputera:

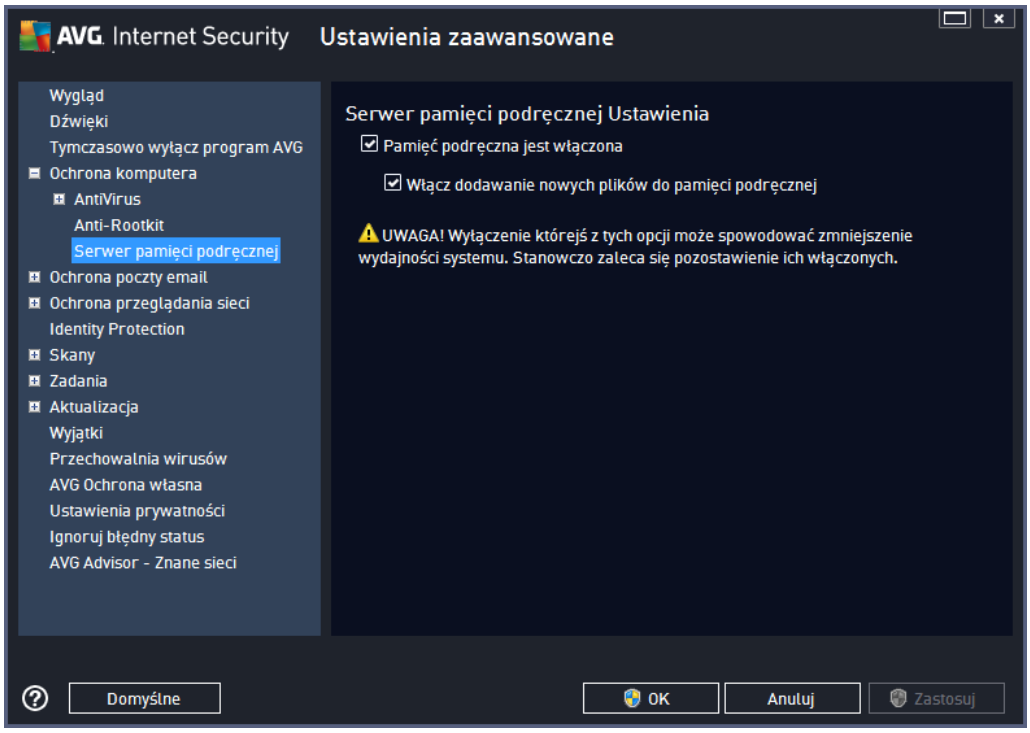


Opcje Skanuj aplikacje i ***Skanuj napędy*** pozwalają szczegółowo określić, co ma obejmować skanowanie Anti-Rootkit. Ustawienia te są przeznaczone dla użytkowników zaawansowanych. Zaleca się pozostawienie wszystkich opcji włączonych. Można również wybrać tryb skanowania w poszukiwaniu programów typu rootkit:

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

9.4.3. Serwer pamięci podręcznej

Okno ***Ustawienia serwera pamięci podręcznej*** odnosi się do procesu serwera pamięci podręcznej, który ma za zadanie przyspieszenie wszystkich testów **AVG Internet Security 2014**:



Zbiera on i przechowuje informacje o zaufanych plikach (*tych, które zostały podpisane cyfrowo przez znane źródło*). Pliki takie są automatycznie uznawane za bezpieczne, więc nie muszą być powtórnie skanowanie i mogą zostać pominięte.

Okno ***Ustawienia serwera pamięci podręcznej*** zawiera następujące opcje:

- ***Włączona pamięć podręczna*** (*opcja domyślnie włączona*) – odznaczenie tego pola powoduje wyłączenie funkcji ***Serwer pamięci podręcznej*** i opróżnienie pamięci podręcznej. Należy pamiętać, że skanowanie może spowolnić 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*) – odznaczenie tego pola umożliwia wyłączenie funkcji dodawania kolejnych plików do pamięci podręcznej. Wszystkie pliki zapisane w pamięci podręcznej są w niej przechowywane dopóki funkcja nie zostanie zupełnie wyłączona lub do czasu kolejnej aktualizacji bazy wirusów.

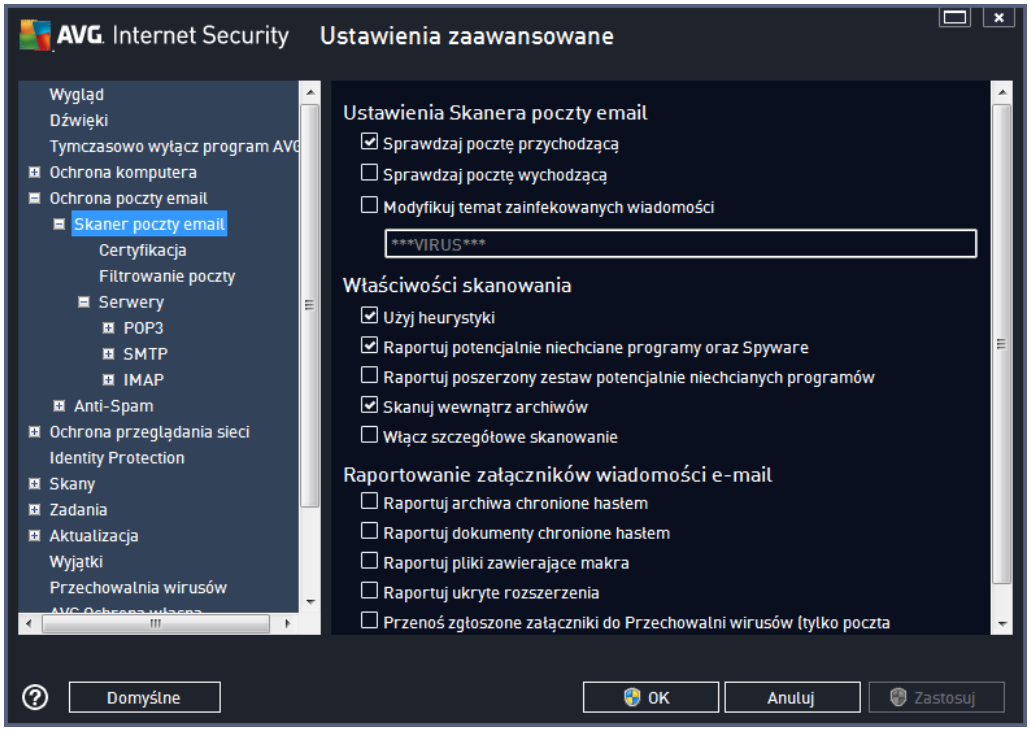
Jeśli nie posiadasz ku temu ważnego powodu, stanowczo odradzamy wyłączanie serwera pamięci podręcznej! Unikniesz dzięki temu znacznego obniżenia wydajności systemu.

9.5. Skaner poczty Email

W tej sekcji możesz edytować konfigurację składników Skaner poczty Email oraz Anti-Spam:

9.5.1. Skaner poczty Email

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 włączone*) – zaznacz lub odznacz to pole, aby włączyć/wyłączyć opcję skanowania wszystkich wiadomości e-mail dostarczanych do klienta poczty e-mail.

- ***Sprawdzaj pocztę wychodzącą*** (*domyślnie wyłączone*) – zaznacz lub odznacz to pole, aby włączyć/wyłączyć opcję skanowania wszystkich wiadomości e-mail wysyłanych z klienta poczty e-mail.

- ***Modyfikuj temat zainfekowanych wiadomości*** (*domyślnie wyłączone*) – jeśli chcesz otrzymywać ostrzeżenia o tym, że przeskanowana wiadomość e-mail została zaklasyfikowana jako zainfekowana, zaznacz to pole i wprowadź żądany tekst w polu tekstowym. Ten tekst będzie dodawany do tematu każdej wykrytej zainfekowanej wiadomości e-mail, aby ułatwić ich identyfikowanie i filtrowanie. Wartość domyślna to ***VIRUS***; zaleca się jej zachowanie.

Właściwości skanowania

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

- ***Użyj analizy heurystycznej*** (*domyślnie włączone*) – 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 i spyware*** (*opcja 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 wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** (*opcja 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 Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- ***Skanuj wewnątrz archiwów*** (*domyślnie włączone*) – zaznaczenie tego pola umożliwia skanowanie zawartości archiwów dołączonych do wiadomości e-mail.

- ***Włącz szczegółowe skanowanie*** (*domyślnie wyłączone*) – w określonych sytuacjach (*np. gdy zachodzi podejrzenie, że komputer jest zainfekowany przez wirus lub atak*) można zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będą one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest 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 Zagrożenia wykryte przez Ochrony poczty email:

- ***Raportuj archiwa chronione hasłem*** – archiwów (*ZIP, RAR itp.*) chronionych hasłem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.

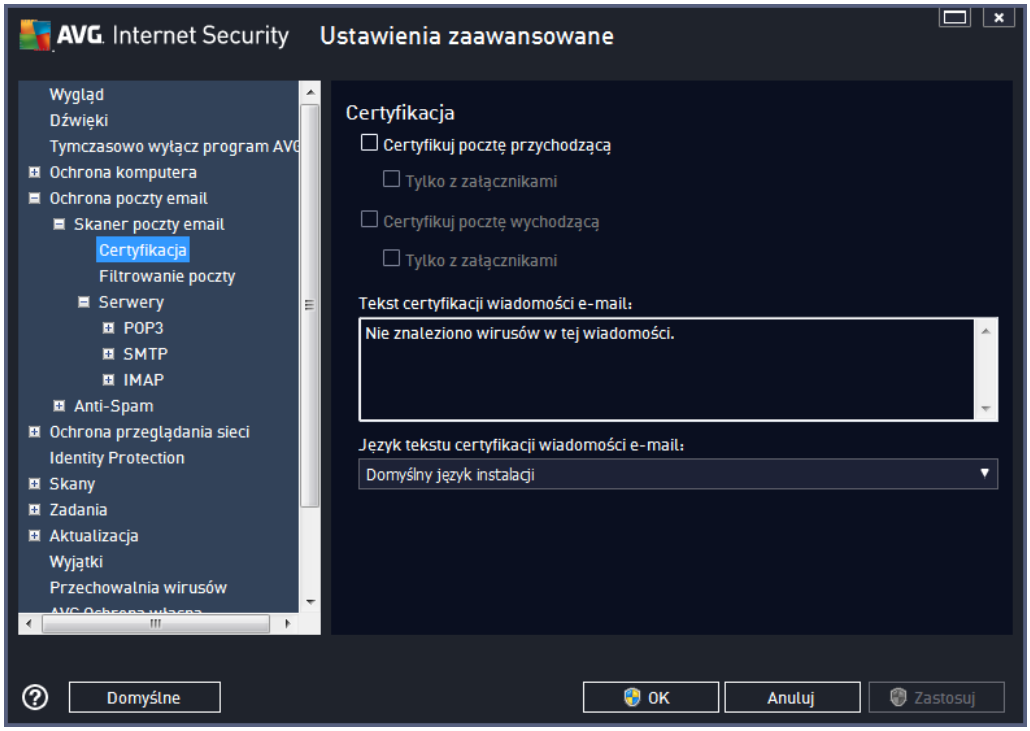
- ***Raportuj dokumenty chronione hasłem*** – dokumentów chronionych hasłem nie można skanować w poszukiwaniu wirusów. Należy zaznaczyć to pole wyboru, aby system AVG zgłaszał je jako potencjalnie niebezpieczne.

- ***Raportuj pliki zawierające makra*** – makro to predefiniowana sekwencja kroków mająca ułatwiać 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). Należy zaznaczyć to pole wyboru, aby zgłaszać je jako potencjalnie niebezpieczne.

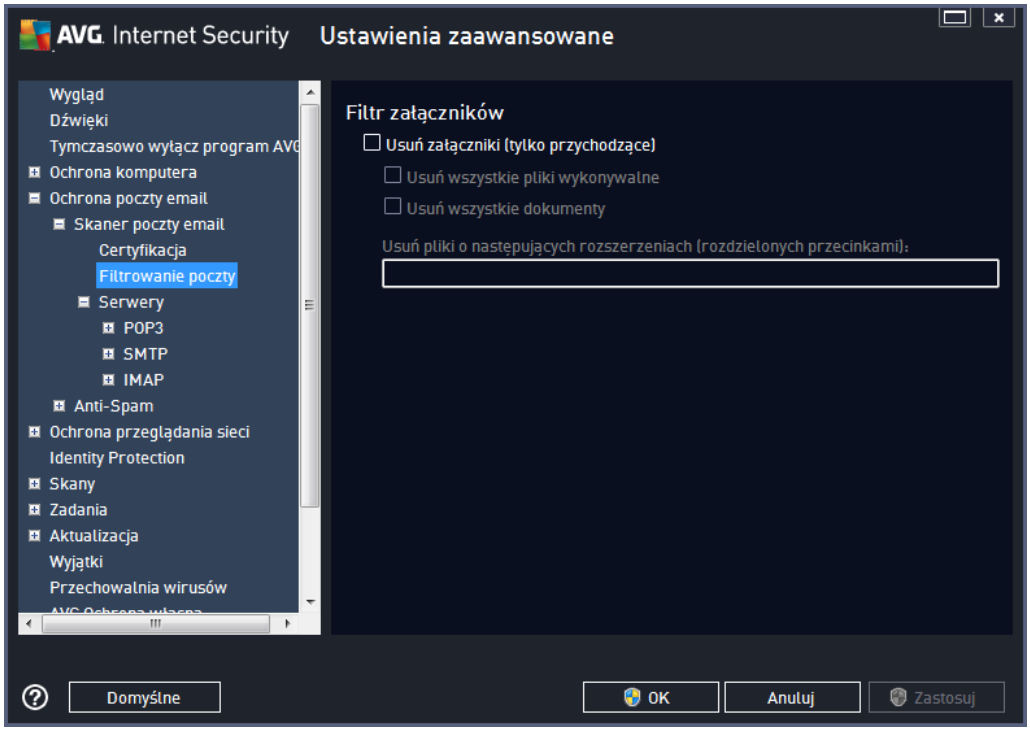
- ***Przenoś raportowane załączniki do Przechowalni wirusów*** – możesz skonfigurować system AVG tak, aby powiadamiał Cię poprzez e-mail o wykrytych archiwach i dokumentach zabezpieczonych hasłem, plikach zawierających makra lub ukrytych rozszerzeniach, które zostaną wykryte w załącznikach skanowanych wiadomości. Należy także określić, 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 po prostu, że *Nie znaleziono wirusów w tej wiadomości.* Treść tą można jednak łatwo zmienić, korzystając z pola ***Tekst certyfikacji wiadomości e-mail***. Sekcja ***Język tekstu certyfikacji wiadomości e-mail*** pozwala na zmianę języka automatycznie generowanej części certyfikacji (*Nie znaleziono wirusów w tej wiadomości*).

Uwaga: *We wskazanym języku będzie wyświetlany jedynie domyślny tekst certyfikacji. Część zdefiniowana przez użytkownika nie zostanie automatycznie przetłumaczona!*



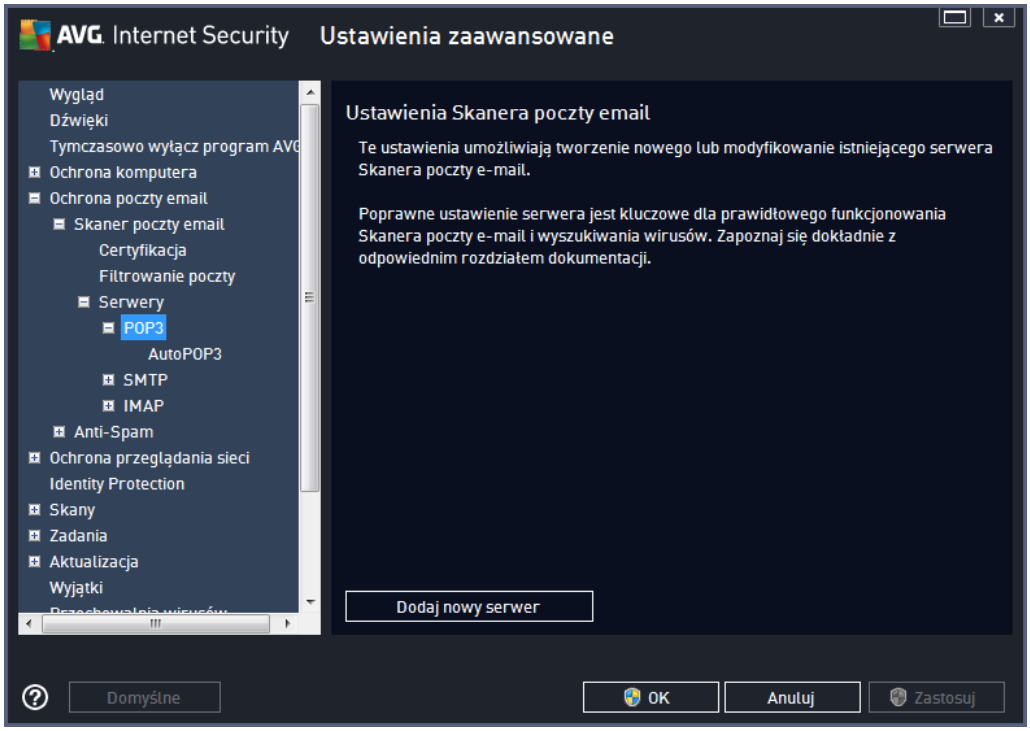
W oknie dialogowym ***Filtr załączników*** można ustawiać parametry skanowania załączników do wiadomości e-mail. Opcja ***Usuń załączniki*** jest domyślnie wyłączona. Jeśli zostanie włączona, wszystkie załączniki wiadomości zidentyfikowane jako zainfekowane lub potencjalnie niebezpieczne, będą automatycznie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

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

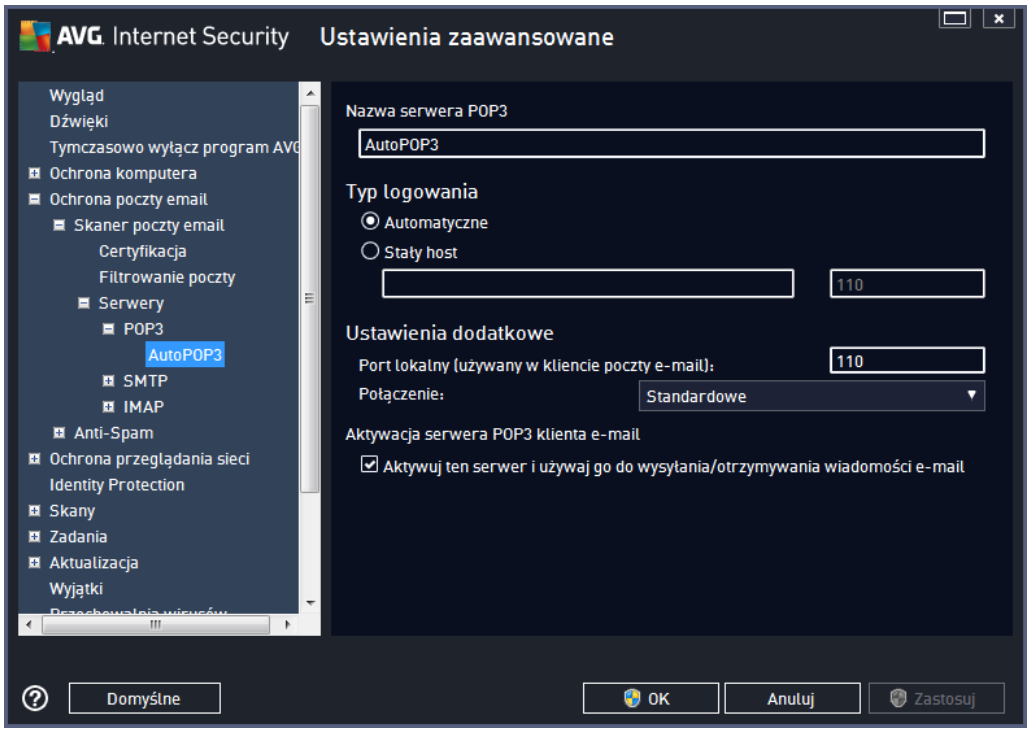
W sekcji ***Serwery*** edytować można parametry serwerów Skanera poczty e-mail:

- 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 Skanera poczty Email nowy serwer poczty przychodzącej, korzystający z protokołu POP3:



- ***Nazwa serwera PO3*** – 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). W przypadku automatycznie utworzonych serwerów AutoPOP3 to pole jest nieaktywne.

- ***Typ logowania*** – definiuje metodę określania serwera pocztowego dla wiadomości przychodzących:

    - ***Automatycznie*** – logowanie jest przeprowadzane automatycznie zgodnie z ustawieniami klienta poczty e-mail.

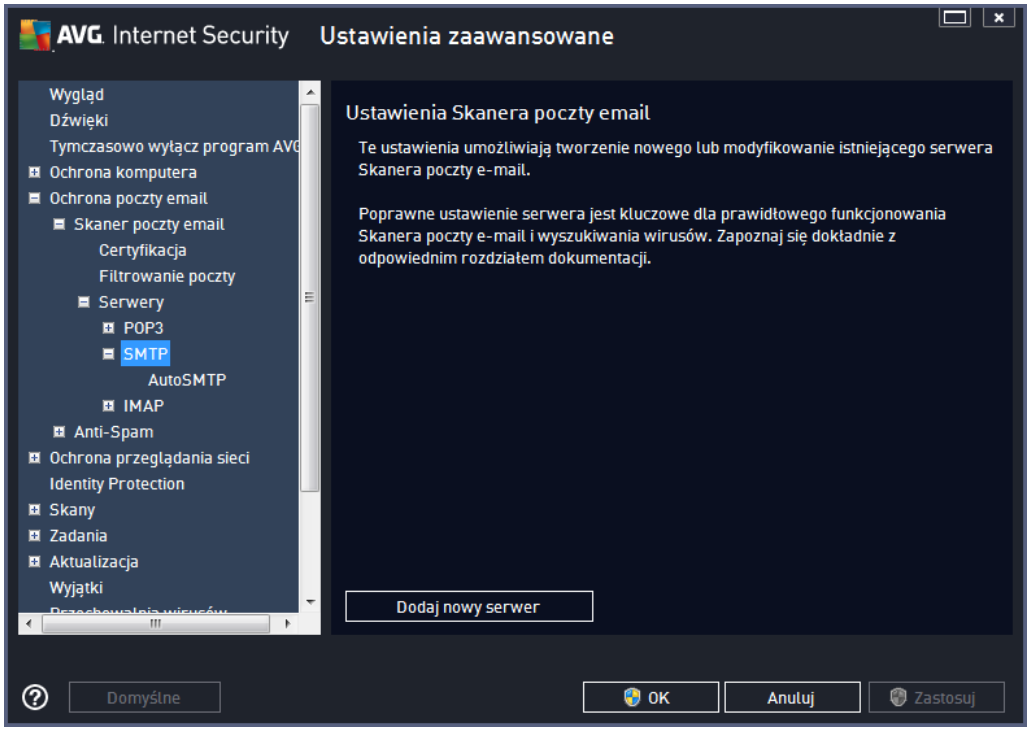
    - ***Stały host*** – po wybraniu tej opcji program będzie zawsze korzystał z serwera określonego w tym miejscu. Należy podać adres lub nazwę serwera pocztowego. Login użytkownika pozostaje niezmieniony. Jako nazwy można użyć nazwy domeny (*np. pop.domena.com*) lub adresu IP (*np. 123.45.67.89*). Jeśli serwer pocztowy używa niestandardowego portu, można podać go po dwukropku, zaraz za nazwą serwera (*np. pop.domena.com:8200*). Standardowym portem protokołu POP3 jest 110.

- ***Ustawienia dodatkowe*** – pozwalają zdefiniować bardziej szczegółowe parametry:

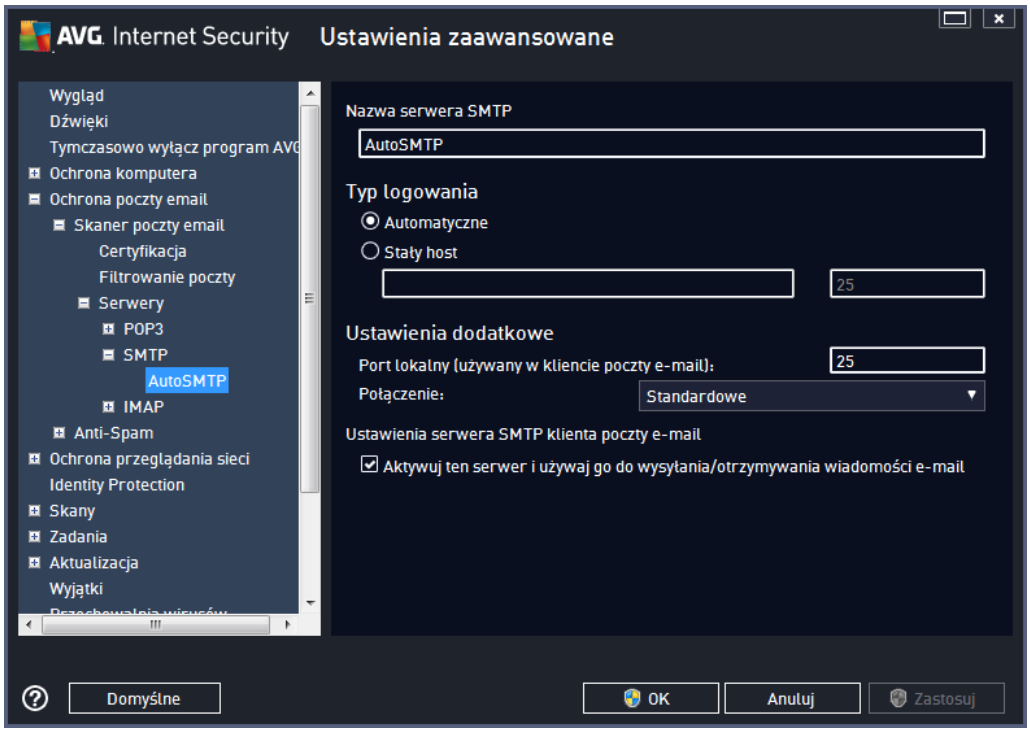
    - ***Port lokalny*** – określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w kliencie poczty jako port docelowy serwera POP3.

    - ***Połączenie*** – z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.

- ***Aktywacja serwera POP3 klienta poczty e-mail*** – opcję tę należy zaznaczyć/odznaczyć, aby aktywować lub dezaktywować określony serwer POP3



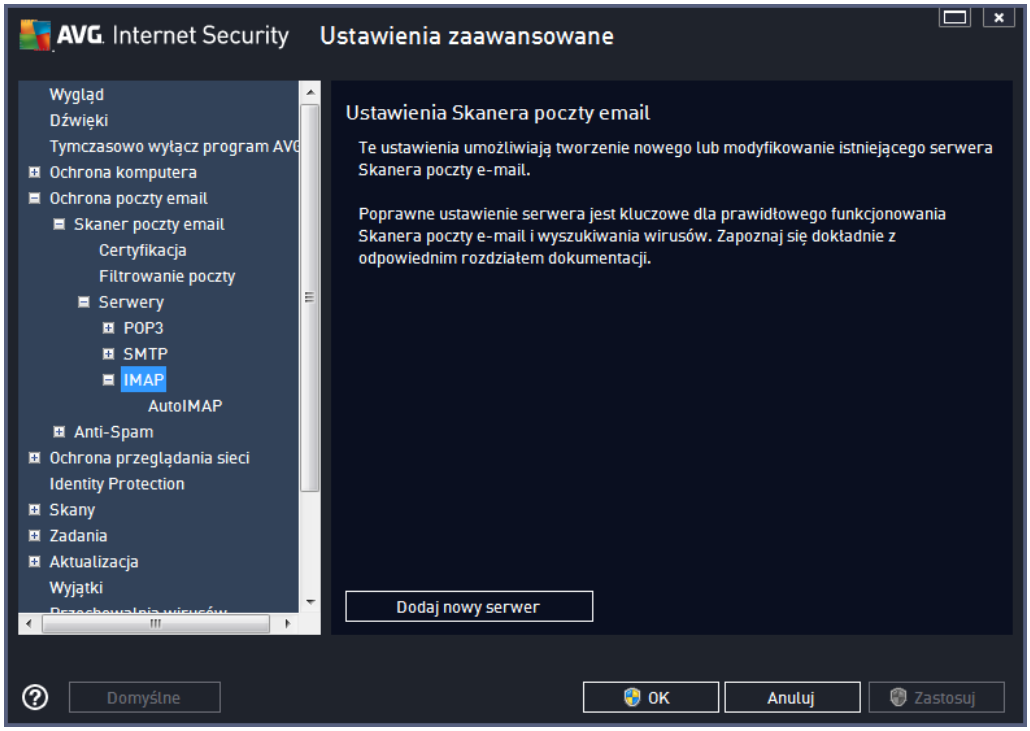
W tym oknie dialogowym można zdefiniować na potrzeby Skanera poczty Email nowy serwer poczty przychodzącej, korzystający z protokołu SMTP:



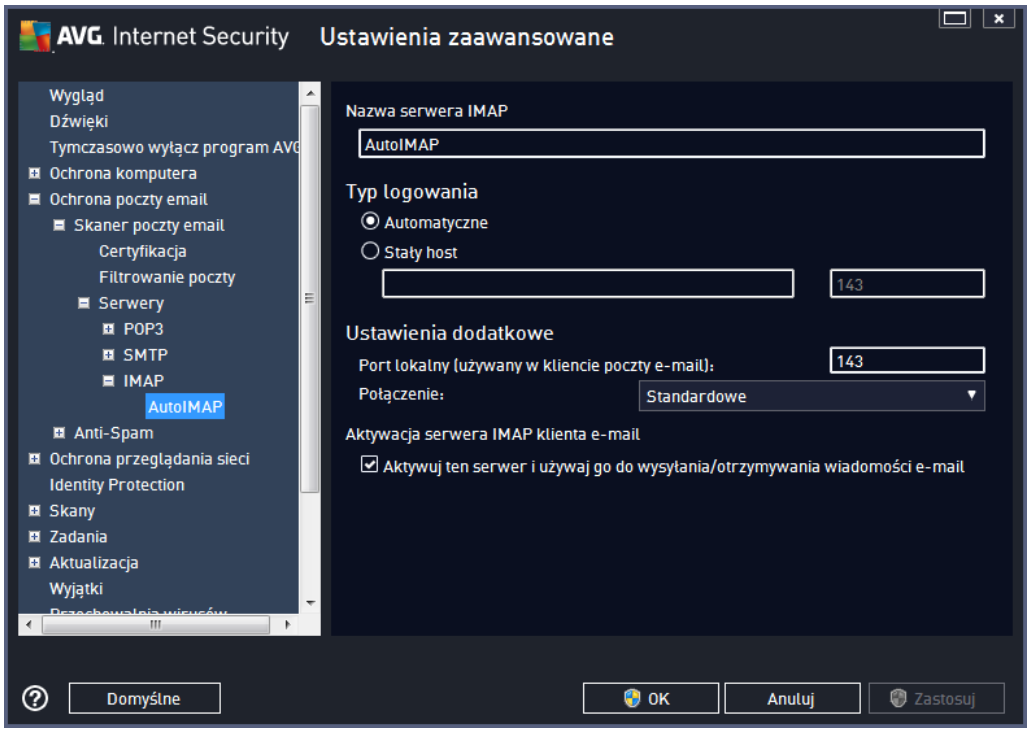
- ***Nazwa serwera SMTP*** – w tym polu można podać nazwę nowo dodanego serwera (*aby*

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 określania 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 protokołu SMTP jest port 25.
- ***Ustawienia dodatkowe*** – pozwalają zdefiniować bardziej szczegółowe parametry:
    - ***Port lokalny*** – określa port nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port komunikacji SMTP.
    - ***Połączenie*** – z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, system AVG skorzysta z funkcji szyfrowania danych, co zmniejsza ryzyko ich przechwycenia lub monitorowania przez inne osoby. Funkcja ta dostępna jest tylko wtedy, gdy obsługuje ją docelowy serwer pocztowy.
- ***Aktywacja klienta SMTP 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 przychodzącej, korzystający z protokołu IMAP:

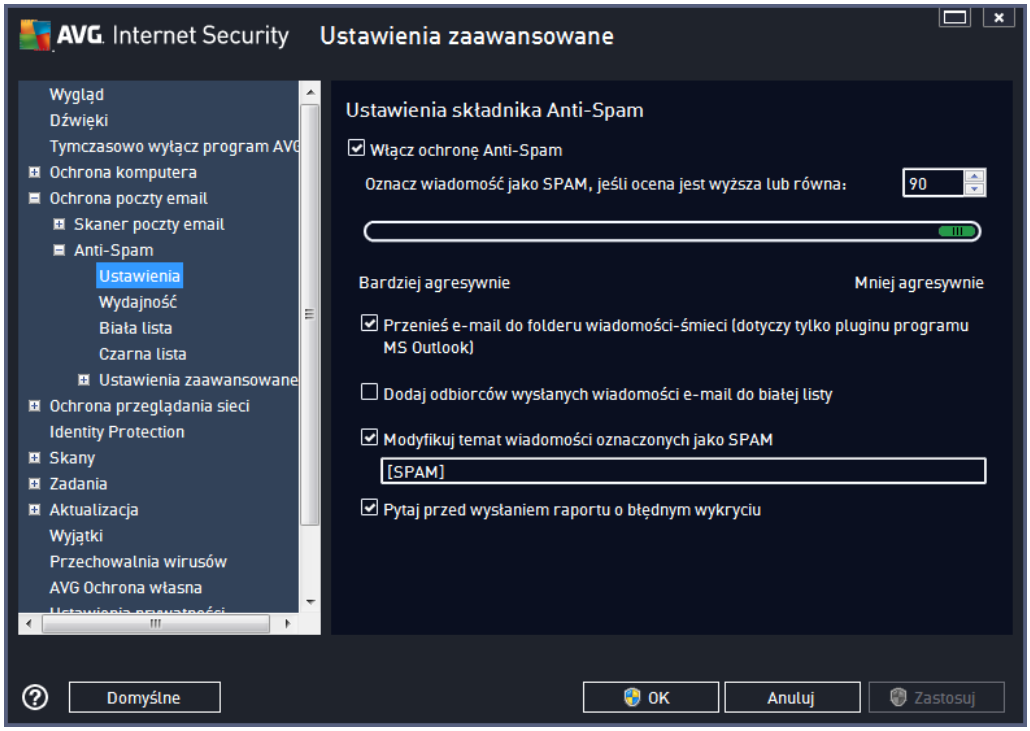


- ***Nazwa serwera IMAP*** – w tym polu można podać nazwę nowo dodanego serwera (*aby*

dodać serwer IMAP, kliknij prawym przyciskiem myszy pozycję IMAP w menu nawigacyjnym po lewej stronie). W przypadku automatycznie utworzonych serwerów AutoIMAP to pole jest nieaktywne.

- ***Typ logowania*** – definiuje metodę określania 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 nasłuchu dla aplikacji pocztowej. Ten sam port należy następnie określić w aplikacji pocztowej jako port do komunikacji IMAP.
    - ***Połączenie*** – z menu rozwijanego należy wybrać rodzaj używanego połączenia (*zwykłe/SSL/domyślne SSL*). Jeśli zostanie wybrane połączenie SSL, dane będą szyfrowane, co zmniejsza ryzyko ich śledzenia 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

9.5.2. Anti-Spam



W oknie dialogowym ***Ustawienia składnika Anti-Spam*** można zaznaczyć pole ***Włącz ochronę Anti-Spam***, aby włączyć/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 metody oceny. Filtr ***Anti-Spam*** przypisuje każdej wiadomości ocenę (*tj. wskaźnik informujący, jak bardzo jej treść przypomina SPAM*) na podstawie kilku dynamicznych technik skanowania. W sekcji ***Oznacz wiadomość jako spam, jeśli ocena jest większa niż*** możesz wpisać odpowiednią wartość ręcznie lub ustawić suwak (*porusza się on w przedziale 50-90*).

Zwykle zaleca się stosowanie progu z przedziału od 50 do 90, a jeśli nie ma pewności co do właściwego ustawienia – równego 90. Poniżej przedstawiono opis progów oceny:

- ***Wartość 80-90*** – wiadomości e-mail, które stanowią potencjalny spam, są poprawnie odfiltrowywane. Niektóre z pożądanych wiadomości (niebędących spamem) mogą zostać błędnie zablokowane.
- ***Wartość 60–79*** – umiarkowanie agresywna konfiguracja. Wiadomości e-mail, które mogą stanowić spam, są poprawnie odfiltrowywane. Pożądane wiadomości (niebędące spamem) mogą zostać błędnie zablokowane.
- ***Wartość 50–59*** – bardzo agresywna konfiguracja. Wiadomości e-mail niebędące spamem są odfiltrowywane w równym stopniu, jak 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:

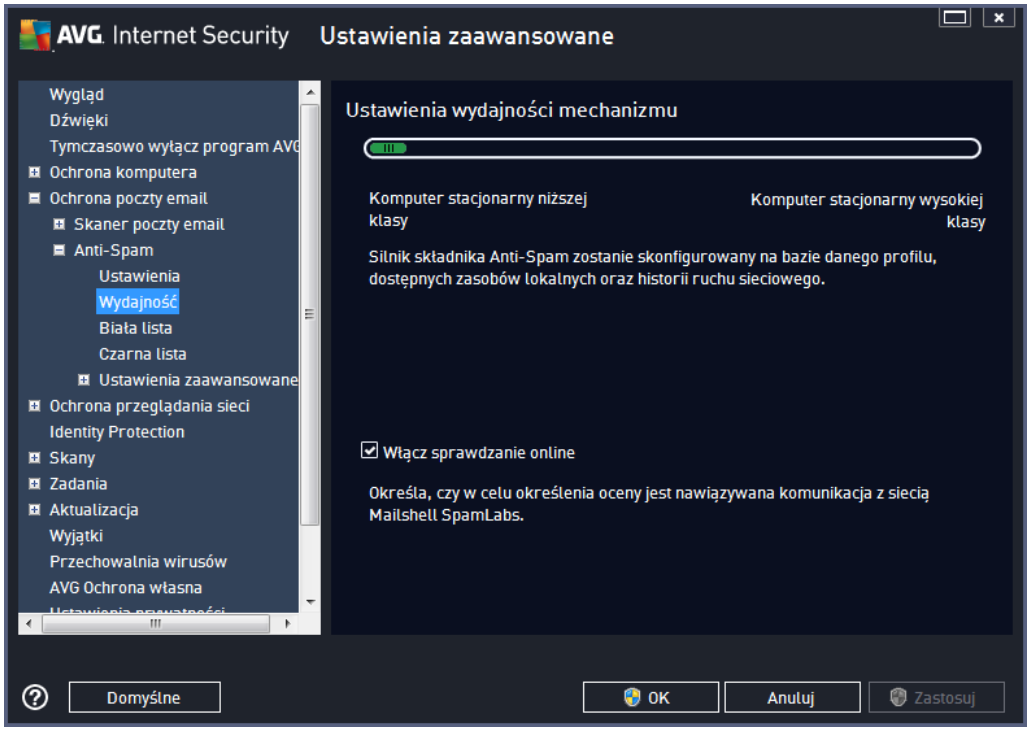
- ***Przenieś wiadomość do folderu wiadomości-śmieci*** *(tylko plugin Microsoft Outlook)* – jeśli ta opcja jest zaznaczona, wykryty spam będzie automatycznie przenoszony do wskazanego folderu wiadomości-śmieci w kliencie poczty. Obecnie funkcja ta nie jest obsługiwana przez pozostałych klientów poczty 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 więc poczta przychodzące 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) wskazaną frazą lub znakiem; żądany tekst można wpisać w polu znajdującym się poniżej.

- ***Pytaj przed wysłaniem raportu o błędnym wykryciu*** – opcja ta jest dostępna, jeśli podczas instalacji użytkownik zdecydował się uczestniczyć w projekcie Ustawienia prywatności. Zgodziłeś się tym samym na raportowanie wykrytych zagrożeń firmie AVG. Raporty tworzone są automatycznie. Można jednak zaznaczyć to pole wyboru, aby przed wysłaniem raportu o wykrytym spamie do firmy AVG wyświetlać pytanie, czy dana wiadomość faktycznie jest niepożądana.

Okno ***Ustawienia wydajności mechanizmu*** (*połączone elementem* ***Wydajność*** *z lewej części okna nawigacji*) oferuje ustawienia wydajności składnika ***Anti-Spam***:



Przesuń suwak w lewo lub w prawo, aby zmienić poziom wydajności skanowania pomiędzy opcjami ***Komputer niższej klasy*** / ***Komputer wysokiej klasy***.

- ***Komputer niższej klasy*** – podczas skanowania w poszukiwaniu spamu, żadne reguły nie

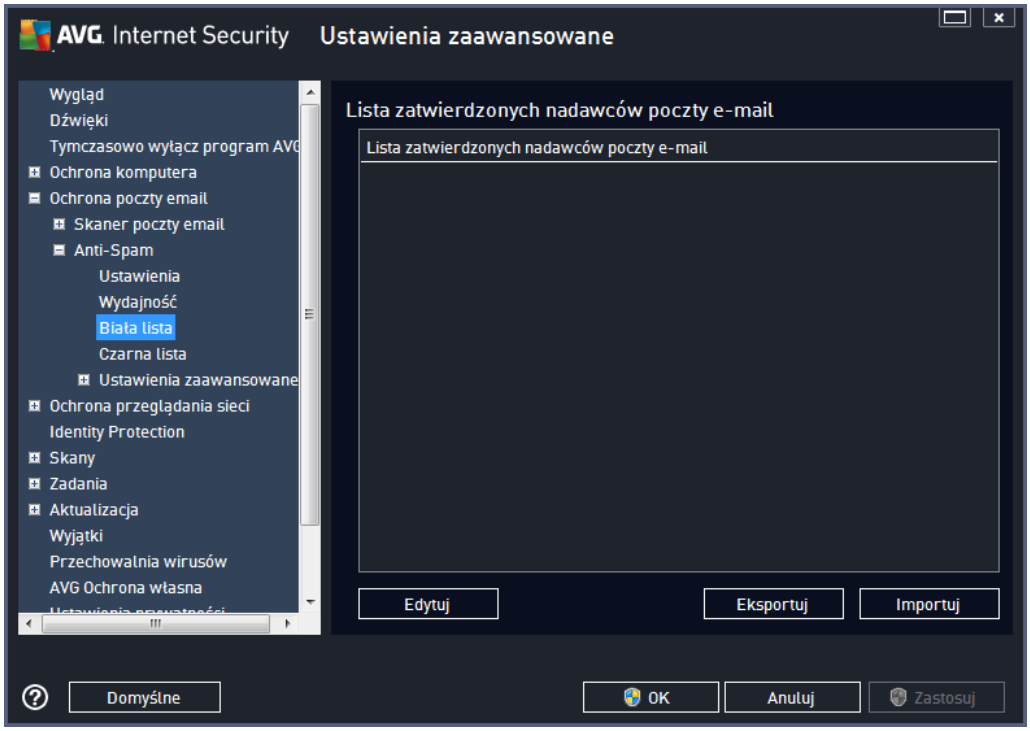
będą brane pod uwagę. Do identyfikacji będą używane tylko dane szkoleniowe. Ten tryb nie jest zalecany do częstego stosowania, chyba że konfiguracja sprzętowa komputera jest bardzo słaba.

- ***Komputer wysokiej klasy*** – tryb ten pochłonie znaczne ilości pamięci. W czasie skanowania w poszukiwaniu spamu stosowane będą następujące funkcje: pamięć podręczna dla reguł i definicji spamu, reguły podstawowe i zaawansowane, adresy IP spamerów i inne bazy danych.

Opcja ***Włącz sprawdzanie online*** jest domyślnie włączona. Pozwala ona skuteczniej wykrywać spam dzięki współpracy z serwerami Mailshell. Skanowane dane są porównywane z bazami danych online firmy Mailshell.

Zwykle zaleca się zachowanie ustawień domyślnych i zmienianie ich tylko w uzasadnionych przypadkach. Wszelkie zmiany konfiguracji powinny być wprowadzane wyłącznie przez użytkowników, którzy doskonale wiedzą, co robią!

Kliknięcie elementu ***Biała lista*** pozwala otworzyć okno dialogowe ***Lista zatwierdzonych nadawców poczty e-mail*** zawierające listę akceptowanych adresów nadawców i nazw domen, z których wysyłane wiadomości nigdy nie są oznaczane jako spam.



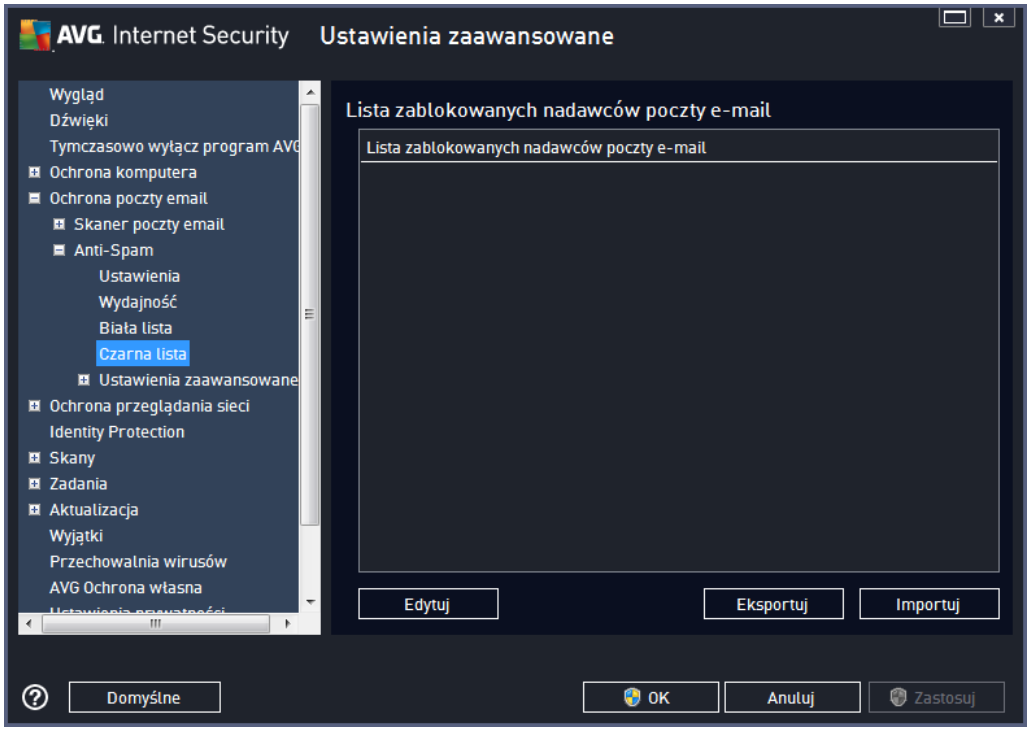
W interfejsie tym można utworzyć listę nadawców, którzy nigdy nie wysyłają niepożądanych wiadomości (spamu). Można także utworzyć listę nazw całych domen (np. *avg.com*), które nie wysyłają spamu. Jeśli lista adresów nadawców i/lub nazw domen jest już gotowa, jej elementy można wprowadzać pojedynczo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

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-wklej*). Każdą pozycję (*nadawcę lub nazwę domeny*) należy wprowadzić w osobnym wierszu.
- ***Eksportuj*** – jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zastaną zapisane w zwykłym pliku tekstowym.
- ***Importuj*** – jeżeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, można go zaimportować za pomocą tego przycisku. Pliku 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 zawsze są oznaczane jako spam.



W interfejsie tym można utworzyć listę nadawców, którzy wysyłają lub prawdopodobnie będą wysyłali niepożądane wiadomości *(spam)*. Można także utworzyć listę pełnych nazw domen (*np. spammingcompany.com*), z których otrzymujesz (lub spodziewasz się otrzymywać) spam. Wszystkie wiadomości e-mail wysłane z 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 na raz.

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-wklej*). Każdą pozycję (*nadawcę lub nazwę domeny*) należy wprowadzić w osobnym wierszu.
- ***Eksportuj*** – jeżeli z jakiegoś powodu chcesz wyeksportować wpisy, można użyć przycisku Eksportuj. Wszystkie wpisy zastaną zapisane w zwykłym pliku tekstowym.
- ***Importuj*** – jeżeli posiadasz plik tekstowy z adresami e-mail lub nazwami domen, można go zaimportować za pomocą tego przycisku.

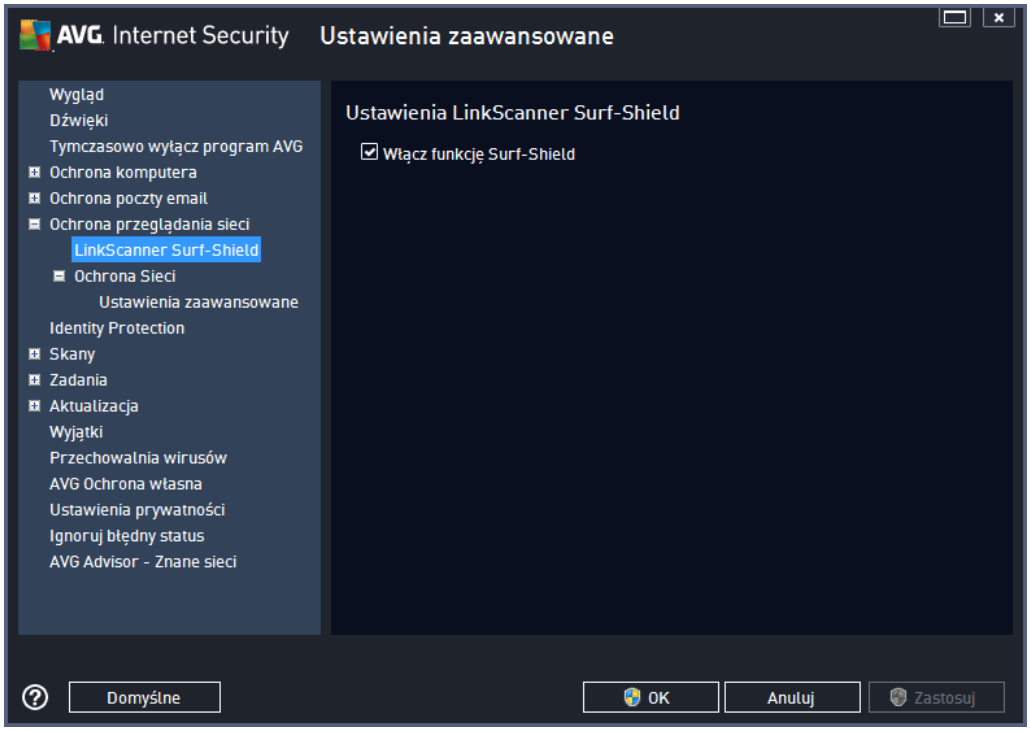
Gałąź Ustawienia eksperta zawiera wiele dodatkowych opcji funkcji Anti-Spam. Ustawienia te są przeznaczone wyłącznie dla doświadczonych użytkowników (zwykle administratorów sieci), którzy chcą szczegółowo skonfigurować filtry antyspamowe w celu uzyskania optymalnej ochrony serwerów poczty. Z tego względu nie istnieją tematy pomocy dla poszczególnych okien dialogowych, a jedynie krótkie opisy odpowiednich opcji, dostępne bezpośrednio w interfejsie użytkownika. Stanowczo zalecamy pozostawienie tych ustawień bez zmian, jeśli nie posiadasz pełnej wiedzy na temat zaawansowanych ustawień silnika antyspamowego Spamcatcher (MailShell Inc.). Nieodpowiednie zmiany mogą skutkować obniżoną wydajnością lub nieprawidłowym działaniem składnika.

Aby mimo wszystko zmienić konfigurację składnika Anti-Spam na bardzo zaawansowanym poziomie, należy postępować zgodnie z instrukcjami wyświetlanymi w interfejsie użytkownika. W każdym oknie znajdziesz jedną, konkretną funkcję, którą możesz edytować. Jej opis jest zawsze widoczny w tym samym oknie. Możesz edytować następujące parametry:

- ***Filtry*** – lista języków, lista krajów, akceptowane adresy IP, zablokowane adresy IP, zablokowane kraje, zablokowane zestawy znaków, fałszywi nadawcy
- ***RBL*** – serwery RBL, trafienia wielokrotne, próg, limit czasu, maksymalna liczba adresów IP
- ***Połączenie internetowe*** – limit czasu, serwer proxy, uwierzytelnianie na serwerze proxy

9.6. Ochrona przeglądania sieci

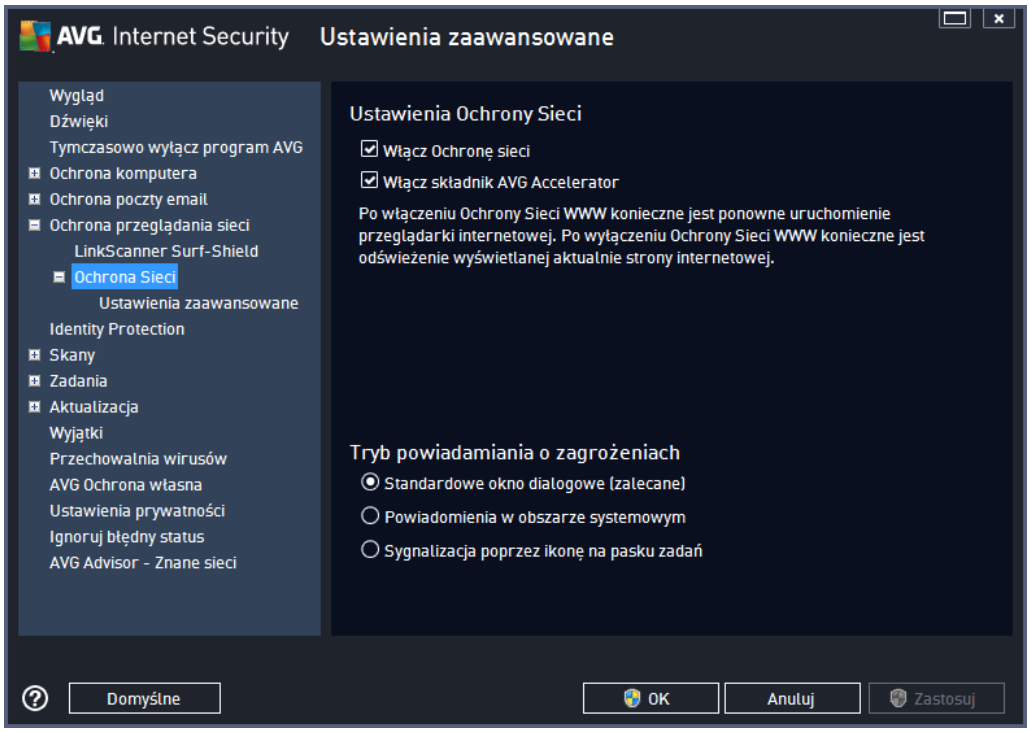
Okno ***Ustawienia LinkScanner*** pozwala zaznaczyć/odznaczyć następujące funkcje:



- ***Włącz funkcję Surf-Shield*** (*domyślnie włączona*) – aktywna ochrona przed niebezpiecznymi witrynami napotykanymi w internecie (*w czasie rzeczywistym*). Znane złośliwe witryny i ich niebezpieczna zawartość blokowane są już w momencie otwarcia ich przez użytkownika za pomocą przeglądarki (*lub jakiejkolwiek innej aplikacji korzystającej z protokołu HTTP*).

- ***Dodaj informację „Zabezpieczone przez LinkScanner”...*** (*opcja domyślnie wyłączona*) – zaznacz tę opcję, aby zapewnić, że wszystkie wiadomości wysyłane za pośrednictwem sieci społecznościowych Facebook/MySpace, które zawierają aktywne łącza, będą certyfikowane przez LinkScanner.

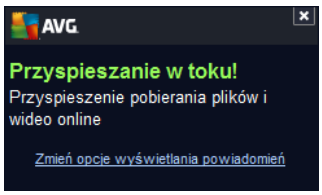
9.6.1. Ochrona Sieci



Okno ***Ochrona Sieci*** zawiera następujące opcje:

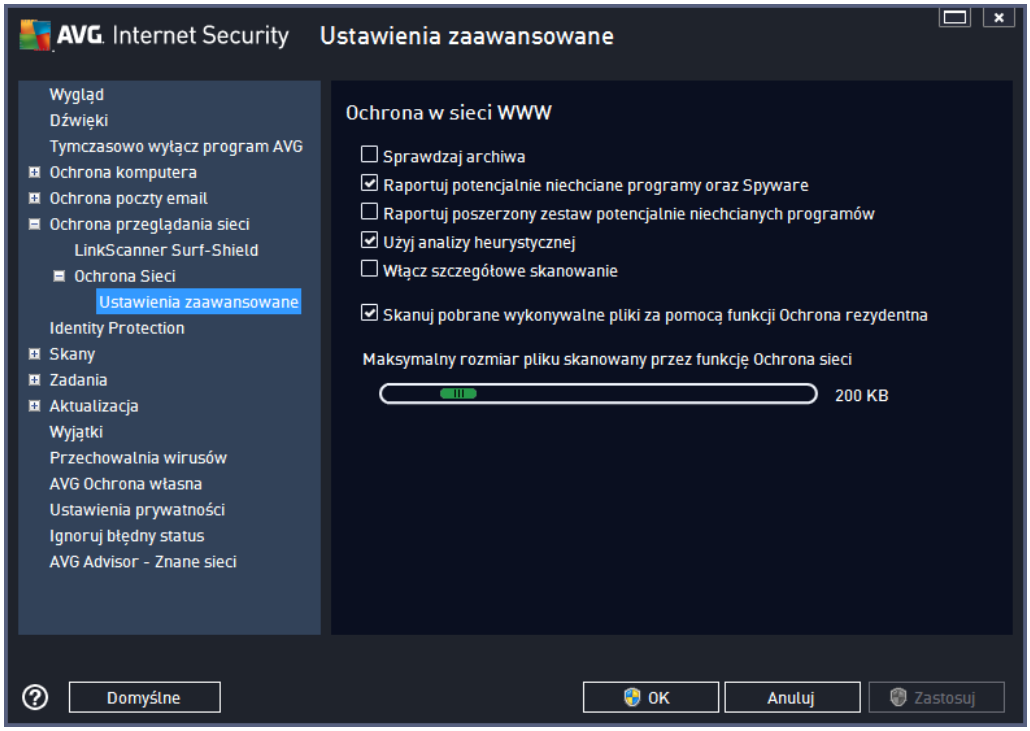
- ***Włącz Ochronę Sieci*** *(domyślnie włączona)* – Włącza/wyłącza wszystkie usługi składnika ***Ochrona Sieci***. Zaawansowane ustawienia ***Ochrony Sieci*** znajdują się w kolejnym oknie, nazwanym Web Protection.

- ***Włącz AVG Accelerator*** *(domyślnie włączony)* – Włącza/wyłącza usługę AVG Accelerator. AVG Accelerator pozwala na płynniejsze odtwarzanie filmów online i łatwiejsze pobieranie dodatkowych plików. W czasie działania składnika AVG Accelerator wyświetlane będzie odpowiednie powiadomienie nad Ikoną AVG na pasku zadań:



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 sieci WWW*** można edytować konfigurację dotyczącą skanowania zawartości witryn internetowych. Interfejs pozwala modyfikować następujące ustawienia:

- ***Sprawdzaj archiwa*** – (*opcja domyślnie wyłączona*) – skanowanie ma obejmować także archiwa zawarte na wyświetlanych stronach WWW.

- ***Raportuj potencjalnie niechciane programy oraz Spyware*** – (*opcja domyślnie włączona*) – zaznaczenie tego pola umożliwi 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 wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj poszerzony zestaw potencjalnie niechcianych programów*** – (opcja 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 Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też domyślnie jest wyłączona.

- ***Użyj heurystyki*** – (*opcja domyślnie włączona*) – skanowanie zawartości wyświetlanych stron ma wykorzystywać analizę heurystyczną (*dynamiczną emulację instrukcji skanowanego obiektu w wirtualnym środowisku*).

- ***Włącz szczegółowe skanowanie*** – (*opcja domyślnie wyłączona*) – w określonych sytuacjach (*gdy zachodzi podejrzenie, że komputer jest zainfekowany*) można

zaznaczyć tę opcję, aby aktywować dokładniejsze algorytmy skanowania. W celu uzyskania absolutnej pewności będą one skanować nawet te obszary komputera, dla których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

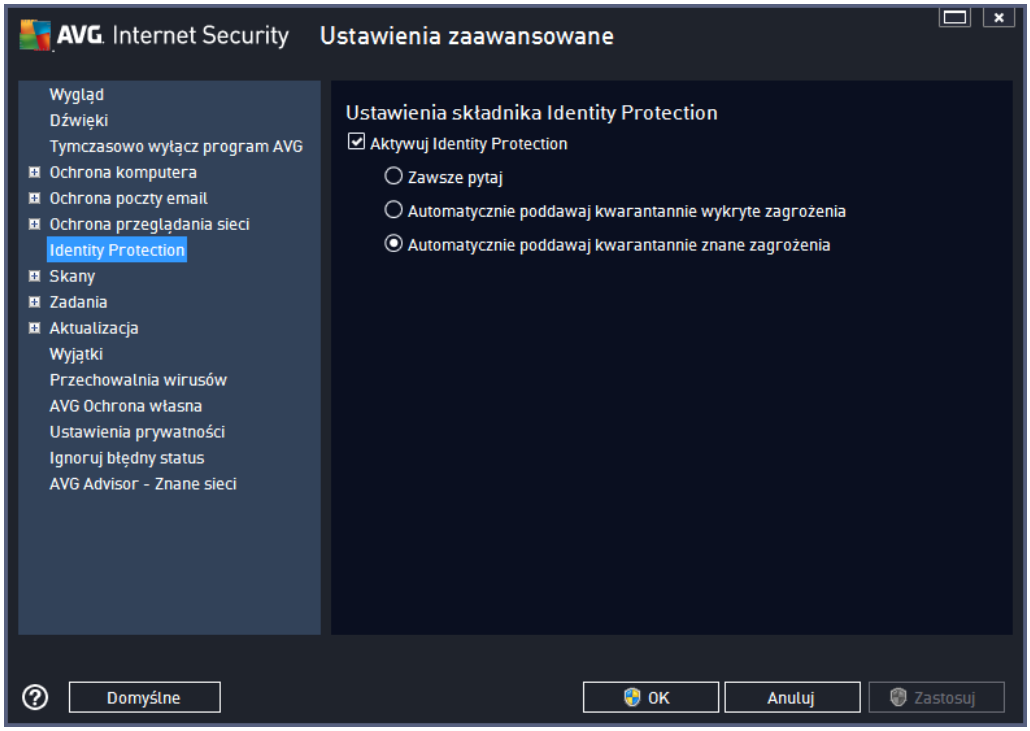
- ***Skanuj pobrane pliki wykonywalne za pomocą Ochrony rezydentnej*** – (*opcja domyślnie włączona*) – służy do skanowania plików wykonywalnych *(zwykle są to pliki o rozszerzeniach exe, bat, com)* po ich pobraniu. Działanie Ochrony rezydentnej polega na skanowaniu plików przed ich pobraniem w celu zapewnienia, że żaden złośliwy kod nie dostanie się do komputera. Ten rodzaj skanowania jest jednak ograniczony wartością opcji ***Maksymalny rozmiar części skanowanego pliku*** – zobacz następny element w tym oknie dialogowym. Z tego względu duże pliki są skanowane częściami (dotyczy to także większości plików wykonywalnych. Pliki wykonywalne mogą wykonywać różne zadania w komputerze, dlatego powinny być w 100% bezpieczne. Ich bezpieczeństwo można zapewnić, skanując ich części 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 większości przypadków nie będzie jednak możliwe zbadanie pliku wykonywalnego jako całości, co może czasami prowadzić do wyświetlania fałszywych alarmów.

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

9.7. Identity Protection

Identity to składnik chroniący Cię 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 włączona*) – można usunąć zaznaczenie tego pola, aby wyłączyć składnik Identity.

Stanowczo odradza się wyłączanie tej funkcji bez uzasadnionej przyczyny!

Jeśli składnik Identity Protection jest aktywny, można określić jego zachowanie w przypadku wykrycia zagrożenia:

- ***Zawsze monituj*** (*opcja domyślnie włączona*) – w przypadku wykrycia zagrożenia użytkownik zostanie zapytany, czy dany proces ma zostać poddany kwarantannie. Dzięki temu aplikacje, które mają pozostać uruchomione, nie zostaną usunięte.

- ***Automatycznie poddawaj kwarantannie wykryte zagrożenia*** – zaznacz to pole, aby wszystkie wykryte zagrożenia były natychmiast przenoszone w bezpieczne miejsce (do Przechowalni wirusów). Jeśli ustawienia domyślne zostaną zachowane, w przypadku wykrycia zagrożenia użytkownik zostanie zapytany, czy dany proces ma zostać przeniesiony do kwarantanny. Dzięki temu aplikacje, które mają pozostać uruchomione, nie zostaną usunięte.

- ***Automatycznie poddawaj kwarantannie znane zagrożenia*** – tylko znane zagrożenia będą automatycznie poddawane kwarantannie (przenoszone do Przechowalni wirusów).

9.8. Skany

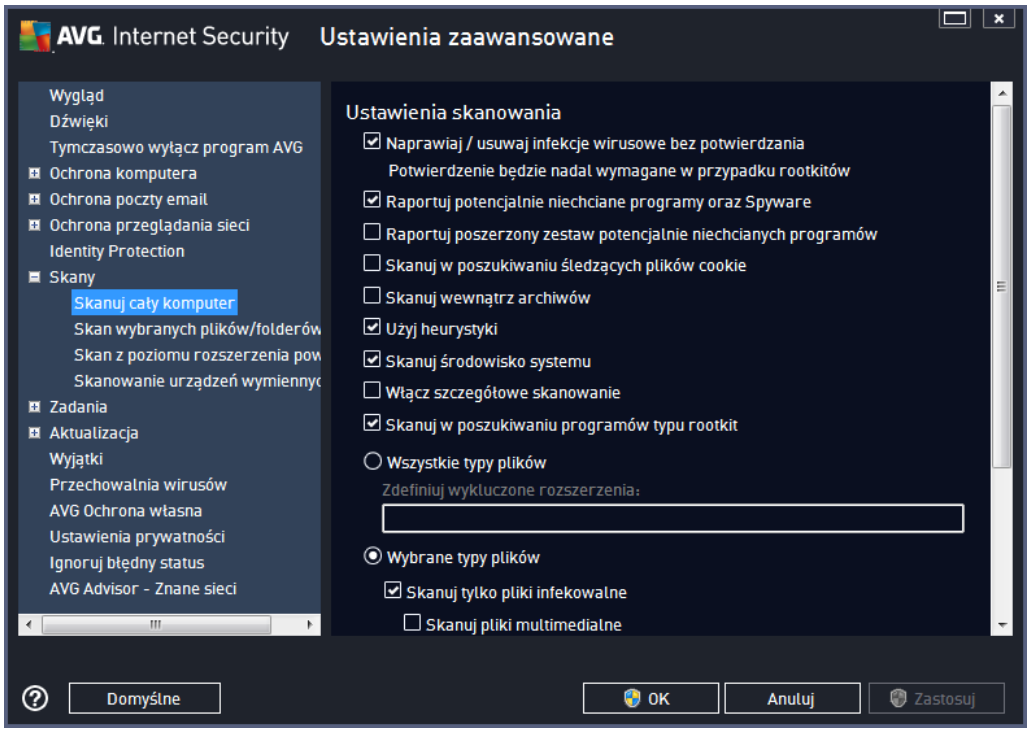
Zaawansowane ustawienia skanowania są podzielone na cztery kategorie odnoszące się do określonych typów testów:

- Skan całego komputera – standardowe, zdefiniowane wstępnie skanowanie całego komputera.

- Skan wybranych plików lub folderów – standardowe, zdefiniowane wstępnie skanowanie wskazanych obszarów komputera
- Skan rozszerzenia powłoki – skanowanie wybranych obiektów bezpośrednio z interfejsu Eksploratora Windows.
- Skan urządzeń wymiennych – skanowanie urządzeń wymiennych podłączonych do komputera.

9.8.1. Skan całego komputera

Opcja ***Skan całego komputera*** umożliwia edycję parametrów jednego z testów zdefiniowanych wstępnie przez dostawcę oprogramowania, tj. Skan całego komputera:



Ustawienia skanowania

Obszar ***Ustawienia skanowania*** zawiera listę parametrów skanowania, które można włączać i wyłączać:

- ***Naprawiaj / usuwaj infekcje wirusowe bez potwierdzania*** (*opcja domyślnie włączona*) – jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do Przechowalni wirusów.
- ***Raportuj potencjalnie niechciane programy oraz Spyware*** (opcja domyślnie włączona) – zaznacz to pole, aby włączyć skanowanie w poszukiwaniu oprogramowania szpiegującego, a także wirusów. Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale

niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj poszerzony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) – zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego: 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 też domyślnie jest wyłączona.

- ***Skanuj w poszukiwaniu śledzących plików cookie*** (*opcja domyślnie wyłączona*) – ten parametr określa, czy pliki cookie mają być wykrywane; (*pliki cookie w protokole HTTP używane są do uwierzytelniania, śledzenia i przechowywania określonych informacji o użytkownikach, np. ustawień witryny i zawartości koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** (*domyślnie wyłączone*) – parametr ten określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) – analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** (*domyślnie włączone*) – skanowanie obejmie także obszary systemowe komputera.

- ***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 pewności będą 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 włączone*) – 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 skanować

- ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików (*po zapisaniu przecinki zostają zamienione na średniki*), które mają być pomijane;

- ***Wybrane typy plików*** – skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio – jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje)*. Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

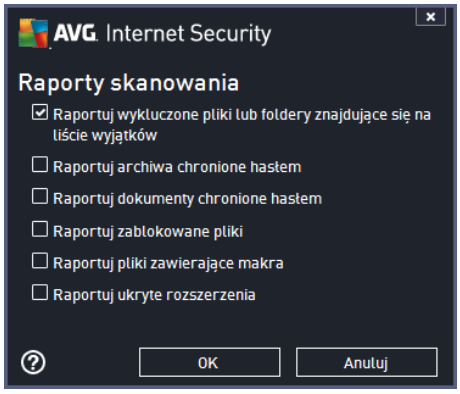
- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** – ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

Określ, jak długo ma trwać skanowanie

W obszarze ***Określ, jak długo ma trwać skanowanie*** można określić żądaną szybkość skanowania, która zależna jest od poziomu wykorzystania zasobów systemowych. Domyślna wartość tej opcji to poziom *Zależny 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 (*opcji można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

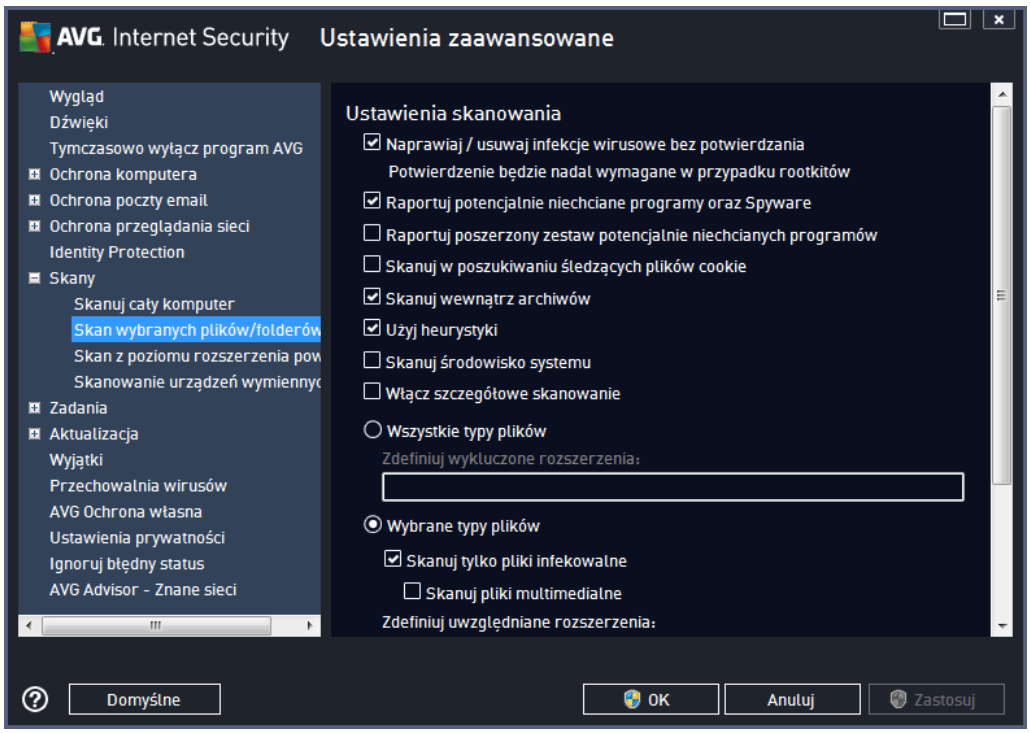
Ustaw dodatkowe raporty skanowania...

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



9.8.2. Skan wybranych plików/folderów

Interfejs konfiguracji ***Skanu wybranych plików lub folderów*** jest identyczny jak w przypadku okna Skan całego komputera. Wszystkie opcje konfiguracyjne są takie same, jednak ustawienia domyślne dla Skanu całego komputera są bardziej rygorystyczne:

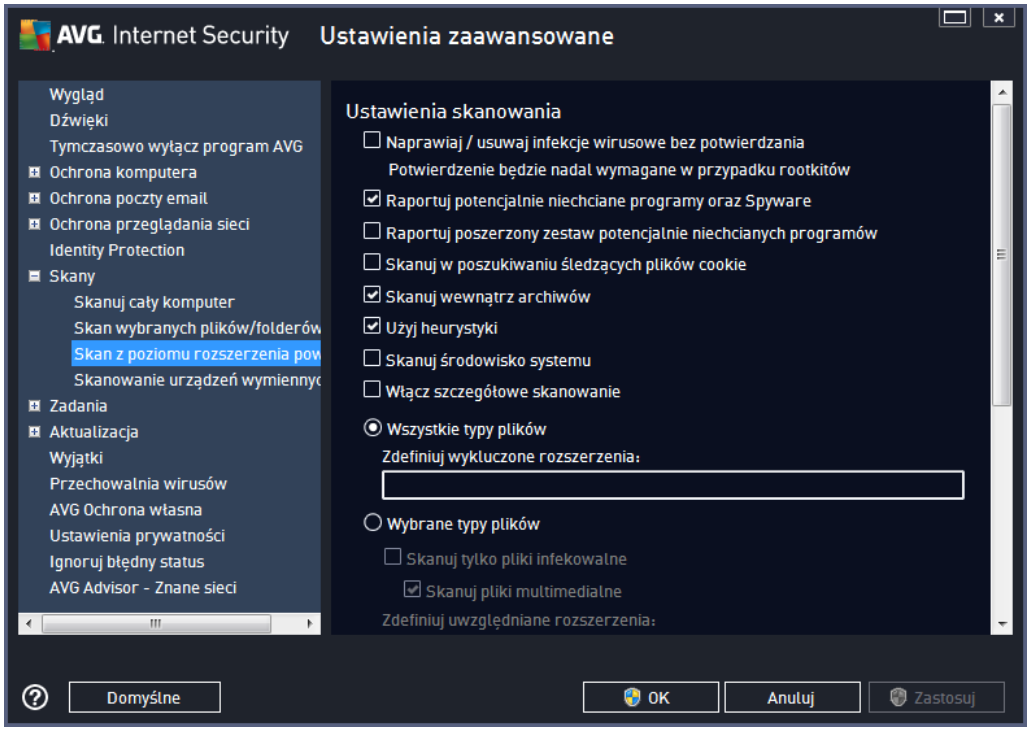


Wszystkie parametry ustawiane w tym oknie dialogowym odnoszą się tylko do obszarów wybranych do Skanowania określonych plików lub folderów!

Uwaga: *Opis poszczególnych parametrów zawiera rozdział Zaawansowane ustawienia AVG / Skany / Skan całego komputera.*

9.8.3. Skan rozszerzenia powłoki

Analogicznie do elementu Skan całego komputera, test ***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:



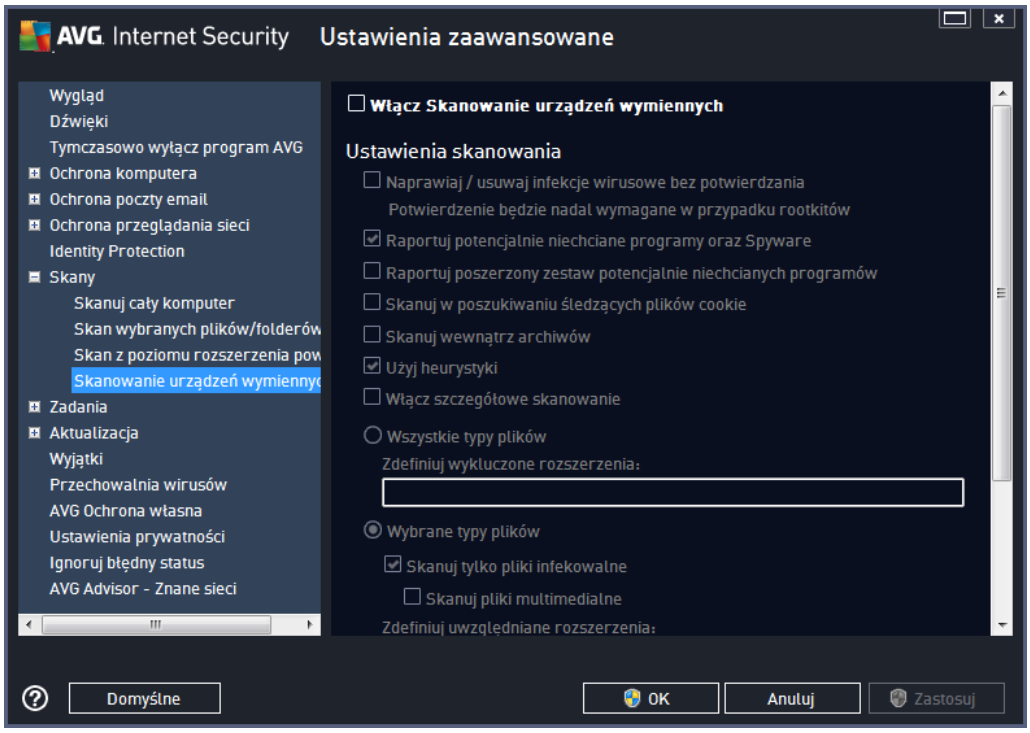
Lista parametrów jest identyczna jak dla Skan całego komputera. Jednak ustawienia domyślne obu skanów różnią się (*np. Skan całego komputera nie sprawdza archiwów, lecz skanuje środowisko systemowe, podczas gdy Skan rozszerzenia powłoki – odwrotnie*).

Uwaga: *Opis poszczególnych parametrów zawiera rozdział Zaawansowane ustawienia AVG / Skany / Skan całego komputera.*

Podobnie jak w przypadku okna Skan całego komputera, okno dialogowe ***Skan rozszerzenia powłoki*** również zawiera sekcję o nazwie ***Inne ustawienia...***, w której można określić, czy informacje o postępie 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.

9.8.4. Skan 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 są one częstym źródłem infekcji. Jeśli skan ma być uruchamiany automatycznie, należy zaznaczyć opcję ***Włącz skanowanie urządzeń wymiennych***.

Uwaga: *Opis poszczególnych parametrów zawiera rozdział Zaawansowane ustawienia AVG / Skany / Skan całego komputera.*

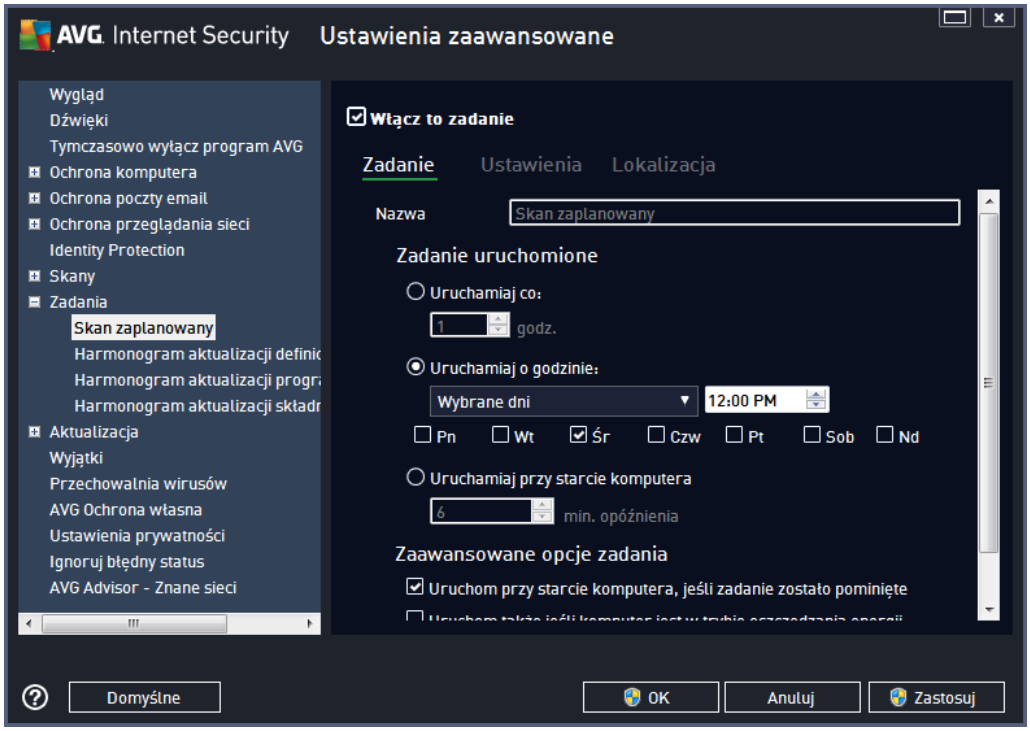
9.9. Zaplanowane zadania

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

- Skan zaplanowany
- Harmonogram aktualizacji definicji
- Harmonogram aktualizacji programu
- Harmonogram aktualizacji składnika Anti-Spam

9.9.1. 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 zaplanowany test lub włączyć go ponownie, gdy zajdzie taka potrzeba:



W polu tekstowym Nazwa (nieaktywne dla 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 krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości.

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

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

Zadanie uruchomione

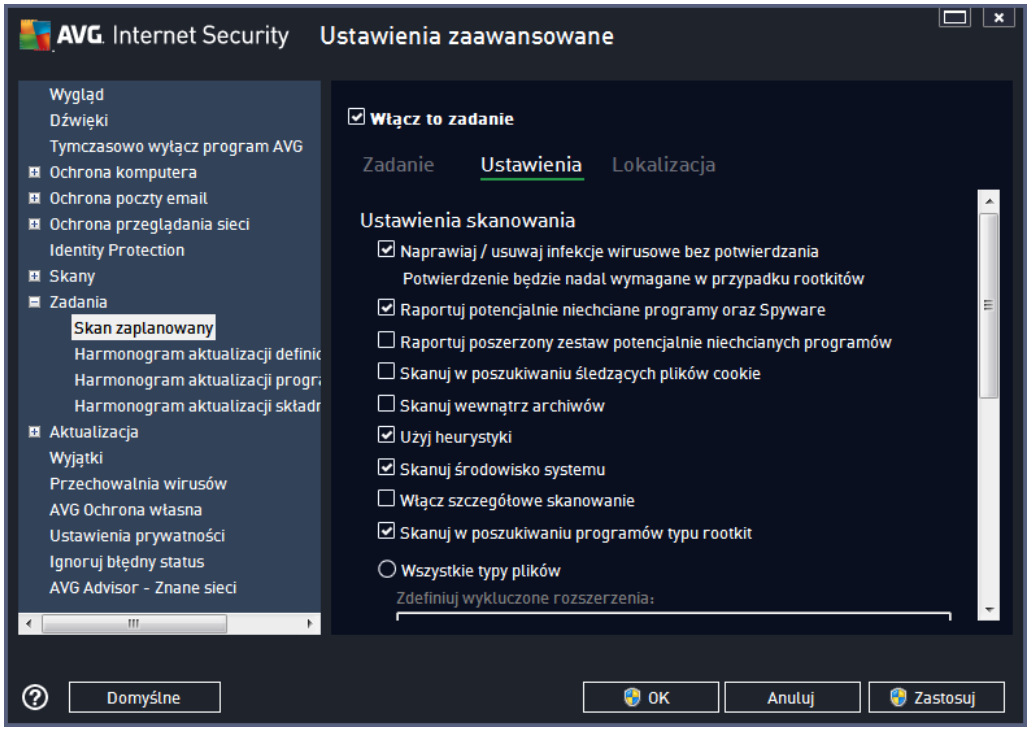
W tym miejscu można określić, jak często ma być uruchamiane nowe skanowanie. Uruchamianie skanowania może być powtarzane w określonych odstępach czasu (***Uruchamiaj co...***) lub w zadanych momentach (***Uruchamiaj o określonej godzinie...***), a także na skutek wystąpienia

określonego zdarzenia (***Akcja powiązana z uruchomieniem komputera***).

Zaawansowane opcje harmonogramu

Ta sekcja umożliwia zdefiniowanie warunków uruchamiania skanowania w czasie, gdy komputer pracuje w trybie oszczędzania energii lub jest wyłączony. Po rozpoczęciu zaplanowanego skanu, nad ikoną AVG na pasku zadań wyświetlone zostanie odpowiednie powiadomienie.

Następnie pojawi się nowa ikona AVG na pasku zadań (*kolorowa, z białą strzałką – jak powyżej*), 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.



Karta ***Ustawienia*** zawiera listę parametrów silnika skanującego. Domyślnie większość funkcji jest włączona, a odpowiadające im ustawienia są stosowane podczas skanowania. ***Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachowując wstępnie zdefiniowaną konfigurację***:

- ***Naprawiaj / usuwaj infekcje wirusowe bez potwierdzania*** *(opcja domyślnie włączona)* – jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy oraz Spyware*** *(opcja domyślnie włączona)* – zaznacz to pole, aby włączyć skanowanie w poszukiwaniu oprogramowania szpiegującego, a także wirusów. Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych

programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj poszerzony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) – zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego: 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 też 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. ustawień witryn i zawartości koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** (*opcja domyślnie wyłączona*) – ten parametr określa, czy skanowanie ma obejmować wszystkie pliki, nawet te znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) – analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** (*opcja domyślnie włączona*) – skanowanie obejmie także obszary systemowe komputera.

- ***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 pewności będą 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 włączone) – 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 skanować

- ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń plików (*po zapisaniu przecinki zostają zamienione na średniki*), które mają być pomijane.

- ***Wybrane typy plików*** – skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio – jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje)*. Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

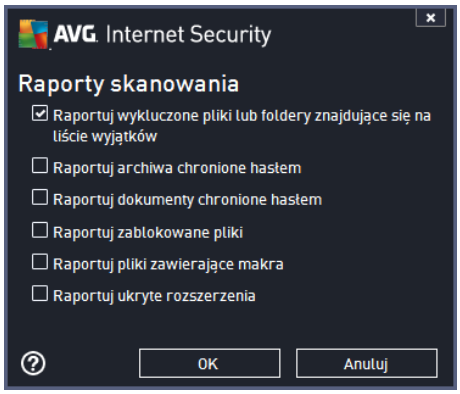
- Opcjonalnie można zdecydować o ***skanowaniu plików bez rozszerzenia*** – ta opcja jest domyślnie włączona i zaleca się niezmienianie tego stanu bez ważnego powodu. Pliki bez rozszerzenia są podejrzane i powinny być skanowane za każdym razem.

Określ, jak długo ma trwać skanowanie

W tej sekcji można szczegółowo określić żądaną prędkość skanowania, w zależności od wykorzystania zasobów systemowych. Domyślna wartość to priorytet *Zależny 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 (*opcji można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

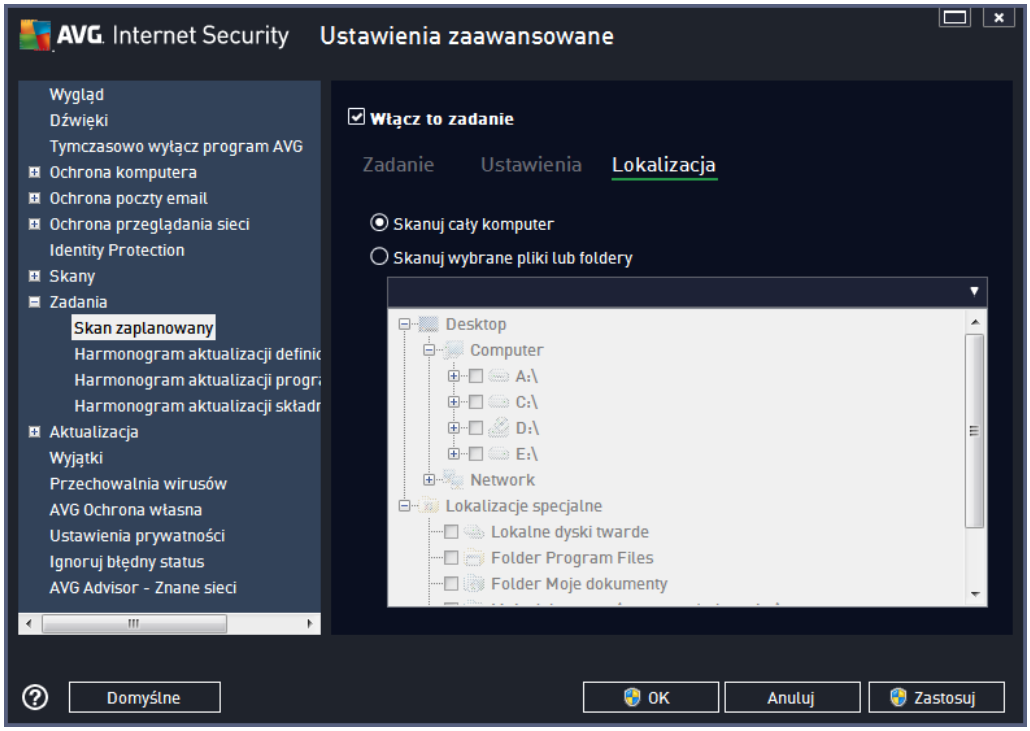
Ustaw dodatkowe raporty skanowania

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



Opcje zamykania komputera

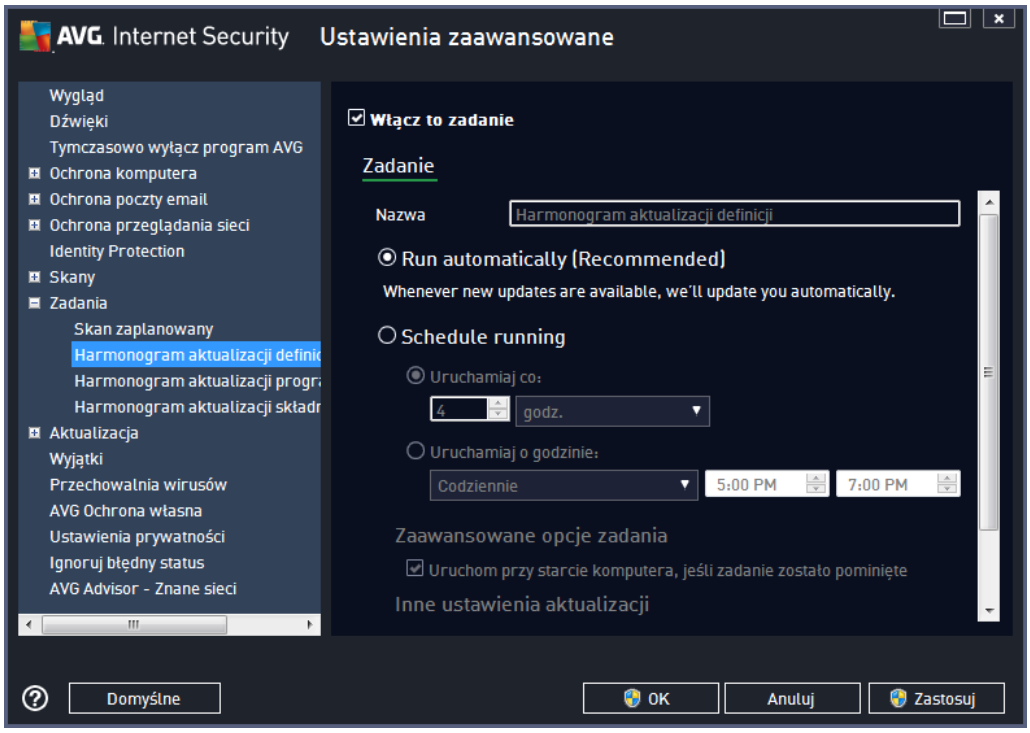
W sekcji ***Opcje zamykania komputera*** będziesz mógł zdecydować, czy chcesz, by komputer został automatycznie wyłączony po zakończeniu bieżącego procesu skanowania. Wybranie opcji (***Zamknij komputer po ukończeniu skanowania***) spowoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet 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.

9.9.2. 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 dobry powód, aby zrobić inaczej! Następnie możesz skonfigurować ręczne uruchomienie zadania i określić odstępy czasowe uruchomień nowo zaplanowanych aktualizacji definicji. Można zaplanować uruchamianie aktualizacji stale co pewien czas (***Uruchom co ...***) lub definiując określoną datę i godzinę (***Uruchom o określonej godzinie ...***).

Zaawansowane opcje harmonogramu

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

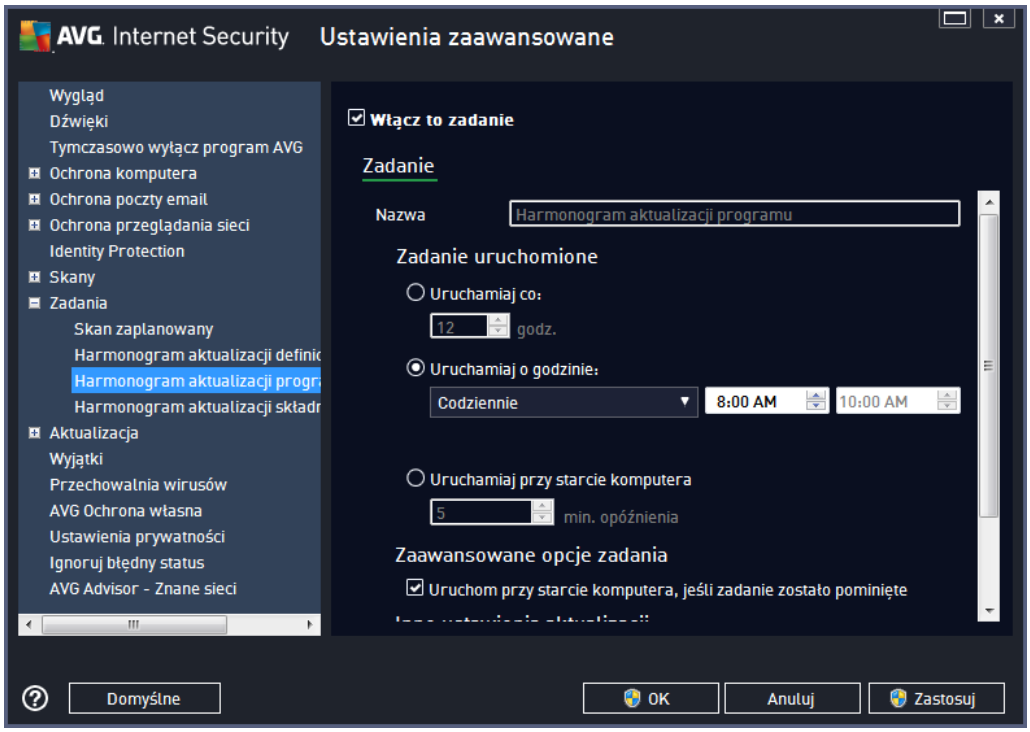
Inne ustawienia aktualizacji

Na koniec należy zaznaczyć 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*).

9.9.3. Harmonogram aktualizacji programu

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



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

Zaawansowane opcje harmonogramu

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

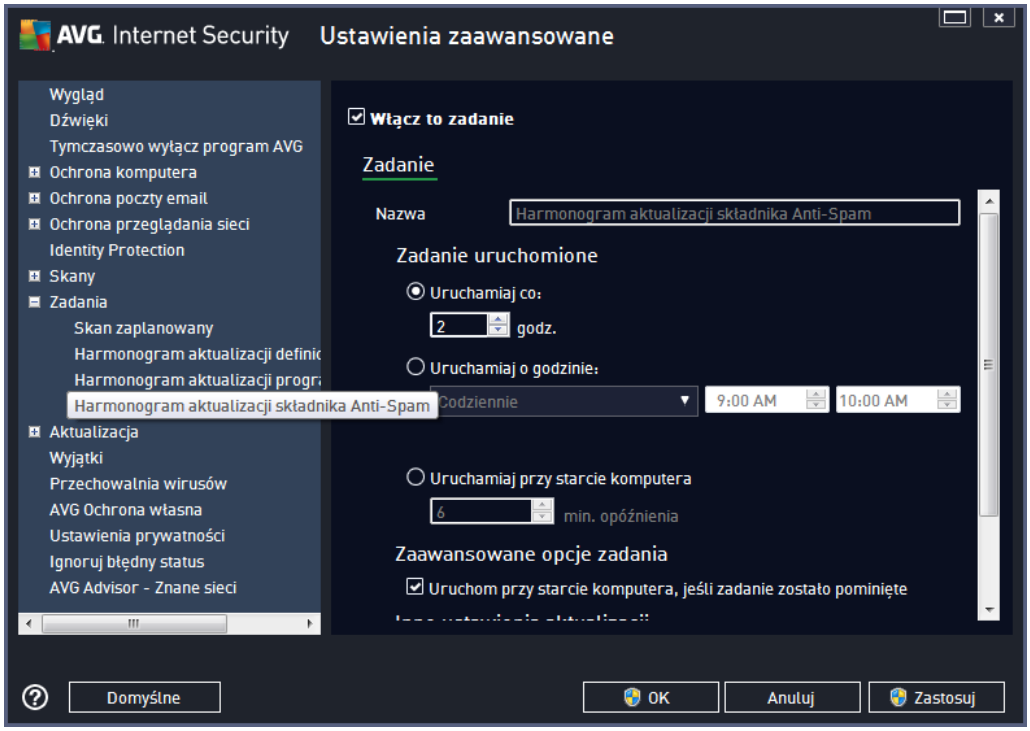
Inne ustawienia aktualizacji

Zaznacz pole wyboru ***Uruchom aktualizację natychmiast po nawiązaniu połączenia z internetem***, aby upewnić się, że aktualizacja zostanie wznowiona po ponownym połączeniu z siecią, jeśli połączenie internetowe zostanie przerwane a proces aktualizacji nie powiedzie się. Po rozpoczęciu zaplanowanego skanowania, nad ikoną AVG na pasku zadań wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji Ustawienia zaawansowane/Wygląd*).

Uwaga: *Jeśli zaplanowane skanowanie i aktualizacja nałożą się, proces aktualizacji będzie miał pierwszeństwo i skanowanie zostanie przerwane. W takiej sytuacji, użytkownik będzie poinformowany o niezgodności.*

9.9.4. Harmonogram aktualizacji składnika Anti-Spam

Jeżeli zajdzie taka potrzeba, możesz skorzystać z pola ***Włącz 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 żądanej godzinie (***Uruchamiaj o określonej godzinie***), a

także na skutek wystąpienia zdefiniowanego zdarzenia (***W oparciu o akcję, np. uruchomienie 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.

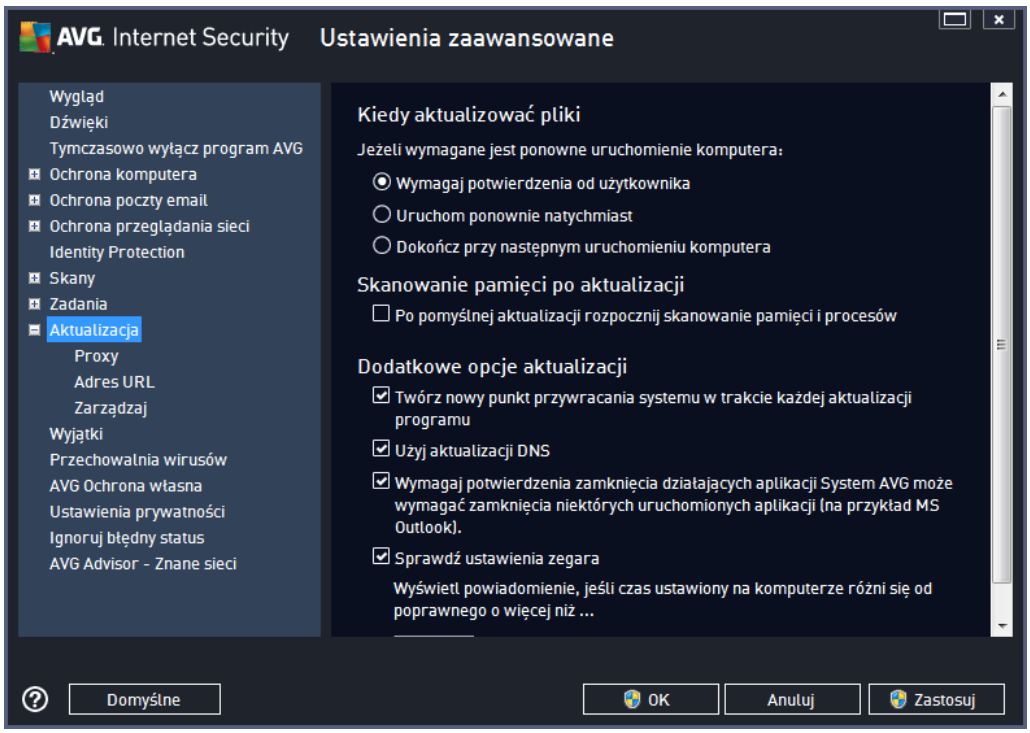
Inne ustawienia aktualizacji

Zaznacz pole wyboru ***Uruchom aktualizację natychmiast po nawiązaniu połączenia z internetem***, aby upewnić się, że aktualizacja zostanie wznowiona po ponownym połączeniu z siecią, jeśli połączenie internetowe zostanie przerwane a proces aktualizacji składnika Anti-Spam nie powiedzie się.

Po rozpoczęciu zaplanowanego skanowania, nad ikoną AVG na pasku zadań wyświetlone zostanie odpowiednie powiadomienie (*przy domyślnej konfiguracji zastosowanej w sekcji Ustawienia zaawansowane/Wygląd*).

9.10. 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 wymagać ponownego uruchomienia komputera. Dokończenie aktualizacji wymaga restartu komputera, który można od razu wykonać:

- ***Wymagaj potwierdzenia od użytkownika*** *(domyślnie)* – przed zakończeniem aktualizacji system zapyta użytkownika o pozwolenie na restart komputera.
- ***Uruchom ponownie natychmiast*** – komputer zostanie automatycznie zrestartowany zaraz po zakończeniu aktualizacji – potwierdzenie ze strony użytkownika nie jest wymagane
- ***Dokończ przy następnym uruchomieniu komputera*** – aktualizacja zostanie automatycznie odłożona i ukończona przy najbliższym restarcie systemu. Należy pamiętać, że tę opcję należy zaznaczyć wyłącznie, jeśli komputer jest regularnie uruchamiany ponownie (co najmniej raz dziennie)!

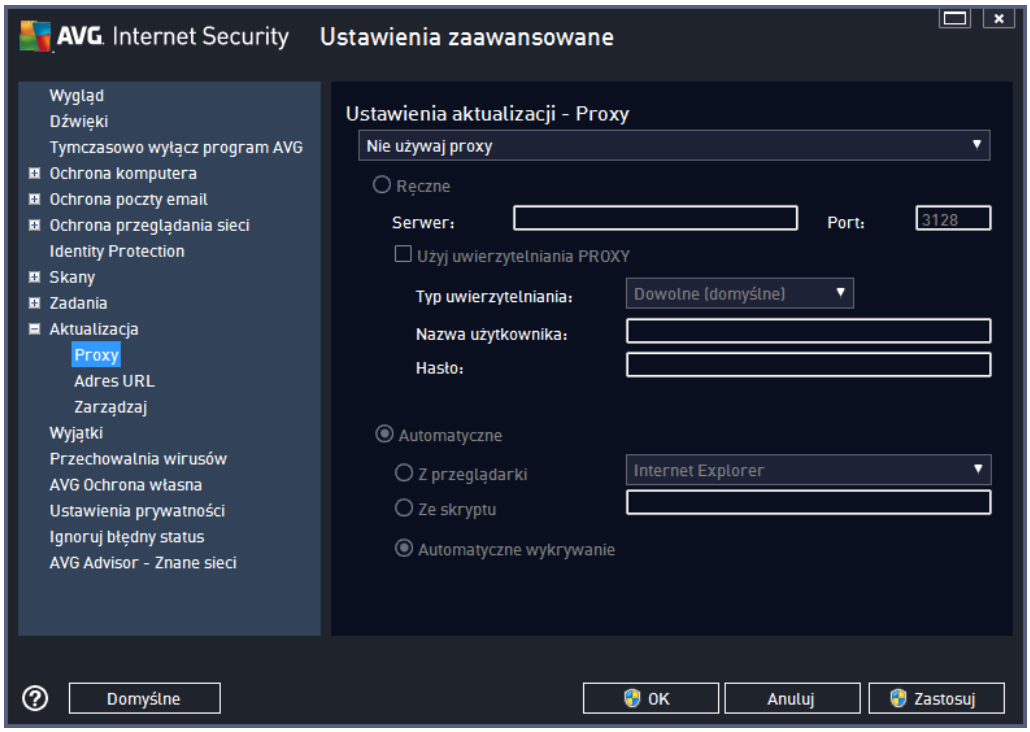
Skanowanie pamięci po aktualizacji

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

Dodatkowe opcje aktualizacji

- ***Twórz nowy punkt przywracania systemu 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: Start / Wszystkie programy / Akcesoria / Narzędzia systemowe / Przywracanie systemu. Nie zalecamy wprowadzania jakichkolwiek zmian niedoświadczonym użytkownikom! Aby korzystać z tej funkcji, pole wyboru musi pozostać zaznaczone.
- ***Użyj aktualizacji DNS*** (*opcja domyślnie włączona*) – gdy to pole jest zaznaczone, przy uruchamianiu aktualizacji system **AVG Internet Security 2014** wyszukuje informacje o najnowszej wersji bazy wirusów i programu na serwerze DNS. Następnie pobierane i instalowane są jedynie niewielkie 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 żadne działające aplikacje nie zostaną zamknięte bez potwierdzenia ze strony użytkownika, jeśli do zakończenia aktualizacji będzie wymagane ponowne uruchomienie komputera.
- ***Sprawdź ustawienia zegara*** (*domyślnie włączone*) – zaznacz to pole jeśli chcesz, aby program AVG wyświetlił powiadomienie, gdy różnica między właściwym a lokalnym czasem komputera przekroczy określoną wartość.

9.10.1. Proxy



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

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

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

Konfiguracja ręczna

W przypadku wybrania konfiguracji ręcznej (zaznaczenie *opcji* ***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 nawiązaniem połączenia.

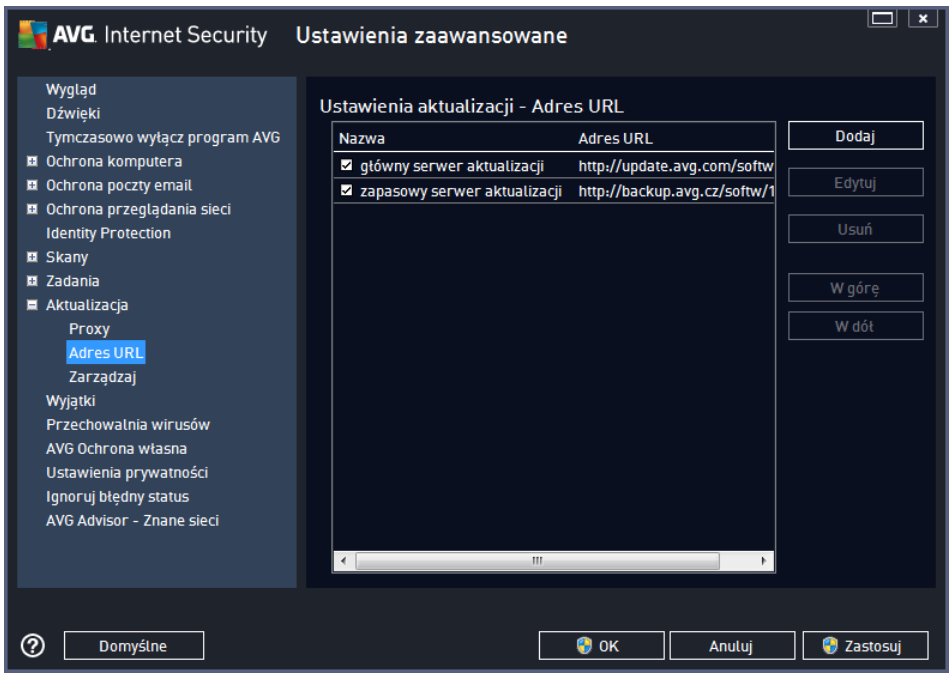
Konfiguracja automatyczna

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

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

9.10.2. URL

W oknie ***URL*** znajduje się lista adresów internetowych, z których będą pobierane pliki aktualizacyjne.



Przyciski kontrolne

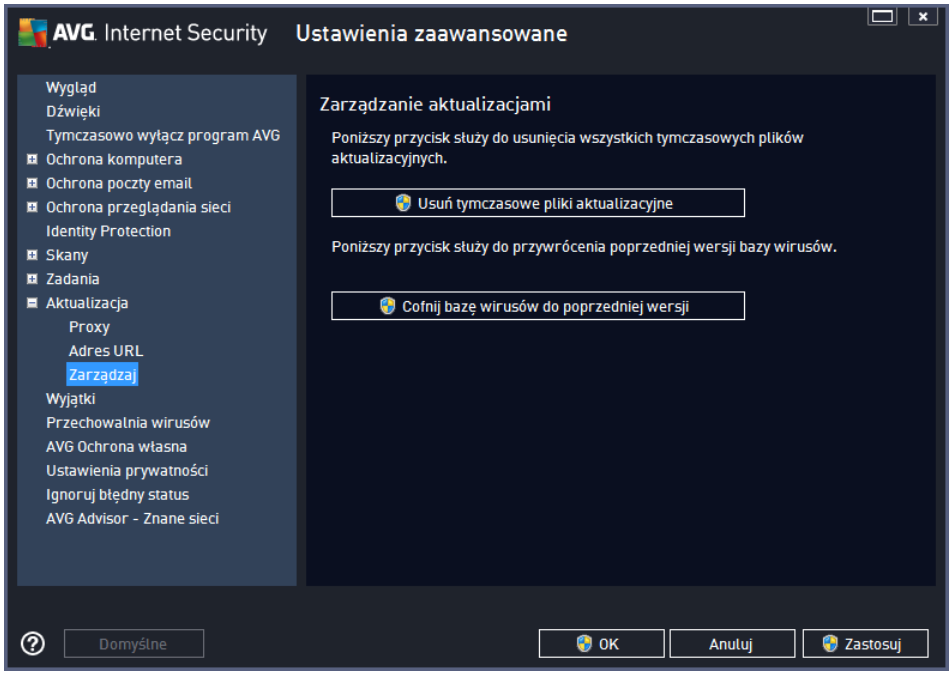
Listę i jej elementy można modyfikować za pomocą następujących przycisków kontrolnych:

- ***Dodaj*** – powoduje otwarcie okna dialogowego umożliwiającego określenie nowego adresu URL, który zostanie dodany do listy

- ***Edytuj*** – powoduje otwarcie okna dialogowego umożliwiającego edycję parametrów wybranego adresu URL
- ***Usuń*** – powoduje usunięcie wybranego adresu URL z listy
- ***W górę*** – przenosi wybrany adres URL o jedną pozycję w górę na liście
- ***W dół*** – przenosi wybrany adres URL o jedną pozycję w dół na liście

9.10.3. 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 bazę wirusów do poprzedniej wersji*** – pozwala usunąć z dysku twardego ostatnią wersję bazy wirusów i przywrócić ją do poprzedniego stanu (*nowa baza będzie częścią najbliższej aktualizacji*).

9.11. Wyjątki

W oknie ***Wyjątki*** można zdefiniować wyjątki, czyli obiekty, które system **AVG Internet Security 2014** powinien ignorować. Zazwyczaj będziesz zmuszony zdefiniować wyjątek, gdy system AVG wciąż 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!

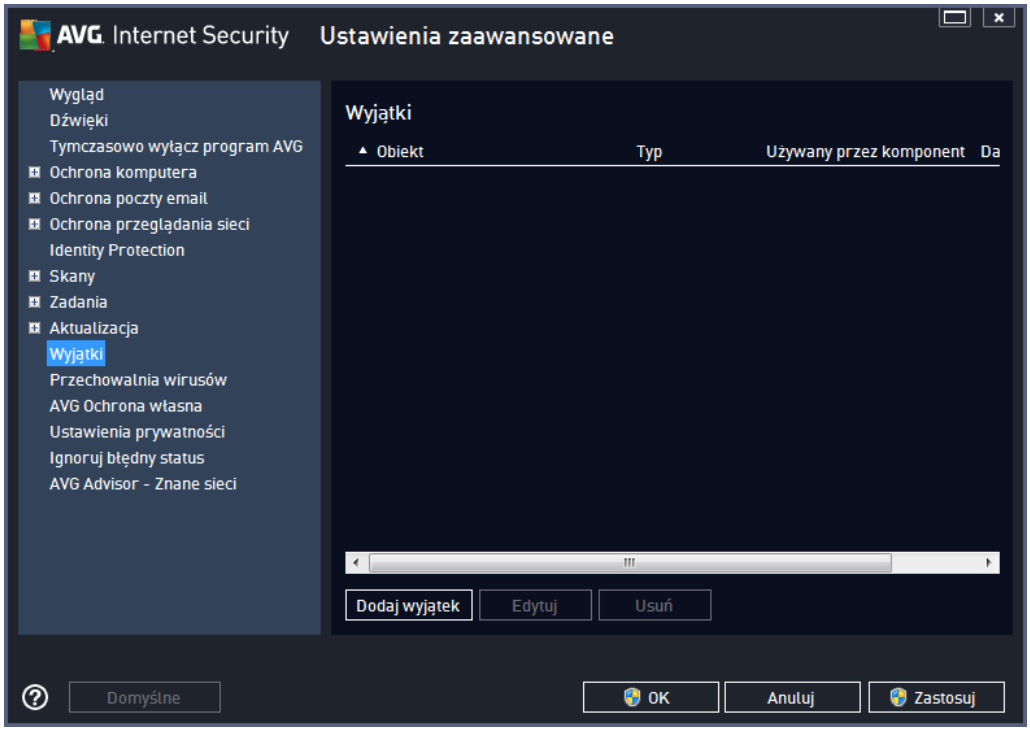


Tabela na tej stronie zawiera listę wyjątków, o ile zostały one już zdefiniowane. Obok każdej pozycji znajduje się pole wyboru. Jeśli pole wyboru jest zaznaczone, obiekt pozostanie wykluczony ze skanowania. Jeśli nie – oznacza to, że wyjątek jest zdefiniowany, ale w danej chwili nie jest aktywny. Klikając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

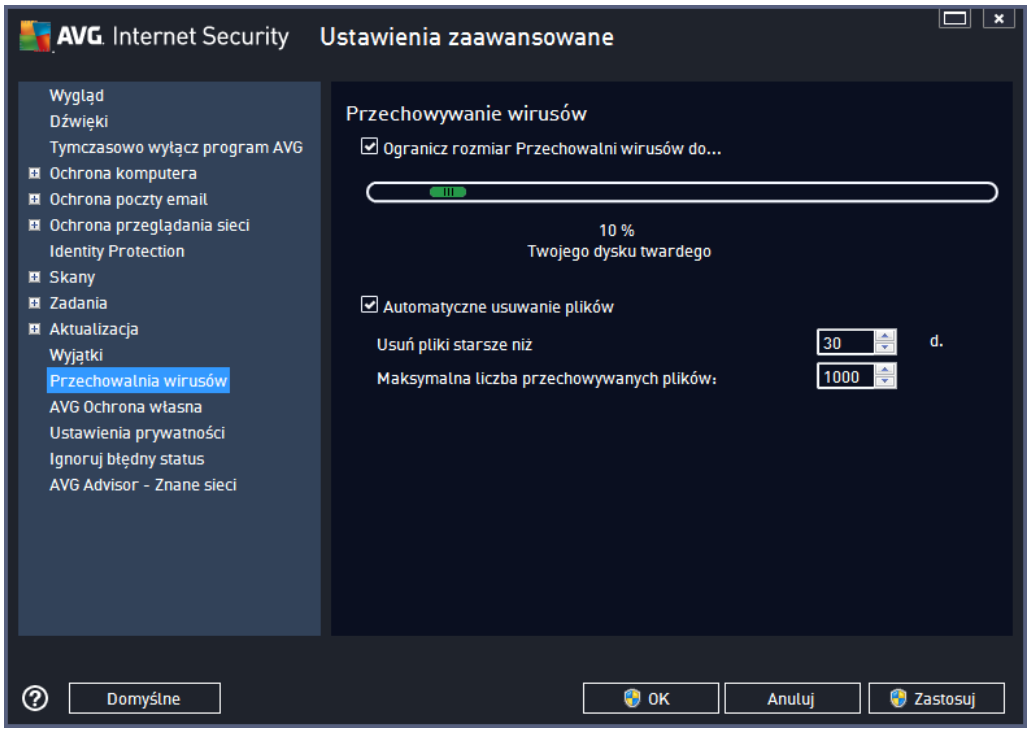
Przyciski kontrolne

- ***Dodaj wyjątek*** – Kliknij ten przycisk, aby otworzyć nowe okno, które umożliwia zdefiniowanie nowego obiektu wykluczonego ze skanowania AVG. W pierwszej kolejności wymagane będzie podanie typu obiektu – czy jest on plikiem, folderem czy adresem URL. Następnie zostaniesz poproszony o wskazanie ścieżki do obiektu na dysku lub wprowadzenie adresu URL. Na końcu możesz także wskazać, które funkcje AVG powinny ignorować wskazany obiekt *(Ochrona rezydentna, Tożsamość, Skaner, Anti-Rootkit)*.

- ***Edytuj*** – Ten przycisk aktywny jest tylko wówczas, gdy zdefiniowane już zostały jakiekolwiek wyjątki i znajdują się one na liście. Użycie tego przycisku spowoduje wówczas otwarcie nowego okna umożliwiającego konfigurację parametrów wybranego wyjątku.

- ***Usuń*** – Użyj tego przycisku, by anulować wcześniej zdefiniowany wyjątek. Możesz usuwać 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. Przypominamy, że usunięty zostanie jedynie wyjątek, a nie sam plik czy folder!

9.12. Przechowalnia wirusów

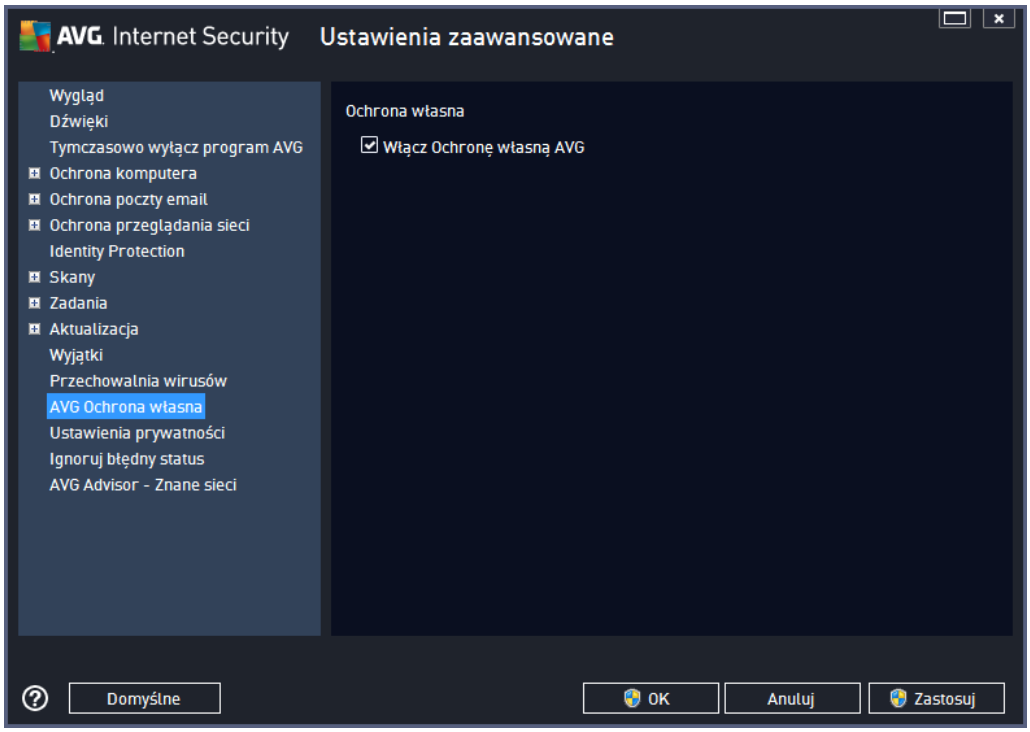


Okno dialogowe ***Przechowalnia wirusów*** pozwala zdefiniować kilka parametrów dotyczących administrowania obiektami znajdującymi się w Przechowalni wirusów:

- ***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 należy zdefiniować maksymalny okres przebywania obiektów w Przechowalni wirusów (***Usuń pliki starsze niż .. dni***) oraz maksymalną liczbę plików, które mogą znajdować się w Przechowalni wirusów (***Maksymalna liczba przechowywanych plików***).

9.13. Ochrona własna AVG

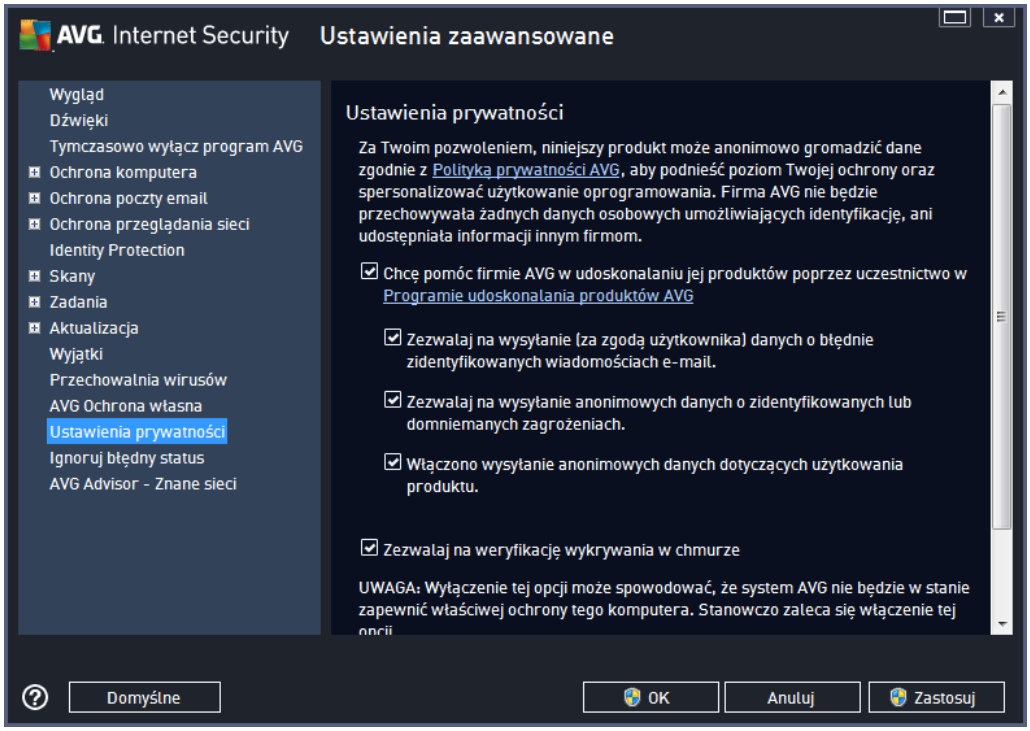


Funkcja ***Ochrona własna AVG*** pozwala systemowi **AVG Internet Security 2014** chronić swoje własne pliki, wpisy rejestru i sterowniki przed modyfikacją lub wyłączeniem. Głównym powodem stosowania tej ochrony jest istnienie pewnych wyszukanych zagrożeń, które próbują rozbroić oprogramowanie antywirusowe, by następnie swobodnie przystąpić do działalności szkodliwej dla komputera.

Zalecamy zachowanie tej funkcji włączonej!

9.14. 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, jeśli mamy im przeciwdziałać. Raportowanie odbywa się automatycznie, a więc nie powinno powodować niedogodności. W raportach nie są zawarte żadne dane osobowe. Zgłaszanie wykrytych zagrożeń jest opcjonalne – prosimy jednak o pozostawienie tej opcji włączonej. 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 poprzez uczestniczenie w Programie udoskonalania produktów*** *(domyślnie włączone)* – jeśli chcesz pomóc nam wciąż udoskonalać **AVG Internet Security 2014**, 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 udoskonalać naszą ochronę. Zgłaszanie witryn obsługiwane jest automatycznie, więc nie powoduje żadnych niedogodności. Raporty nie zawierają także 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 oznaczanych jako spam lub wiadomościach będących spamem, 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 domniemanych 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 użytkowania produktu*** *(opcja domyślnie włączona)* – wysyłanie podstawowych statystyk dotyczących korzystania z aplikacji, takich jak liczba wykrytych zagrożeń, uruchomionych skanów, pomyślnych 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, włączając 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 Ci usługi precyzyjnie dostosowane do Twoich potrzeb, aby zapewnić Ci maksymalne bezpieczeństwo.

Najpopularniejsze zagrożenia

Obecnie istnieje znacznie więcej zagrożeń niż zwykłe wirusy. Autorzy szkodliwych programów i niebezpiecznych witryn internetowych są niezwykle kreatywni, więc nowe rodzaje zagrożeń pojawiają się bardzo często. Zdecydowana większość rozprzestrzenia się samodzielnie poprzez internet. Najpopularniejsze zagrożenia to:

- ***Wirus*** to szkodliwy kod, który tworzy własne kopie i rozprzestrzenia się, często pozostając niezauważonym do czasu, gdy wyrządzi szkody. Niektóre wirusy stanowią poważne zagrożenie (usuwają lub celowo zmieniają napotkane pliki), a inne mają pozornie nieszkodliwe działanie (np. odtwarzają fragment utworu muzycznego). Wszystkie wirusy są jednak niebezpieczne ze względu na swoją podstawową cechę – możliwość mnożenia się. Nawet prosty wirus może w jednej chwili zająć całą pamięć komputera i spowodować awarię systemu.

- ***Robaki*** są podkategorią wirusów i – w przeciwieństwie do swoich tradycyjnych kuzynów – nie potrzebują „nosicieli", do których musiałyby się dołączać; robaki rozsyłają się same na wiele komputerów (zwykle w wiadomościach e-mail) i w efekcie mogą spowodować przeładowanie serwerów pocztowych i systemów sieciowych.

- ***Oprogramowanie szpiegujące*** jest zazwyczaj definiowane jako kategoria szkodliwego oprogramowania (*szkodliwe oprogramowanie to wszelkie złośliwe oprogramowanie, w tym wirusy*) obejmująca programy (zwykle konie trojańskie), których zadaniem jest kradzież danych osobistych (haseł, numerów kart kredytowych) lub przeniknięcie do systemu komputerowego w celu umożliwienia atakującemu przejęcia nad nim kontroli (wszystko oczywiście bez wiedzy lub zgody właściciela komputera).

- ***Potencjalnie niechciane programy*** to rodzaj oprogramowania szpiegującego, które może – ale niekoniecznie musi – być niebezpieczne dla komputera. Specyficznym przykładem PNP jest oprogramowanie reklamowe, przeznaczone do emitowania reklam, zazwyczaj w postaci wyświetlania wyskakujących okienek; irytujące, ale w zasadzie nieszkodliwe.

- ***Również śledzące pliki cookie*** mogą być uznawane za oprogramowanie szpiegujące. Te małe pliki (przechowywane w przeglądarce internetowej i wysyłane do macierzystej witryny przy jej kolejnym odwiedzeniu) mogą zawierać historię przeglądania i tym podobne informacje.

- ***Exploity*** – szkodliwe programy wykorzystujące luki w systemie operacyjnym, przeglądarce internetowej lub innym programie.

- ***Phishing*** – próba zdobycia poufnych informacji poprzez podszywanie się pod wiarygodną i znaną organizację. Zazwyczaj kontakt z potencjalnymi ofiarami następuje przy użyciu masowo wysyłanych wiadomości e-mail zawierających np. prośbę o uaktualnienie

szczegółów rachunku bankowego. Aby to zrobić, odbiorcy są proszeni o kliknięcie łącza prowadzącego do fałszywej strony internetowej udającej witrynę banku.

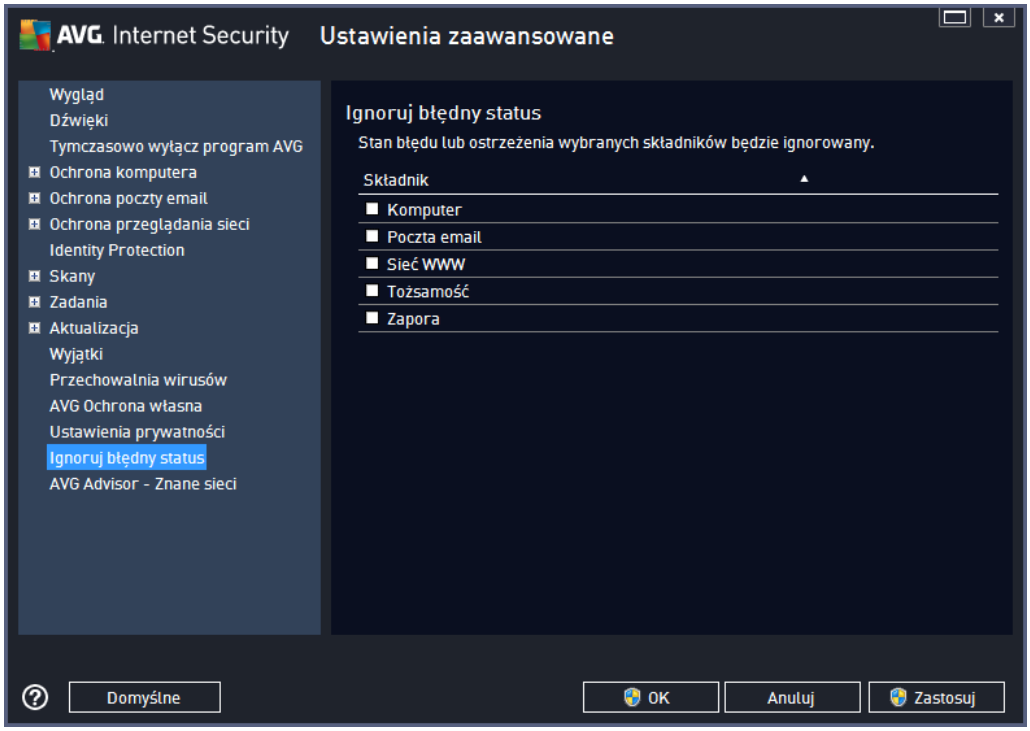
- ***Fałszywy alarm*** to masowo wysyłana wiadomość e-mail zawierająca informacje o wyimaginowanym niebezpieczeństwie czy zagrożeniu. Wiele z opisanych powyżej zagrożeń rozprzestrzenia się za pośrednictwem wiadomości e-mail zwanych fałszywkami.

- ***Istnieją także szkodliwe witryny sieci Web*** instalujące na komputerze złośliwe oprogramowanie, oraz podobnie działające zainfekowane strony WWW, które padły ofiarą hakerów wykorzystujących je do rozprzestrzeniania wirusów.

Aby zapewnić ochronę przed wszystkimi wymienionymi rodzajami zagrożeń, system AVG Internet Security 2014 zawiera szereg wyspecjalizowanych składników. Szczegółowe informacje o ich funkcjach zawiera rozdział Przegląd składników.

9.15. 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 błędu, natychmiast wygenerowane zostanie powiadomienie:

- ikona na pasku zadań – gdy wszystkie składniki systemu AVG działają prawidłowo, wyświetlana ikona jest czterokolorowa; w przypadku błędu wyświetlany jest żółty wykrzyknik;

- tekstowy opis problemu jest widoczny w sekcji Informacje o stanie bezpieczeństwa okna głównego AVG.

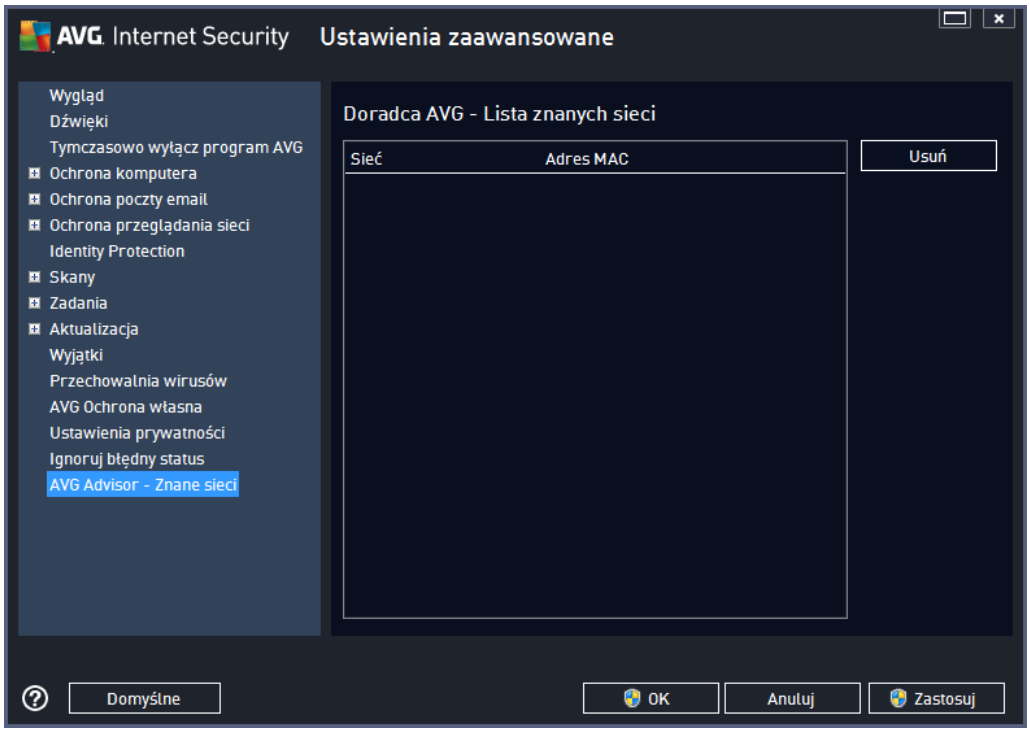
Istnieją jednak sytuacje, w których z pewnego powodu musisz tymczasowo wyłączyć wybrany składnik. ***Nie jest to zalecane – wszystkie składniki powinny być stale włączone i pracować z domyślną konfiguracją***, ale i tak jest to możliwe. W takim przypadku ikona na pasku zadań automatycznie informuje o stanie błędu składnika. W takiej sytuacji nie ma jednak faktycznego błędu, ponieważ wyłączenie składnika było celowe, a ryzyko z tym związane jest znane. Ponadto, gdy ikona jest szara, nie może już informować o ewentualnych realnych błędach.

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

9.16. 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) powiadomić Cię o tym i doradzić upewnienie się co do jej bezpieczeństwa.* Jeśli zdecydujesz, że połączenie z nową siecią jest bezpieczne, możesz zapisać ją na liście *(poprzez link widoczny w powiadomieniu Doradcy AVG, które pojawia się nad zasobnikiem systemowym po wykryciu nowej sieci. Szczegóły można znaleźć w rozdziale poświęconym Doradcy AVG)*. Doradca AVG zapamięta wówczas unikalne atrybuty danej sieci *(a dokładniej jej adres MAC)* i nie będzie ponownie wyświetlał tego powiadomienia. Każda sieć, z jaką nawiążesz połączenie, będzie automatycznie uznawana za znaną sieć i dodawana do listy. Możesz usunąć pojedynczą sieć klikając przycisk ***Usuń*** – zostanie ona znów uznana za potencjalnie niebezpieczną.

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



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

10. 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 udostępnia następujące parametry:

- Ogólne
- Aplikacje
- Udostępnianie plików i drukarek

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

- Ustawienia zaawansowane
- Zdefiniowane sieci
- Usługi systemowe
- Dzienniki

Dostawca oprogramowania skonfigurował jednak wszystkie składniki systemu AVG Internet Security 2014 pod kątem optymalnej wydajności. Nie należy modyfikować konfiguracji domyślnej, jeśli nie ma ku temu ważnych powodów. Wszelkie zmiany ustawień powinny być wprowadzane wyłącznie przez doświadczonych użytkowników!

10.1. 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 2014 pod kątem optymalnej wydajności. Nie należy modyfikować konfiguracji domyślnej, jeśli nie ma ku temu ważnych powodów. Wszelkie zmiany ustawień powinny być wprowadzane wyłącznie przez doświadczonych użytkowników!

Zapora umożliwia definiowanie określonych reguł bezpieczeństwa w oparciu o środowisko i tryb pracy komputera. Każda z opcji wymaga innego poziomu zabezpieczeń, 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 będziesz proszony o podejmowanie jakichkolwiek decyzji. Zapora zezwoli na połączenia wszystkich znanych aplikacji, tworząc jednocześnie reguły umożliwiające im nawiązywanie połączeń w przyszłości. Dla innych aplikacji, Zapora zdecyduje, czy pozwolić na komunikację, na podstawie analizy behawioralnej aplikacji. W takich przypadkach nie utworzy ona jednak reguły, więc aplikacja będzie sprawdzana przy każdorazowej próbie połączenia. ***Tryb automatyczny nie narzuca się i jest polecany większości użytkowników.***

- ***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. Zalecane tylko dla użytkowników zaawansowanych.

- ***Blokuj dostęp do internetu*** – Połączenie z internetem będzie całkowicie zablokowane, nie będzie można dostać się do internetu, a także nikt z zewnątrz nie będzie mógł się dostać do komputera. Tylko do stosowania wyjątkowego i tymczasowego.

- ***Wyłącz Zaporę*** – wyłączenie Zapory zezwoli na cały ruch przychodzący i wychodzący do i z komputera. W rezultacie stanie się on podatny na ataki hakerów. Prosimy o stosowanie tej opcji ze rozwagą.

Należy zwrócić uwagę na specyficzny, automatyczny tryb pracy Zapory. Tryb ten jest aktywowany w tle za każdym razem, gdy składnik Komputer lub Identity Protection zostanie wyłączony, co naraża Twój komputer na zwiększone niebezpieczeństwo. W takim przypadku Zapora zezwoli automatycznie jedynie na ruch sieciowy znanych i absolutnie bezpiecznych aplikacji. We

wszystkich pozostałych przypadkach będziesz pytany o decyzję. Służy to zrównoważeniu ryzyka spowodowanego wyłączonymi składnikami i jest sposobem na zachowanie bezpieczeństwa Twojego komputera.

10.2. Aplikacje

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

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

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

Przypominamy, że tylko już zainstalowane aplikacje mogły zostać wykryte. 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 możliwe będzie zapisanie odpowiedzi jako stałej reguły (która wówczas zostanie dodana do listy w tym oknie dialogowym).

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

Poza aplikacjami na liście wyświetlane są jeszcze dwie pozycje specjalne. ***Priorytetowe reguły aplikacji*** (*u góry listy*) są wybierane jako pierwsze i stosowane zawsze przed regułami określonej aplikacji. ***Inne reguły aplikacji*** (*na dole listy*) służą jako „rezerwa”, gdy nie są stosowane żadne

określone reguły, np. dla nieznanych lub niezdefiniowanych aplikacji. Wybierz akcję, która powinna być podjęta, gdy taka aplikacja podejmie próbę komunikacji sieciowej: Blokuj *(komunikacja będzie zawsze blokowana)*, Pozwól *(komunikacja będzie dozwolona we wszystkich sieciach)*, Pytaj *(zostaniesz każdorazowo zapytany o to, czy chcesz zezwolić na komunikację)*. ***Te pozycje mają inne opcje niż zwykłe ustawienia aplikacji i są przeznaczone tylko dla doświadczonych użytkowników. Stanowczo zalecamy niemodyfikowanie tych ustawień!***

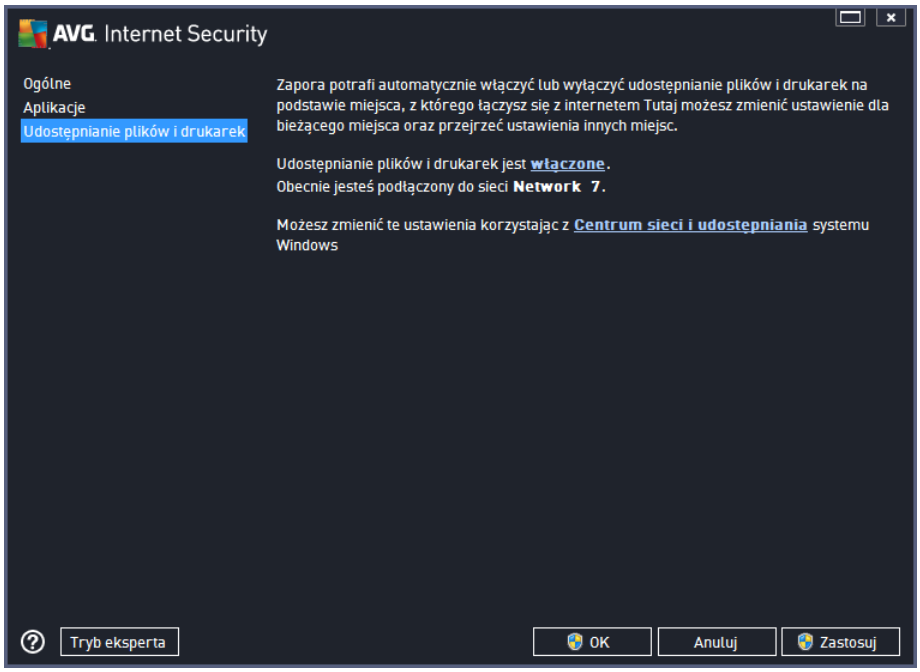
Przyciski kontrolne

Listę można edytować przy użyciu następujących przycisków kontrolnych:

- ***Dodaj*** – otwiera puste okno dialogowe pozwalające zdefiniować nowe reguły aplikacji.
- ***Edytuj*** – otwiera to samo okno dialogowe pozwalające edytować zestaw reguł aplikacji.
- ***Usuń*** – usuwa wybrany zbiór reguł z listy.

10.3. 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 obiektów jest pożądane jedynie w sieciach uważanych za bezpieczne *(np. w domu, w pracy lub w szkole)*. Jeśli jednak połączony jesteś z siecią publiczną *(jak np. Wi-Fi na lotnisku lub w kawiarence internetowej)*, najprawdopodobniej nie chcesz czegokolwiek udostępniać. Zapora AVG umożliwia łatwe zablokowanie lub odblokowanie udostępniania, a także zapisanie Twojej decyzji dla już odwiedzonych sieci.

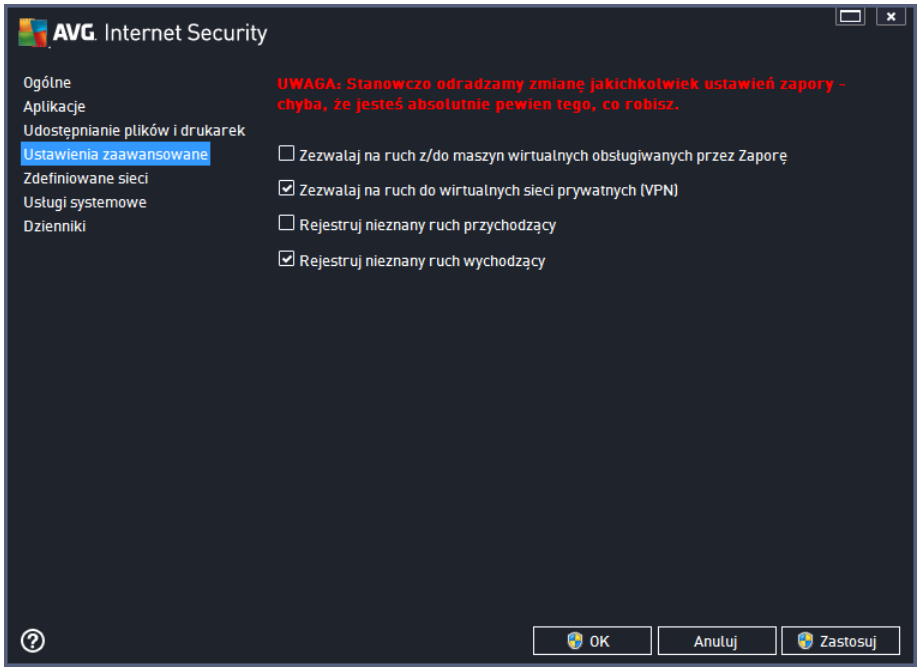


W oknie ***Udostępnianie plików i drukarek*** możesz edytować konfigurację udostępniania plików i

drukarek, a także obecnie podłączone sieci. W systemie Windows XP nazwa sieci odpowiada nazwie wybranej dla danej sieci podczas pierwszego połączenia z nią. W systemie Windows Vista i nowszych, nazwa sieci pobierana jest automatycznie z Centrum Sieci i Udostępniania.

10.4. Ustawienia zaawansowane

Jakiekolwiek zmiany w oknie Ustawień zaawansowanych powinny być wprowadzane JEDYNIE PRZEZ DOŚWIADCZONYCH UŻYTKOWNIKÓW!



Okno ***Ustawień 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 ze zdalnymi komputerami)*.
- ***Rejestruj nieznany ruch przychodzący/wychodzący*** – wszystkie próby komunikacji *(przychodzącej/wychodzącej)* nieznanych aplikacji 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 aplikację w bazie danych zaufanych aplikacji itp. Jeśli aplikacji nie będzie można uznać za bezpieczną, Zapora będzie traktować aplikację zgodnie z wybranym trybem:
    - jeśli Zapora działa w ***trybie automatycznym***, aplikacja domyślnie nie będzie blokowana;

- jeśli Zapora działa w ***trybie interaktywnym***, aplikacja będzie blokowana i zostanie wyświetlone okno dialogowe z prośbą, aby użytkownik zdecydował o sposobie obsługi aplikacji.

Odpowiednią procedurę obsługi dla każdej aplikacji można oczywiście zdefiniować w oknie dialogowym Aplikacje.

10.5. Zdefiniowane sieci

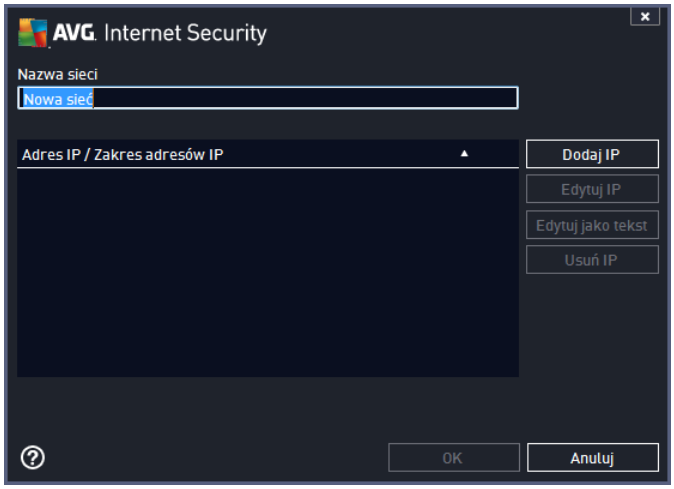
Jakiekolwiek modyfikacje w oknie Zdefiniowane sieci powinny być wprowadzane JEDYNIE PRZEZ DOŚWIADCZONYCH UŻYTKOWNIKÓW!

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 podłączony 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 ***Nazwę sieci*** i jej ***zakres adresów IP***:

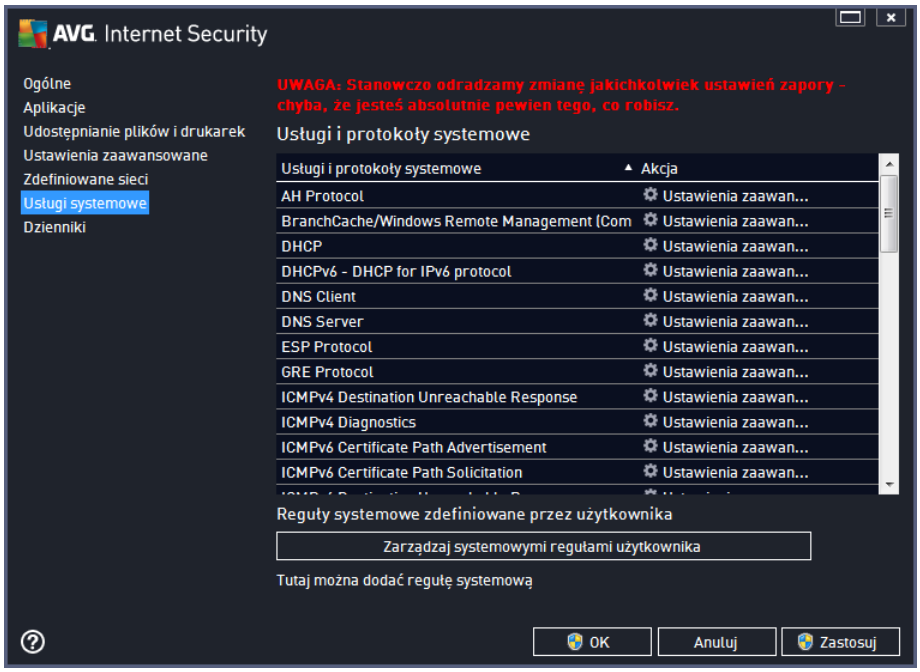


- ***Edytuj sieć*** – powoduje otwarcie okna dialogowego ***Właściwości sieci*** (*patrz wyżej*), w którym można edytować parametry zdefiniowanej sieci (*okno to jest identyczne jak podczas dodawania nowej sieci. Zobacz opis w poprzednim akapicie*).

- ***Usuń sieć*** – usuwa wybraną sieć z listy.

10.6. Usługi systemowe

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



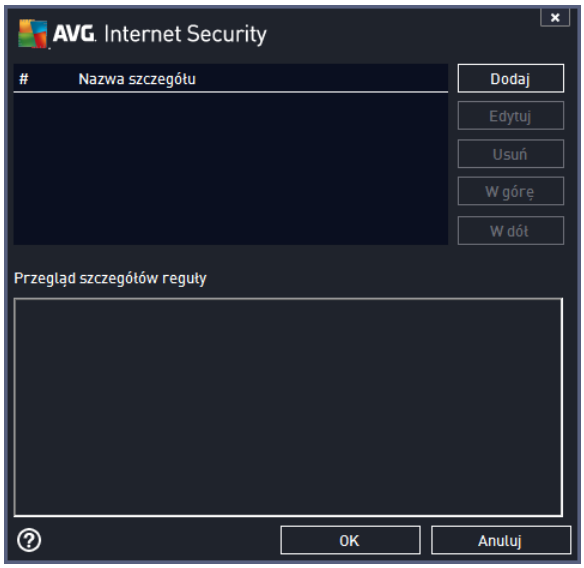
W oknie dialogowym ***Usługi i protokoły systemowe*** dostępna jest lista standardowych usług i protokołów systemu Windows, które mogą wymagać komunikacji poprzez sieć. Tabela zawiera następujące kolumny:

- ***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*), należy kliknąć tę pozycję prawym przyciskiem myszy i wybrać polecenie ***Edytuj***. ***Edycja reguł systemowych powinna być przeprowadzana jedynie przez zaawansowanych użytkowników.***

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 którejkolwiek z istniejących pozycji usług systemowych i protokołów. Górna sekcja tego okna dialogowego zawiera przegląd wszystkich szczegółów edytowanej w danej chwili reguły systemowej. W dolnej sekcji wyświetlany jest wybrany szczegół. Szczegóły reguły mogą być dodawane, edytowane i usuwane, dzięki odpowiednim przyciskom



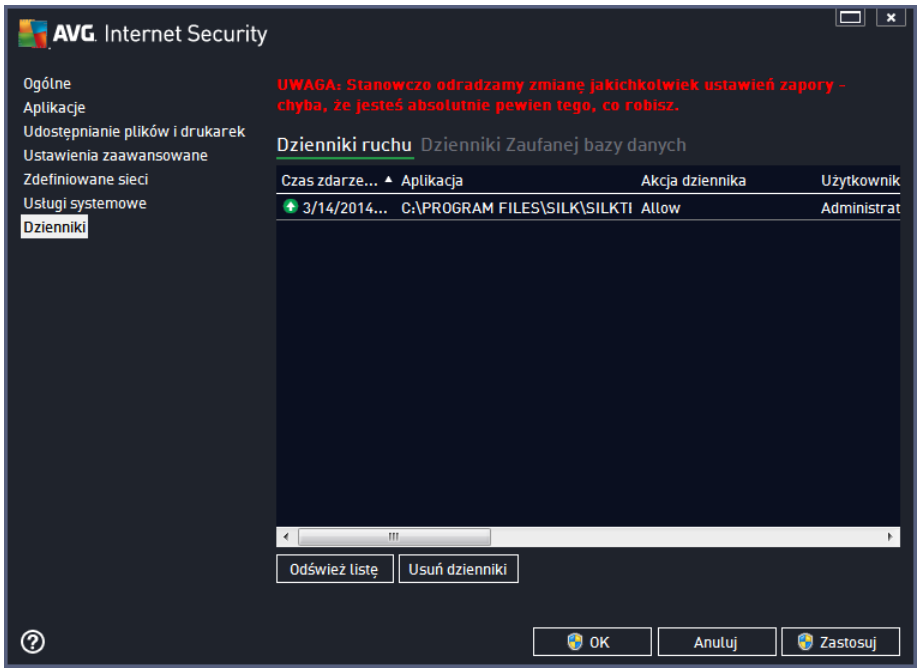
Należy pamiętać, że są to ustawienia zaawansowane, kierowane przede wszystkim do administratorów sieci, którzy wymagają pełnej kontroli nad konfiguracją Zapory. W przypadku braku wystarczającej wiedzy o typach protokołów, numerach portów sieciowych, adresach IP itp. nie należy modyfikować tych ustawień!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

10.7. Dzienniki

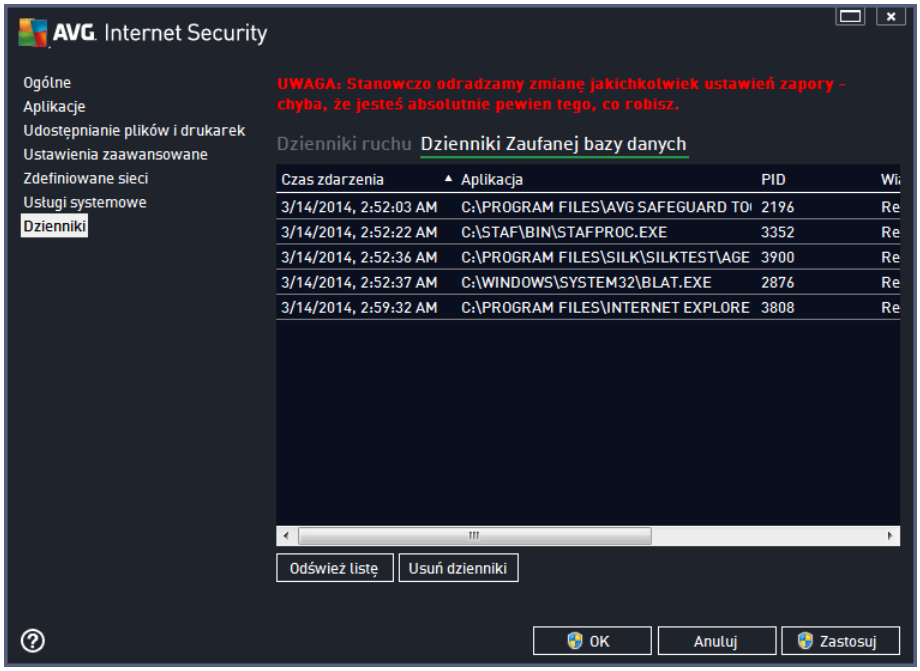
Jakiekolwiek modyfikacje w oknie Dzienniki powinny być wprowadzane JEDYNIE PRZEZ DOŚWIADCZONYCH UŻYTKOWNIKÓW!

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 zdarzenia, nazwie aplikacji, zarejestrowanej akcji, nazwie użytkownika, numerze PID, kierunku ruchu, typie protokołu, numerze portu zdalnego i lokalnego, a także 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 siecią (*np. gdy jeszcze nie została utworzona reguła Zapory dla tej aplikacji*), konieczna jest decyzja, czy zezwolić na komunikację sieciową. Najpierw system AVG przeszukuje bazę *Trusted Database*. Jeśli aplikacja znajduje się na liście, dostęp do sieci zostanie jej automatycznie umożliwiony. Dopiero gdy 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.



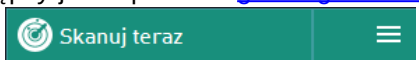
Przyciski kontrolne

- ***Odśwież listę*** – wszystkie zarejestrowane parametry można uporządkować według wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) – wystarczy kliknąć odpowiedni nagłówek kolumny. Użyj przycisku ***Odśwież listę***, aby zaktualizować wyświetlane informacje.

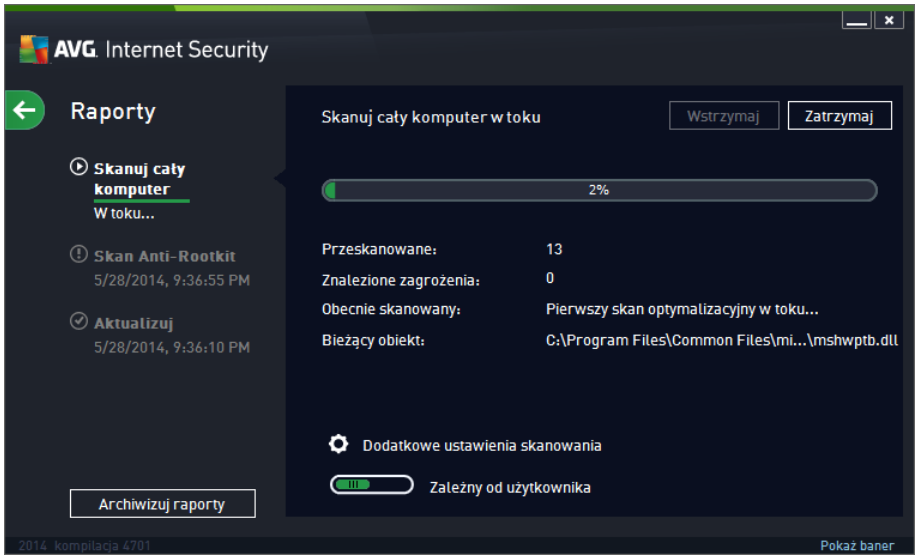
- ***Usuń dzienniki*** – pozwala usunąć wszystkie wpisy.

11. Skanowanie AVG

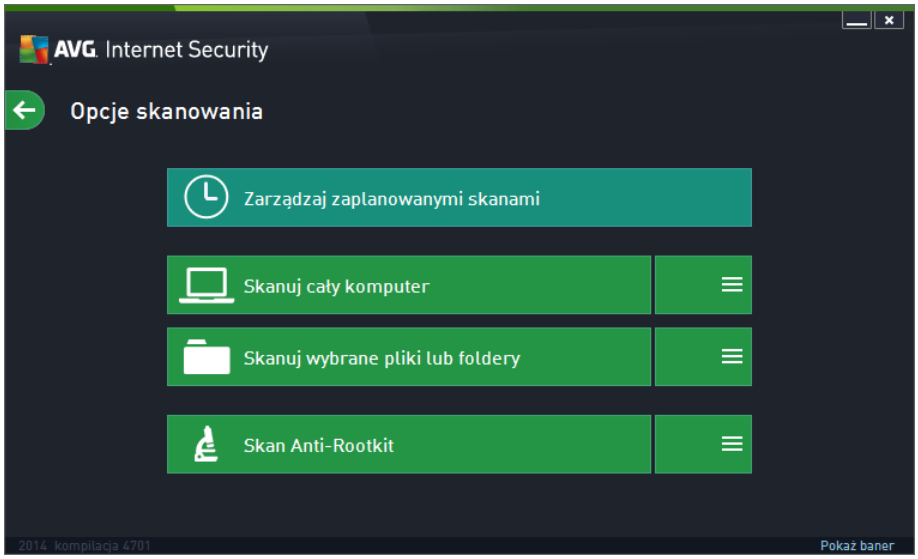
Domyślnie system **AVG Internet Security 2014** nie uruchamia żadnych testów, ponieważ po przeprowadzeniu wstępnego skanowania (*o które zostaniesz poproszony*) ochronę potrafią zapewnić rezydentne składniki **AVG Internet Security 2014**, które przez cały czas czuwają, by złośliwe oprogramowanie nie miało szans przedostania się na Twój komputer. Oczywiście wciąż możesz zaplanować skanowanie w regularnych odstępach czasu lub uruchamiać je ręcznie w zależności od potrzeb.

Interfejs skanera AVG dostępny jest z poziomu głównego interfejsu użytkownika poprzez przycisk podzielony na dwie sekcje: 

- ***Skanuj teraz*** – kliknij ten przycisk, by natychmiastowo uruchomić 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)* by otworzyć ***Opcje skanowania***, które umożliwiają zarządzanie zaplanowanymi skanami oraz edytowanie parametrów Skanowania całego komputera / Skanowania określonych plików lub folderów:



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

- ***Zarządzaj zaplanowanymi skanami*** – wybierz tę opcję, by otworzyć nowe okno 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 je prawym przyciskiem i wybierz z menu kontekstowego opcję *Włącz zadanie*. Po włączeniu skanu zaplanowanego, możesz edytować jego konfigurację poprzez kliknięcie przycisku *Edytuj harmonogram skanowania* Możesz także kliknąć *Dodaj harmonogram skanowania*, aby utworzyć nowy, własny harmonogram.

- ***Skanuj cały komputer / Ustawienia*** – Ten przycisk składa się z dwóch sekcji. Kliknij opcję *Skanuj cały komputer*, by natychmiastowo uruchomić skanowanie całego komputera *(szczegóły dotyczące skanowania całego komputera można znaleźć w odpowiednim rozdziale, zatytułowanym Predefiniowane skany / Skan całego komputera)*. Kliknięcie sekcji *Ustawienia* przeniesie Cię do okna konfiguracji skanowania całego komputera.

- ***Skanuj określone pliki lub foldery / Ustawienia*** – Ten przycisk również podzielony jest na dwie sekcje. Kliknij opcję *Skanuj określone pliki lub foldery*, by natychmiastowo uruchomić skanowanie wybranych obszarów komputera *(szczegóły dotyczące skanowania określonych plików lub folderów znajdują się w odpowiednim rozdziale, zatytułowanym Predefiniowane skany / Skan określonych plików lub folderów)*. Kliknięcie sekcji *Ustawienia* przeniesie Cię do okna konfiguracji skanowania określonych 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 Wstępnie zdefiniowane skany / Skanuj komputer w poszukiwaniu programów typu rootkit)*. Kliknięcie sekcji *Ustawienia* przeniesie Cię do okna konfiguracji skanowania rootkit .

11.1. Wstępnie zdefiniowane testy

Jedną z głównych funkcji systemu **AVG Internet Security 2014** 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.

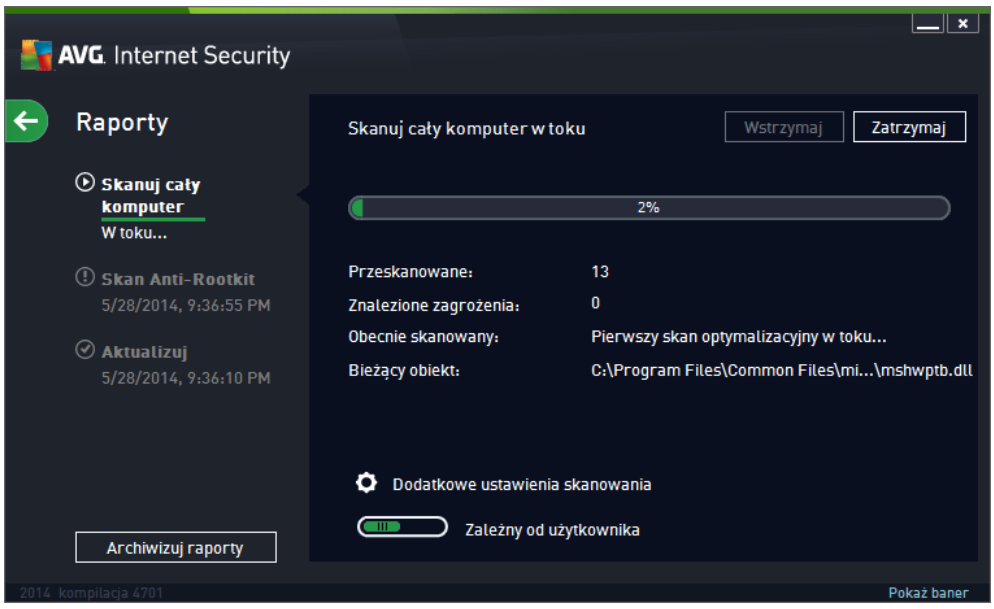
W systemie **AVG Internet Security 2014** dostępne są następujące typy skanowania zdefiniowane wstępnie przez producenta:

11.1.1. Skanuj cały komputer

Skan całego komputera – skanuje cały komputer w poszukiwaniu możliwych infekcji i/lub potencjalnie niechcianych programów. 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.

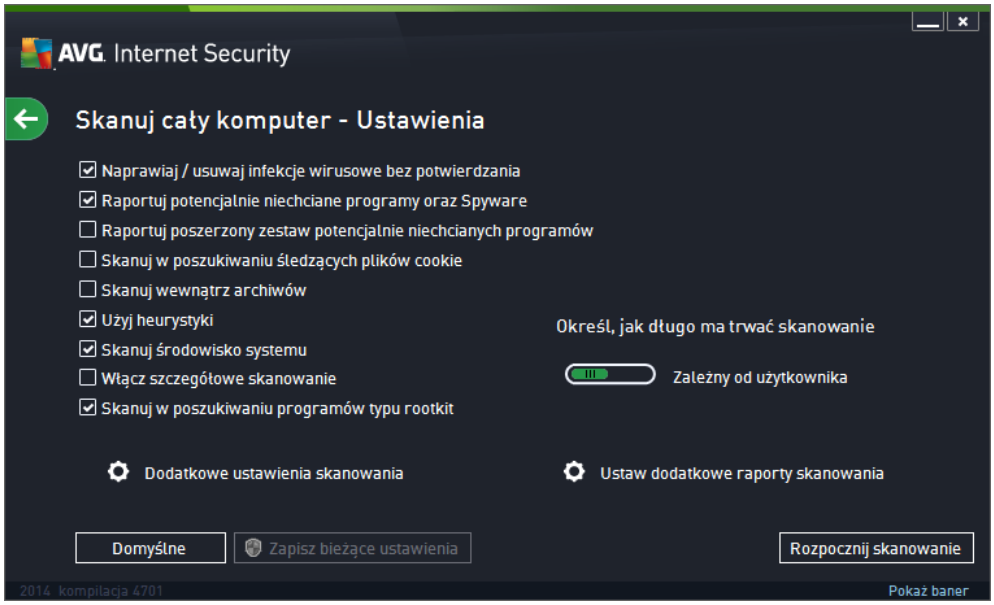
Uruchamianie skanowania

Skan całego komputera może zostać uruchomiony bezpośrednio z poziomu głównego interfejsu użytkownika poprzez 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 ***Skanu całego komputera*** w oknie ***Skan całego komputera – Ustawienia*** *(okno to jest dostępne poprzez link Ustawienia w oknie Opcje skanowania)*. ***Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest konieczne!***



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

- ***Naprawiaj / usuwaj infekcje wirusowe bez potwierdzania*** *(opcja domyślnie włączona)* – jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy i spyware*** *(opcja domyślnie włączona)* – zaznaczenie tego pola umożliwi 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 wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** *(opcja 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 Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też 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 zawartość koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** *(domyślnie wyłączone)* – parametr ten określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) – analiza heurystyczna (*dynamiczna emulacja*

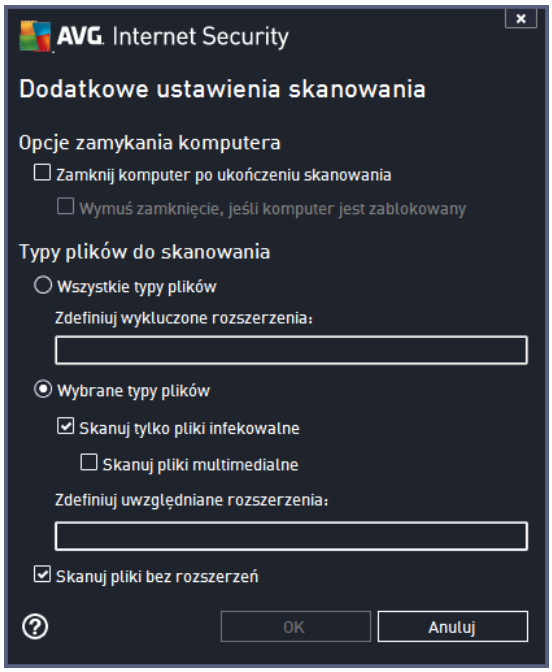
kodu skanowanego obiektu w środowisku wirtualnej maszyny) będzie jedną z metod wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** (*domyślnie włączone*) – skanowanie obejmie także obszary systemowe komputera.

- ***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 pewności będą 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*** *(opcja domyślnie włączona)* – uwzględnia skanowanie anti-rootkit podczas skanu całego komputera. Skan anti-rootkit może być również uruchomiony osobno.

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



  - ***Opcje wyłączania komputera*** – określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukończeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (***Wymuś zamknięcie, jeśli komputer jest zablokowany***).

  - ***Typy plików do skanowania*** – powinieneś także zdecydować, czy chcesz skanować:

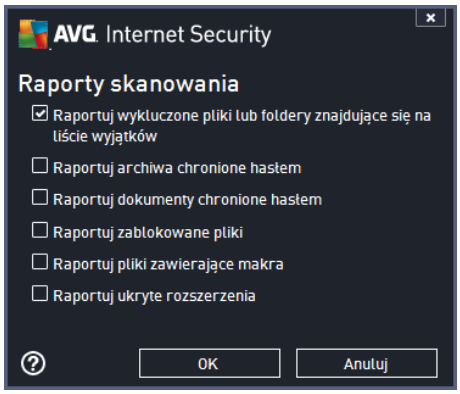
    - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być skanowane;

- ***Wybrane typy plików*** – skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio – jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje)*. Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

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

- ***Określ, jak długo ma trwać skanowanie*** – za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość to priorytet *Zależny 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 trwania skanowania nie ma znaczenia*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer nie jest tymczasowo używany*).

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



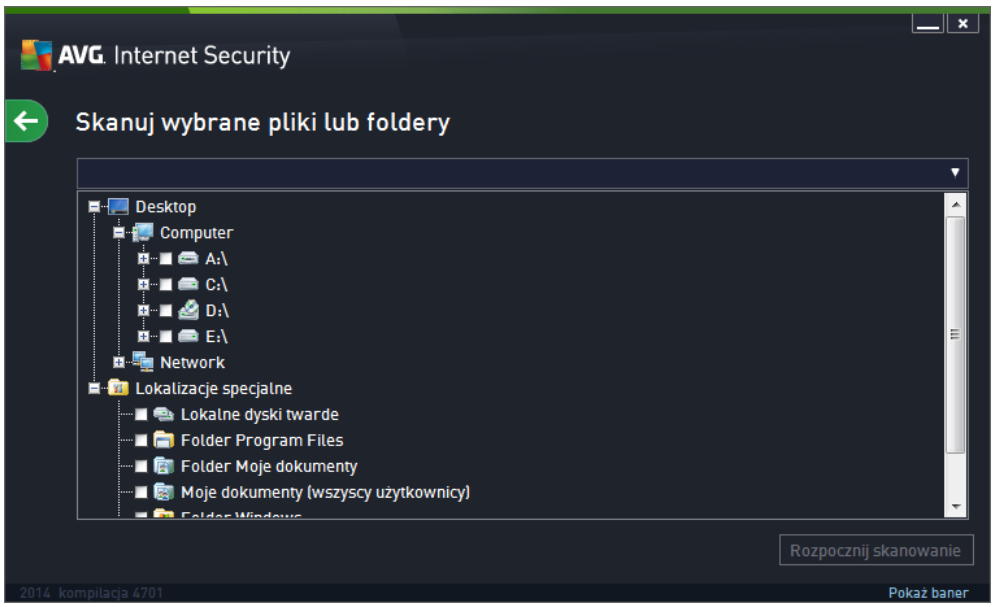
Ostrzeżenie: *Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów – zgodnie z opisem w rozdziale Skanowanie AVG / Planowanie skanowania / Jak skanować. Jeśli jednak domyślna konfiguracja testu* ***Skan całego komputera*** *zostanie zmieniona, nowe ustawienia można zapisać jako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

11.1.2. Skan wybranych plików/folderów

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

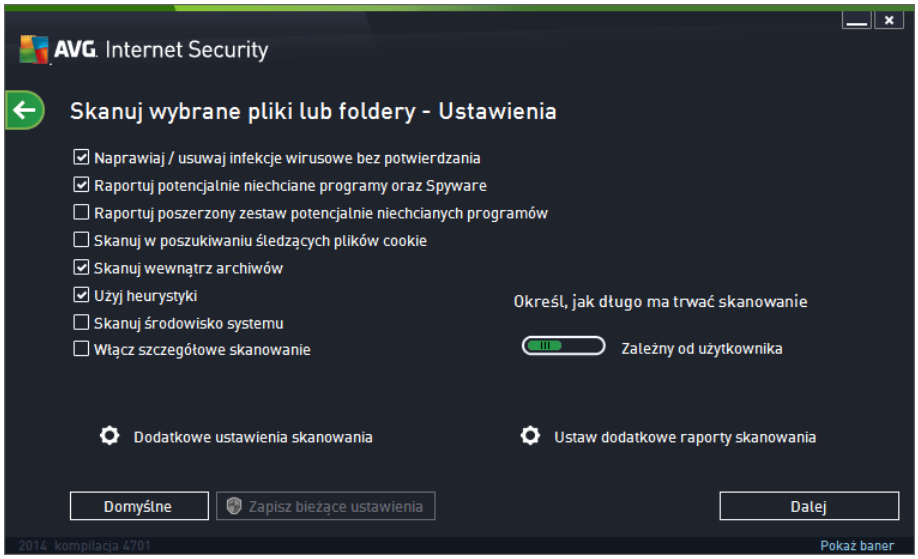
Uruchamianie skanowania

Skan określonych plików lub folderów może być rozpoczęty bezpośrednio z okna Opcje skanowania poprzez kliknięcie przycisku **Skanuj określone pliki lub foldery**. Wyświetlone zostanie nowe okno dialogowe ***Wybierz pliki lub foldery do przeskanowania***. W drzewie dysków komputera należy wybrać foldery, które mają zostać przeskanowane. Ścieżki do wszystkich wybranych folderów zostaną wygenerowane automatycznie i wyświetlone w polu tekstowym w górnej części okna dialogowego. Można także przeskanować wybrany folder, wykluczając jednocześnie ze skanowania wszystkie jego podfoldery: należy wprowadzić znak minus „**-**” przed jego nazwą w wygenerowanej ścieżce (*patrz ilustracja*). Aby wykluczyć cały folder ze skanowania, należy użyć parametru „**!**”. Na koniec, aby uruchomić skanowanie, należy kliknąć przycisk ***Rozpocznij skanowanie***; proces skanowania jest w zasadzie taki sam jak w przypadku Skanu całego komputera.



Edycja konfiguracji skanowania

Możesz edytować ***Skan określonych plików lub folderów*** w oknie ***Skan określonych plików lub folderów – Ustawienia*** *(okno to jest dostępne poprzez link Ustawienia widoczny w oknie Opcje skanowania)*. ***Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest konieczne!***



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

- ***Naprawiaj / usuwaj infekcje wirusowe bez potwierdzania*** *(opcja domyślnie włączona)* – jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy i spyware*** *(opcja domyślnie włączona)* – zaznaczenie tego pola powoduje włączenie silnika i przeprowadzenie skanowania w poszukiwaniu oprogramowania szpiegującego (a także wirusów). Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj udoskonalony zestaw potencjalnie niechcianych programów*** *(opcja 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 Twojego komputera. Funkcja ta może jednak blokować prawidłowo działające programy, dlatego też 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 zawartość koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** *(domyślnie włączone)* – parametr ten określa, czy skanowanie ma obejmować również wszystkie pliki znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

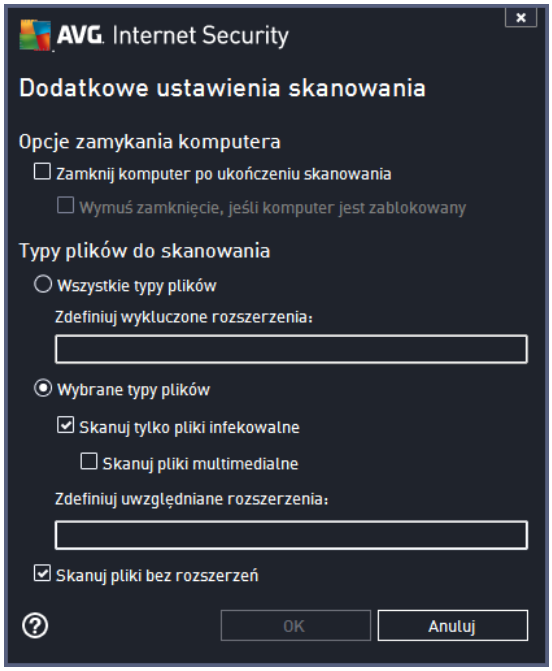
- ***Użyj heurystyki*** *(opcja domyślnie włączona)* – analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod

wykrywania wirusów w czasie skanowania.

- ***Skanuj środowisko systemu*** *(domyślnie wyłączone)* – skanowanie obejmie także obszary systemowe komputera.

- ***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 pewności będą one skanować nawet te obszary komputera, których ryzyko zainfekowania jest znikome. Należy pamiętać, że ta metoda skanowania jest czasochłonna.

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



  - ***Opcje wyłączania komputera*** – określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej opcji (***Zamknij komputer po ukończeniu skanowania***) powoduje aktywowanie nowej funkcji, która pozwala zamknąć komputer nawet, gdy jest zablokowany (***Wymuś zamknięcie, jeśli komputer jest zablokowany***).

  - ***Typy plików do skanowania*** – należy zdecydować, które z poniższych elementów mają być skanowane:

    - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, który nie powinny być skanowane;

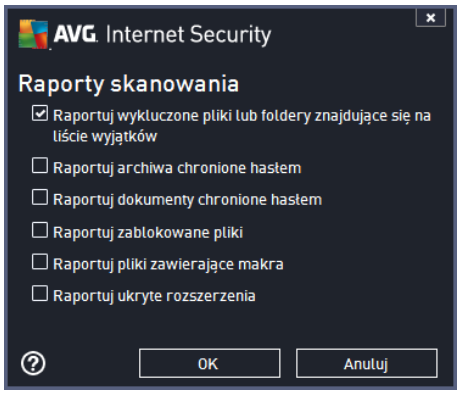
    - ***Wybrane typy plików*** – skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio – jeśli to pole pozostanie niezaznaczone, czas skanowania skróci*

się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje). Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

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

- ***Określ, jak długo ma trwać skanowanie*** – za pomocą suwaka można zmienić priorytet procesu skanowania. Domyślna wartość to priorytet *Zależny 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*), bądź skanowanie szybkie, które oznacza wyższe wykorzystanie zasobów systemowych (*np. gdy komputer jest tymczasowo nieużywany*).

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



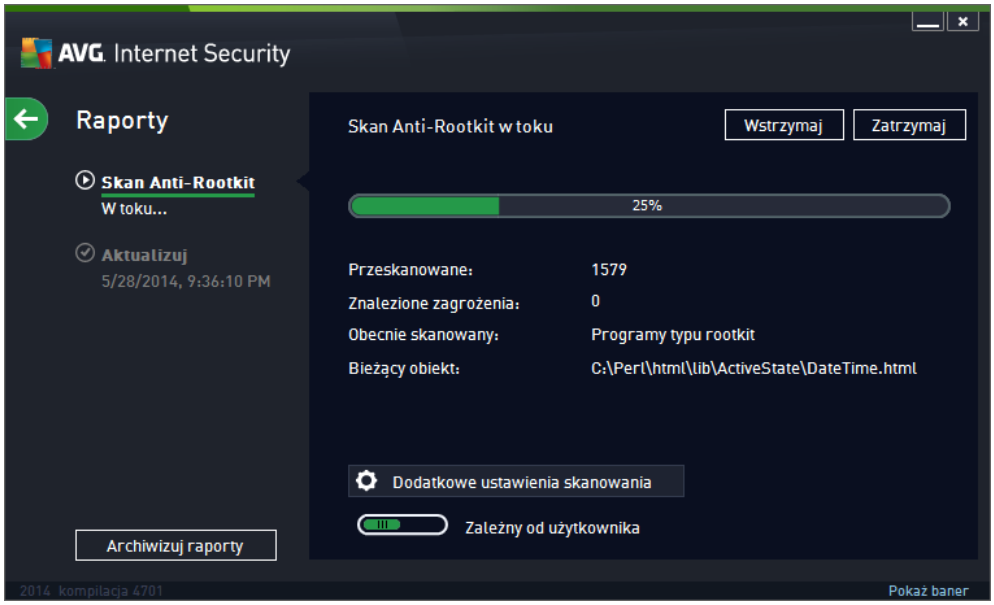
Ostrzeżenie: *Ustawienia te są identyczne jak domyślne parametry nowo utworzonych testów – zgodnie z opisem w rozdziale Skanowanie AVG / Planowanie skanowania / Jak skanować. Jeśli jednak domyślna konfiguracja testu* ***Skan wybranych plików/folderów*** *zostanie zmieniona, nowe ustawienia będzie można zapisać jako konfigurację domyślną, 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 użytkownika oparte są na bieżącej konfiguracji skanu określonych plików lub folderów).*

11.1.3. Skanuj komputer w poszukiwaniu programów typu rootkit

Skanuj komputer w poszukiwaniu programów typu rootkit to specjalistyczne narzędzie do wykrywania i skutecznego usuwania niebezpiecznych programów typu rootkit, tj. 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 programów typu rootkit na podstawie wstępnie zdefiniowanego zestawu reguł. Jeżeli 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.

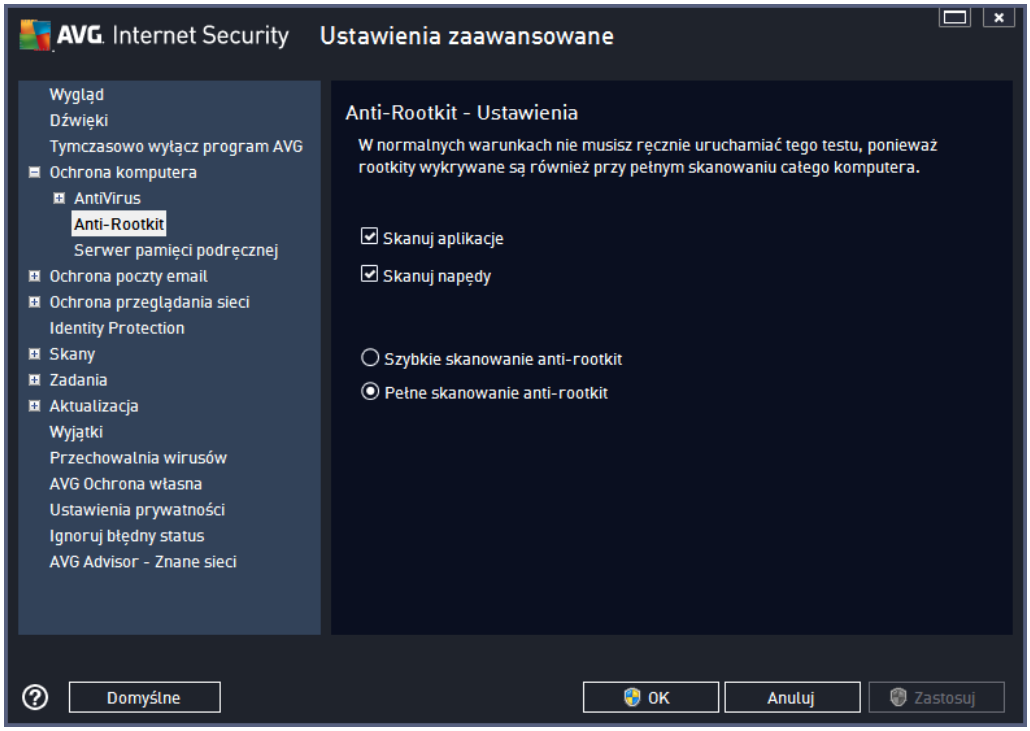
Uruchamianie skanowania

Funkcja ***Skanuj komputer w poszukiwaniu programów typu rootkit*** może być uruchomiona bezpośrednio z okna Opcje skanowania po kliknięciu przycisku ***Skanuj komputer w poszukiwaniu programów typu rootkit***. 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 ***Ustawienia Anti-Rootkit*** *(okno to jest dostępne poprzez link Ustawienia w sekcji Skanowanie komputera w poszukiwaniu programów typu rootkit w oknie Opcje skanowania).* ***Zaleca się nie zmieniać ustawień domyślnych, jeśli nie jest to konieczne!***

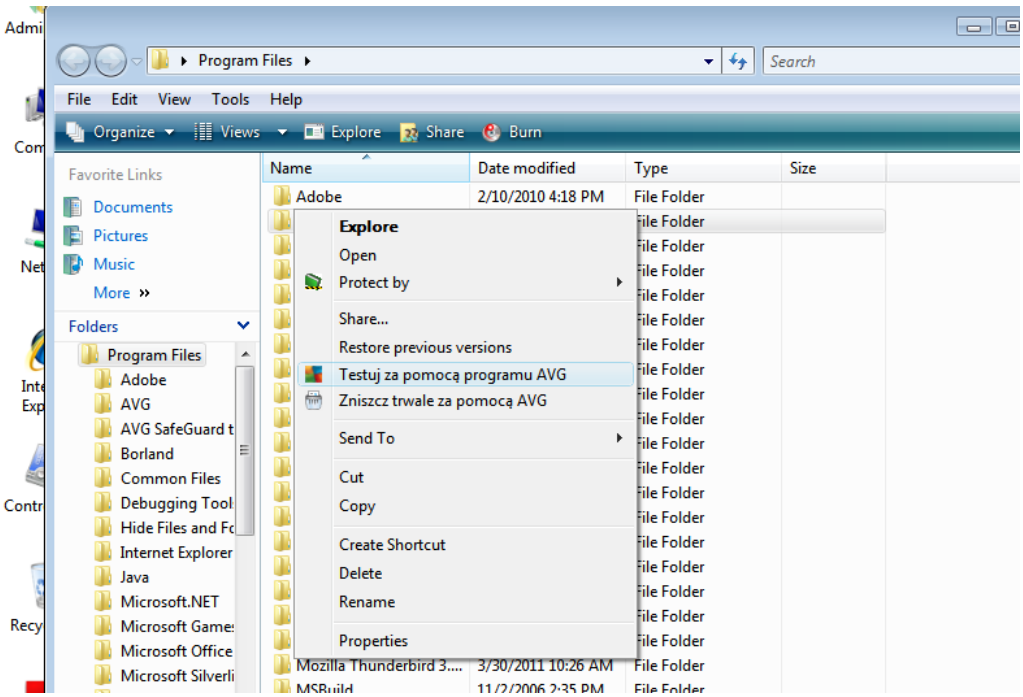


Opcje Skanuj aplikacje i ***Skanuj napędy*** pozwalają szczegółowo określić, co ma obejmować skanowanie Anti-Rootkit. Ustawienia te są przeznaczone dla użytkowników zaawansowanych. Zaleca się pozostawienie wszystkich opcji włączonych. Można również wybrać tryb skanowania w poszukiwaniu programów typu rootkit:

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

11.2. Skan z poziomu eksploratora systemu Windows

Oprócz wstępnie zdefiniowanych skanów obejmujących cały komputer lub wybrane obszary, system **AVG Internet Security 2014** 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 żądanie”. 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 2014**

11.3. Skan z poziomu wiersza poleceń

System **AVG Internet Security 2014** posiada opcję uruchamiania skanowania z poziomu wiersza poleceń. 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 większości 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

Składnia polecenia

Składnia polecenia jest następująca:

- ***avgscanx /parametr*** ... np. ***avgscanx /comp*** w celu przeskanowania całego komputera
- ***avgscanx /parametr /parametr*** .. jeśli używanych jest wiele parametrów, należy wpisać je

w jednym wierszu, rozdzielając spacjami i ukośnikami

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

Parametry skanowania

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

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

Skanowanie z poziomu wiersza poleceń uruchamiane za pomocą interfejsu graficznego

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

Ponieważ okno to jest dostępne tylko w trybie awaryjnym Windows, jego szczegółowy opis zawiera plik pomocy dostępny bezpośrednio z okna.

11.3.1. Parametry skanowania z wiersza poleceń

Oto lista parametrów dostępnych dla skanowania z wiersza poleceń:

- /SCAN — Skanuj określone pliki lub foldery /SCAN=ścieżka;ścieżka *(np. /SCAN=C:\;D:\)*
- /COMP — Skan całego komputera
- /HEUR — Użyj analizy heurystycznej
- /EXCLUDE — Wyklucz ze skanowania ścieżkę lub pliki
- /@ — Plik polecenia /nazwa pliku/
- /EXT — Skanuj te rozszerzenia /na przykład EXT=EXE,DLL/
- /NOEXT — Nie skanuj tych rozszerzeń /na przykład NOEXT=JPG/
- /ARC — Skanuj archiwa
- /CLEAN — Lecz automatycznie
- /TRASH — Przenieś zainfekowane pliki do Kwarantanny

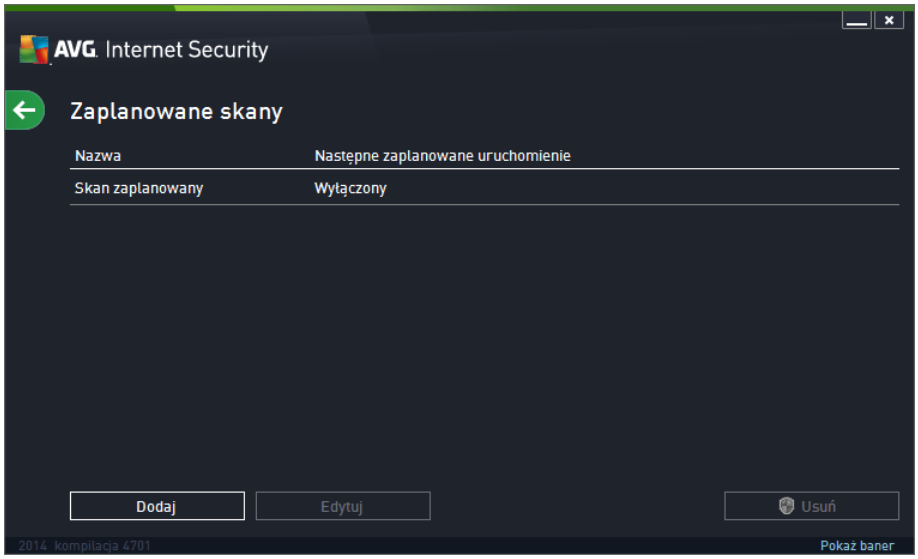
- /QT Szybki test
- /LOG Generuj plik z wynikami skanowania
- /MACROW Raportuj pliki zawierające makra
- /PWDW Raportuj pliki chronione hasłem
- /ARCBOMBSW Raportuj archiwa wielokrotne *(wielokrotnie skompresowane)*
- /IGNLOCKED Ignoruj pliki zablokowane
- /REPORT Raportuj do pliku /nazwa pliku/
- /REPAPPEND Dopisz do pliku raportu
- /REPOK Raportuj niezainfekowane pliki jako OK
- /NOBREAK Nie zezwalaj na przerwanie klawiszami CTRL-BREAK
- /BOOT Włącz sprawdzanie MBR/sektora rozruchowego
- /PROC Skanuj aktywne procesy
- /PUP Raportuj Potencjalnie niechciane programy
- /PUPEXT Raportuj udoskonalony zestaw Potenjalnie niechcianych programów
- /REG Skanuj Rejestr
- /COO Skanuj pliki cookie
- /? Wyświetl pomoc na ten temat
- /HELP Wyświetl pomoc na ten temat
- /PRIORITY *Ustaw priorytet skanowania /Niski, Automatyczny, Wysoki/ (zobacz Ustawienia zaawansowane / Skany)*
- /SHUTDOWN Zamknij komputer po ukończeniu skanowania
- /FORCESHUTDOWN Wymuś zamknięcie komputera po ukończeniu skanowania
- /ADS Skanuj alternatywne strumienie danych *(tylko NTFS)*
- /HIDDEN Raportuj pliki z ukrytymi rozszerzeniami
- /INFECTABLEONLY Skanuj tylko pliki z rozszerzeniami umożliwiającymi infekcje
- /THOROUGHSCAN Włącz szczegółowe skanowanie
- /CLOUDCHECK Sprawdzaj pod kątem błędnych wykryć

- /ARCBOMBSW Raportuj wielokrotnie spakowane archiwa

11.4. Planowanie skanowania

System **AVG Internet Security 2014** 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 wyłączany, pominięty z tego powodu skan zaplanowany jest uruchamiany po ponownym włączeniu komputera.

Harmonogram skanowania może zostać utworzony / edytowany w oknie ***Skany zaplanowane***, dostępnym poprzez przycisk ***Zarządzaj zaplanowanymi skanami*** znajdujący się w oknie Opcje skanowania. W nowym oknie ***Skan zaplanowany*** widoczny będzie przegląd wszystkich zaplanowanych skanów:

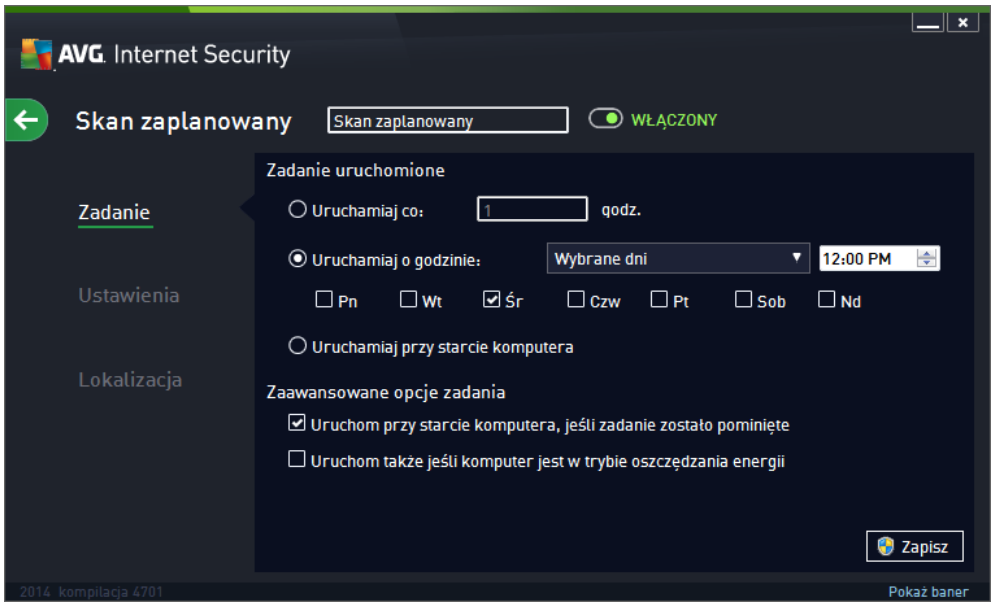


W oknie tym możesz określić własne skanowania. Możesz także użyć przycisku ***Dodaj harmonogram skanowania***, aby utworzyć nowy, własny harmonogram. Parametry zaplanowanego skanu można edytować (*podobnie jak przy tworzeniu nowego harmonogramu*) na trzech kartach:

- Harmonogram
- Ustawienia
- Lokalizacja

Na każdej karcie można łatwo przełączyć przycisk "sygnalizacji świetlnej"  , aby tymczasowo wyłączyć zaplanowany test i włączyć go ponownie, gdy zajdzie taka potrzeba.

11.4.1. Zadanie



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. Przykład: Nazwy takie jak „Nowy skan" lub „Mój skan" nie są odpowiednie, ponieważ nie informują o tym, co jest przedmiotem skanowania. Przykładem dobrej opisowej nazwy jest „Skan obszarów systemowych".

W tym samym oknie można szczegółowo określić następujące parametry skanowania:

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

- ***Zaawansowane opcje zadania*** – ta sekcja umożliwia zdefiniowanie warunków uruchamiania lub nieuruchamiania skanowania w czasie, gdy komputera pracuje w trybie oszczędzania energii lub jest wyłączony. Po rozpoczęciu zaplanowanego skanu nad ikoną AVG na pasku zadań wyświetlone zostanie powiadomienie. Następnie pojawi się nowa ikona AVG na pasku zadań (kolorowa, z białą strzałką – jak powyżej), 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.

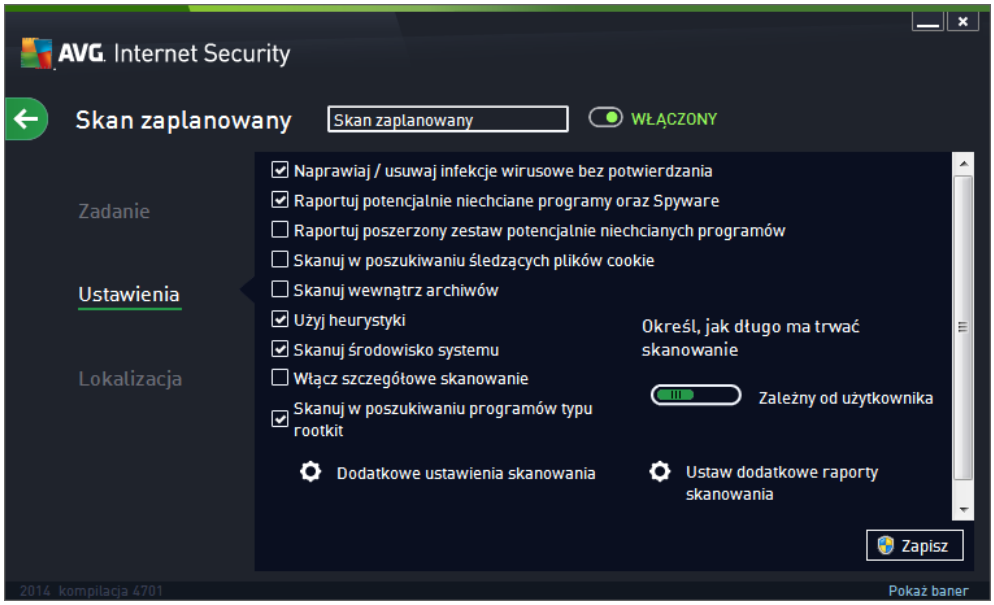
Elementy sterujące dostępne w oknie

- ***Zapisz*** – Powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do przeglądu zaplanowanych skanów. Oznacza to, że aby zapisać nowe parametry testów wprowadzone na wszystkich kartach, należy kliknąć ten przycisk.

- – Użyj zielonej strzałki w lewym górnym rogu okna, by powrócić do przeglądu

zaplanowanych skanów.

11.4.2. Ustawienia



W górnej części ***Ustawień*** widoczne jest pole tekstowe, w którym możesz podać nazwę aktualnie definiowanego skanowania. Należy używać krótkich, opisowych nazw, aby ułatwić rozpoznawanie ich przez innych użytkowników w przyszłości. Przykład: Nazwy takie jak „Nowy skan” lub „Mój skan” nie są odpowiednie, ponieważ nie informują o tym, co jest przedmiotem skanowania. Przykładem dobrej opisowej nazwy jest „Skan obszarów systemowych”.

Karta ***Ustawienia*** zawiera listę parametrów silnika skanującego. ***Ustawienia te należy zmieniać tylko w uzasadnionych przypadkach, w pozostałych zachowując wstępnie zdefiniowaną konfigurację***:

- ***Naprawiaj / usuwaj infekcje wirusowe bez potwierdzania*** *(opcja domyślnie włączona)* – jeżeli podczas skanowania wykryty zostanie wirus, system AVG podejmie próbę automatycznego wyleczenia go. Jeśli zainfekowany plik nie może zostać wyleczony automatycznie, obiekt zostanie przeniesiony do Przechowalni wirusów.

- ***Raportuj potencjalnie niechciane programy oraz Spyware*** *(opcja domyślnie włączona)* – zaznacz to pole, aby włączyć skanowanie w poszukiwaniu oprogramowania szpiegującego, a także wirusów. Oprogramowanie szpiegujące należy do nietypowej kategorii szkodliwych programów. Zazwyczaj stanowi zagrożenie dla bezpieczeństwa, ale niektóre z takich programów mogą zostać zainstalowane umyślnie. Nie zaleca się wyłączania tej opcji – znacząco zwiększa ona poziom ochrony komputera.

- ***Raportuj poszerzony zestaw potencjalnie niechcianych programów*** (*opcja domyślnie wyłączona*) – zaznaczenie tej opcji pozwala wykrywać większą ilość oprogramowania szpiegującego: 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 też 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. ustawień witryn i zawartości koszyków w sklepach internetowych*).

- ***Skanuj wewnątrz archiwów*** (*opcja domyślnie wyłączona*) – ten parametr określa, czy skanowanie ma obejmować wszystkie pliki, nawet te znajdujące się wewnątrz archiwów, np. ZIP, RAR itd.

- ***Użyj heurystyki*** (*opcja domyślnie włączona*) – analiza heurystyczna (*dynamiczna emulacja kodu skanowanego obiektu w środowisku wirtualnej maszyny*) będzie jedną z metod wykrywania wirusów w czasie skanowania.

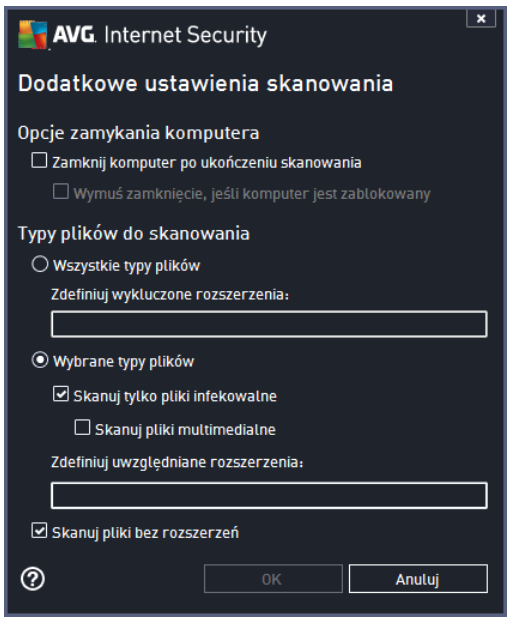
- ***Skanuj środowisko systemu*** (*opcja domyślnie włączona*) – skanowanie obejmie także obszary systemowe komputera.

- ***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 pewności będą 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 włączone) – 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.

Dodatkowe ustawienia skanowania

Link ten otwiera okno dialogowe ***Dodatkowe ustawienia skanowania***, w którym można określić następujące parametry:



- ***Opcje wyłączania komputera*** – określają, czy komputer ma zostać automatycznie wyłączony po zakończeniu skanowania. Wybranie tej 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*** – należy zdecydować, które z poniższych elementów mają być skanowane:

    - ***Wszystkie typy plików*** z opcją zdefiniowania wyjątków skanera poprzez wprowadzenie rozdzielonych przecinkami rozszerzeń, które nie powinny być skanowane.

    - ***Wybrane typy plików*** – skanowane będę tylko pliki infekowalne (*pliki, które nie mogą zostać zainfekowane, nie będą skanowane, np. niektóre pliki tekstowe lub pewne pliki niewykonywalne*), z uwzględnieniem plików multimedialnych (*plików wideo i audio – jeśli to pole pozostanie niezaznaczone, czas skanowania skróci się jeszcze bardziej, ponieważ takie pliku często są duże, a nie są podatne na infekcje)* . Za pomocą rozszerzeń można określić, które pliki mają być zawsze skanowane.

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

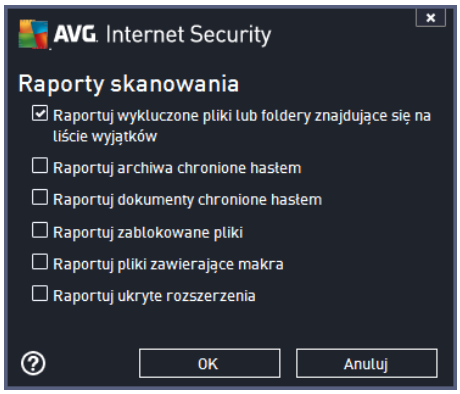
Określ, jak długo ma trwać skanowanie

W tej sekcji można szczegółowo określić żądaną prędkość skanowania, w zależności od wykorzystania zasobów systemowych. Domyślna wartość to priorytet *Zależny 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 (*opcji można śmiało używać wtedy, gdy komputer jest włączony, ale nikt na nim nie pracuje*). Można także obniżyć wykorzystanie zasobów, co przedłuży jednocześnie czas skanowania.

Ustaw dodatkowe raporty skanowania

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

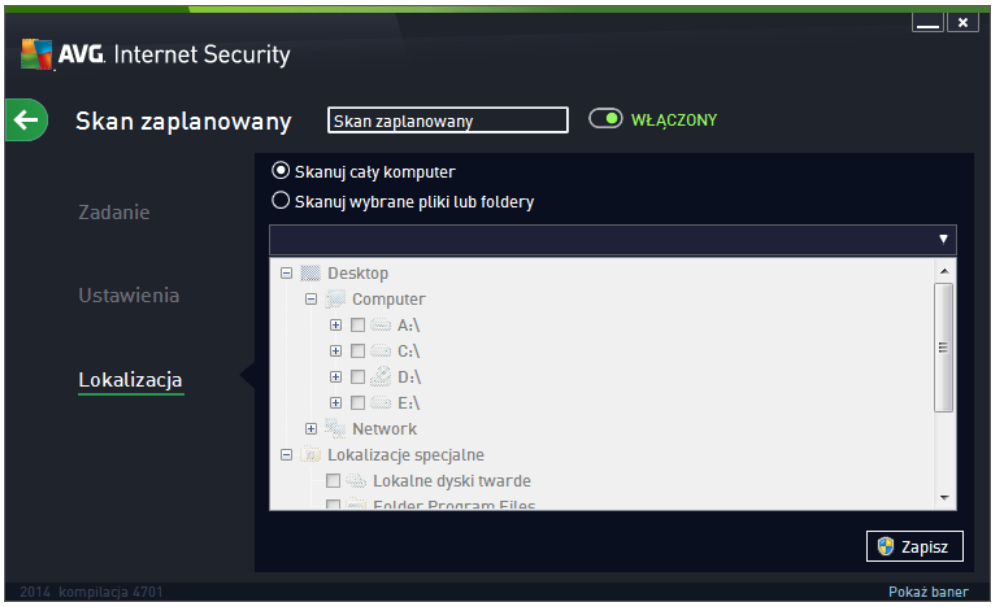


Przyciski dostępne w oknie

- ***Zapisz*** – Powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do przeglądu zaplanowanych skanów. Oznacza to, że aby zapisać nowe parametry testów wprowadzone na wszystkich kartach, należy kliknąć ten przycisk.

- – Użyj zielonej strzałki w lewym górnym rogu okna, by powrócić do przeglądu zaplanowanych skanów.

11.4.3. Lokalizacja



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

Drzewo katalogów zawiera również gałąź ***Lokalizacje specjalne***. Poniżej znajduje się lista tych lokalizacji; będą one skanowane, jeśli 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***
  - *dla systemu Win XP:* C:\Documents and Settings\Default User\Moje dokumenty\
  - *dla systemu Windows Vista/7*: C:\Users\user\Documents\
- ***Moje dokumenty (wszyscy użytkownicy)***
  - *dla systemu Win XP*: C:\Documents and Settings\All Users\Documents\

- *dla systemu Windows Vista/7*: C:\Users\Public\Documents\

- ***Folder 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*)

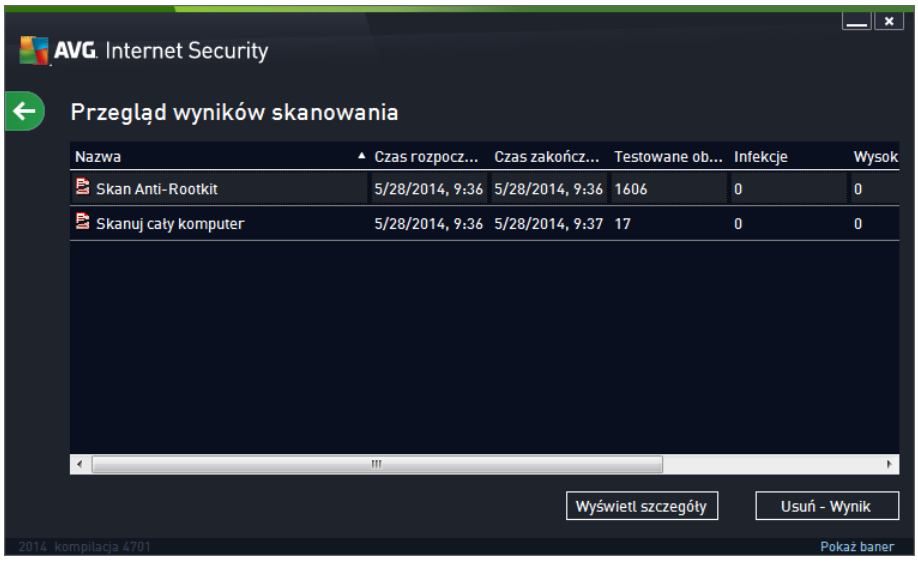
  - *Folder tymczasowych plików internetowych* – C:\Documents and Settings\User\Ustawienia lokalne\Temporary Internet Files\ (*Windows XP*) lub C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Elementy sterujące dostępne w oknie

- ***Zapisz*** – Powoduje zapisanie wszystkich zmian wprowadzonych na dowolnej karcie okna dialogowego i powrót do przeglądu zaplanowanych skanów. Oznacza to, że aby zapisać nowe parametry testów wprowadzone na wszystkich kartach, należy kliknąć ten przycisk.

- – Użyj zielonej strzałki w lewym górnym rogu okna, by powrócić do przeglądu zaplanowanych skanów.

11.5. Wyniki skanowania



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

- ***Ikona*** – Pierwsza kolumna wyświetla ikonę informacyjną podającą status testu:
  - o  Nie znaleziono infekcji, skanowanie zakończone
  - o  Nie znaleziono infekcji, skanowanie przerwane przed ukończeniem
  - o  Znaleziono infekcje, lecz nie wyleczono ich – skanowanie zakończone
  - o  Znaleziono infekcje, lecz nie wyleczono ich – skanowanie przerwane przed ukończeniem
  - o  Znaleziono infekcje – wszystkie zostały wyleczone lub usunięte, skanowanie zakończone
  - o  Znaleziono infekcje – wszystkie zostały wyleczone lub usunięte, skanowanie przerwane przed ukończeniem
- ***Nazwa*** – Ta kolumna podaje nazwę skanu. Będzie 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 / Średni / 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, by zobaczyć szczegóły wybranego skanu *(podświetlonego w tabeli znajdującej się wyżej)*.

Usuń wyniki – Kliknij ten przycisk, by usunąć wyniki wybranego skanowania z tabeli.

 – Użyj zielonej strzałki w prawym górnym rogu okna, aby powrócić do głównego interfejsu użytkownika z przeglądem składników.

11.6. Szczegóły wyników skanowania

Aby otworzyć przegląd szczegółowych informacji o wybranym wyniku skanowania, kliknij przycisk ***Wyświetl szczegóły*** widoczny w oknie Przegląd wyników skanowania. Zostaniesz przekierowany do tego samego interfejsu, opisującego szczegóły wybranego wyniku skanowania. Informacje rozmieszczone są w trzech kartach:

- ***Podsumowanie*** – Udostępnia podstawowe informacje o skanowaniu: czy zostało pomyślnie ukończone, czy znalezione zostały zagrożenia, oraz jakie kroki względem nich podjęto.

- ***Szczegóły*** – Ta strona wyświetla wszystkie informacje o skanowaniu, włączając w to szczegóły na temat każdego znalezionego zagrożenia. Eksportuj przegląd do pliku... umożliwia zapisanie go do pliku .csv.

- ***Detekcje*** – Ta strona wyświetlana jest tylko wtedy, gdy podczas skanowania wykryte zostały zagrożenia. Podaje ona szczegóły na temat zagrożeń:

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

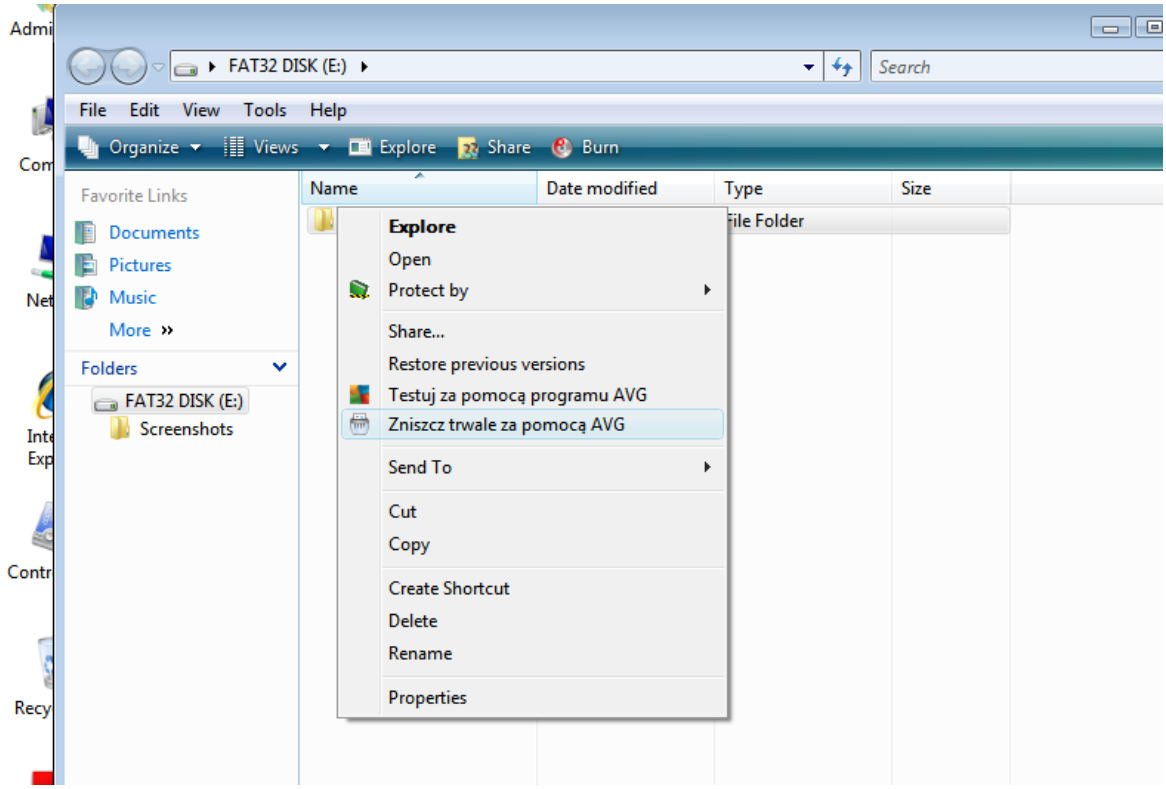
   ***Średni poziom zagrożenia***: zazwyczaj PNP *(potencjalnie niechciane programy, takie jak programy reklamowe*) lub śledzące pliki cookie

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

12. AVG File Shredder

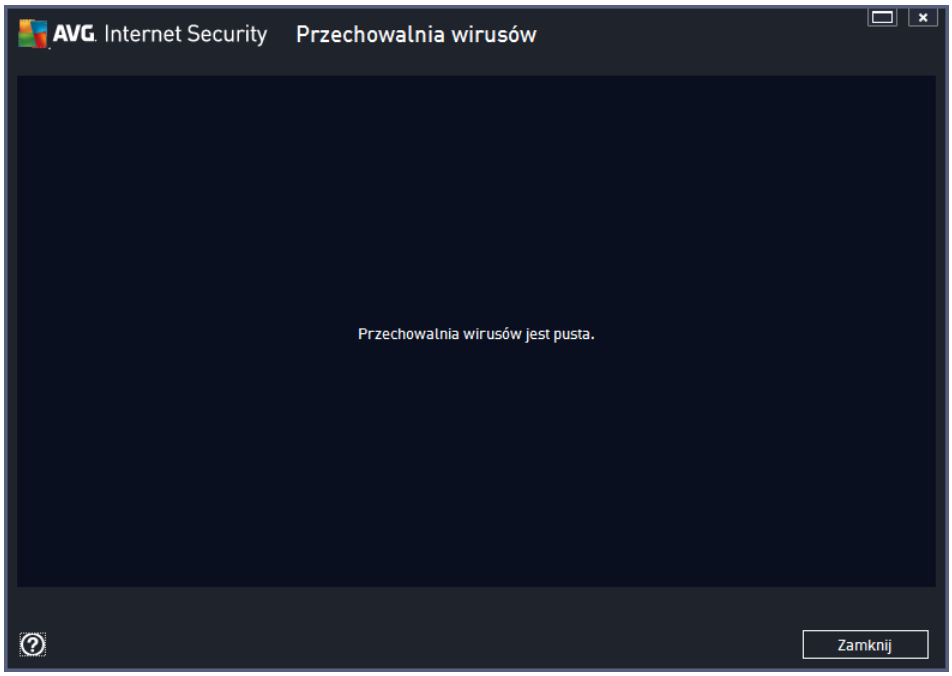
AVG File Shredder służy do usuwania plików w całkowicie bezpieczny sposób, tzn. bez możliwości ich odzyskania, nawet przy pomocy zaawansowanego, specjalnie przeznaczonego do tych celów oprogramowania.

Aby zniszczyć plik lub folder, kliknij prawym przyciskiem myszy w menedżer plików *(Windows Explorer, Total Commander, ...)* i wybierz z menu kontekstowego opcję ***Zniszcz trwale za pomocą AVG***. Pliki z kosza mogą być również zniszczone. Jeżeli znajdujący się w danej lokalizacji plik *(np. na dysku CD)* nie może zostać skutecznie zniszczony, zostaniesz o tym powiadomiony, bądź też opcja z menu kontekstowego w ogóle nie będzie dostępna.



Zapamiętaj dobrze: Zniszczenie pliku jest nieodwracalne.

13. 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 (w przypadku, gdy program AVG nie jest w stanie automatycznie go wyleczyć), użytkownik zostanie poproszony o dokonanie wyboru reakcji na to zagrożenie. Zalecanym rozwiązaniem jest przeniesienie obiektu do ***Przechowalni wirusów***, skąd można będzie podjąć dalsze działanie związane z analizą, wyleczeniem lub usunięciem pliku. Głównym zadaniem ***Przechowalni*** jest przechowywanie wszelkich usuniętych plików przez określony czas, aby możliwe było upewnienie się, że nie były one potrzebne. Jeśli brak pliku powoduje problemy, można go wysłać 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.
- ***Poziom zagrożenia*** – Jeśli zdecydowałeś się zainstalować składnik Tożsamość wraz ze swoim , w tej samej sekcji wyświetlona będzie graficzna reprezentacja poziomu zagrożenia, wg czterostopniowej skali, od niegroźnego **AVG Internet Security 2014** *(trzy zielone kropki)* do bardzo niebezpiecznego *(trzy czerwone kropki)*, a także informacja o typie infekcji (*na podstawie poziomu infekcji – wszystkie zagrożenia mogą być zainfekowane lub potencjalnie zainfekowane*).
- ***Nazwa zagrożenia*** – Nazwa wykrytej infekcji pochodząca z internetowej Encyklopedii wirusów.
- ***Źródło*** – Określa, który składnik **AVG Internet Security 2014** wykrył dane zagrożenie.

- ***Wiadomość*** – W bardzo rzadkich sytuacjach, w tej kolumnie pojawią się szczegółowe komentarze dotyczące wykrytego zagrożenia.

Przyciski kontrolne

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

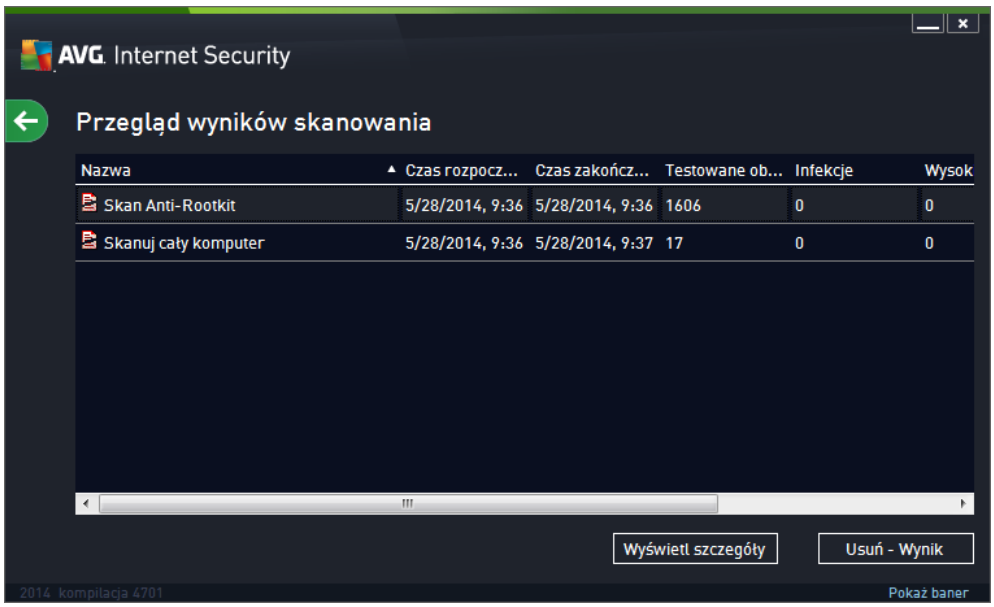
- ***Przywróć*** – przenosi zainfekowany plik do jego oryginalnej lokalizacji.
- ***Przywróć jako*** – przenosi zainfekowany plik do wybranego folderu.
- ***Szczegóły*** – aby uzyskać szczegółowe informacje o konkretnym zagrożeniu znajdującym się w ***Przechowalni wirusów*** podświetl wybraną pozycję na liście i kliknij przycisk ***Szczegóły***, który otworzy nowe okno z opisem wykrytego zagrożenia.
- ***Usuń*** – nieodwracalnie usuwa zainfekowany plik z ***Przechowalni***.
- ***Opróżnij kwarantannę*** – usuwa bezpowrotnie całą zawartość ***kwarantanny***. Usunięcie plików z ***Przechowalni wirusów*** oznacza całkowite i nieodwracalne usunięcie ich z dysku (*nie są one przenoszone do kosza*).

14. Historia

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

- Wyniki skanowania
- Zagrożenia wykryte przez Ochronę rezydentną
- Zagrożenia wykryte przez Ochronę poczty email
- Zagrożenia wykryte przez Ochronę Sieci
- Dziennik historii zdarzeń
- Dziennik zapory

14.1. Wyniki skanowania



To okno dostępne jest poprzez menu Opcje ***/ Historia / Wyniki skanowania w górnej części nawigacyjnej*** głównego okna **AVG Internet Security 2014**. Okno to zawiera listę wcześniejszych skanów oraz informacje o ich wynikach:

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

  – zielona oznacza, że nie wykryto żadnych infekcji;

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

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

Każda z ikon może być widoczna w całości lub „przerwana" – jeśli ikona jest cała, skanowanie zostało prawidłowo 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 testu.
- ***Czas zakończenia*** – data i godzina zakończenia skanowania.
- ***Przetestowano obiektów*** – liczba obiektów sprawdzonych podczas skanowania.
- ***Infekcje*** – liczba infekcji wirusowych, które zostały wykryte/usunięte.
- ***Wysoki / Średni*** – te kolumny podają liczbę usuniętych/wszystkich infekcji o wysokim i średnim poziomie zagrożenia.
- ***Informacja*** – informacje dotyczące przebiegu i wyniku skanowania *(zwykle o jego zakończeniu lub przerwaniu).*
- ***Programy typu rootkit*** – liczba wykrytych programów typu rootkit.

Przyciski kontrolne

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

- ***Wyświetl szczegóły*** – kliknięcie tego przycisku powoduje przełączenie się do okna dialogowego Wyniki skanowania, w którym można przejrzeć szczegółowe dane dotyczące wybranego skanowania.
- ***Usuń wynik*** – kliknięcie tego przycisku powoduje usunięcie wybranej pozycji z przeglądu wyników skanowania.
-  – by powrócić do domyślnego okna głównego AVG *(przeglądu składników),* użyj strzałki znajdującej się w lewym górnym rogu tego okna

14.2. Wyniki narzędzia Ochrona rezydentna

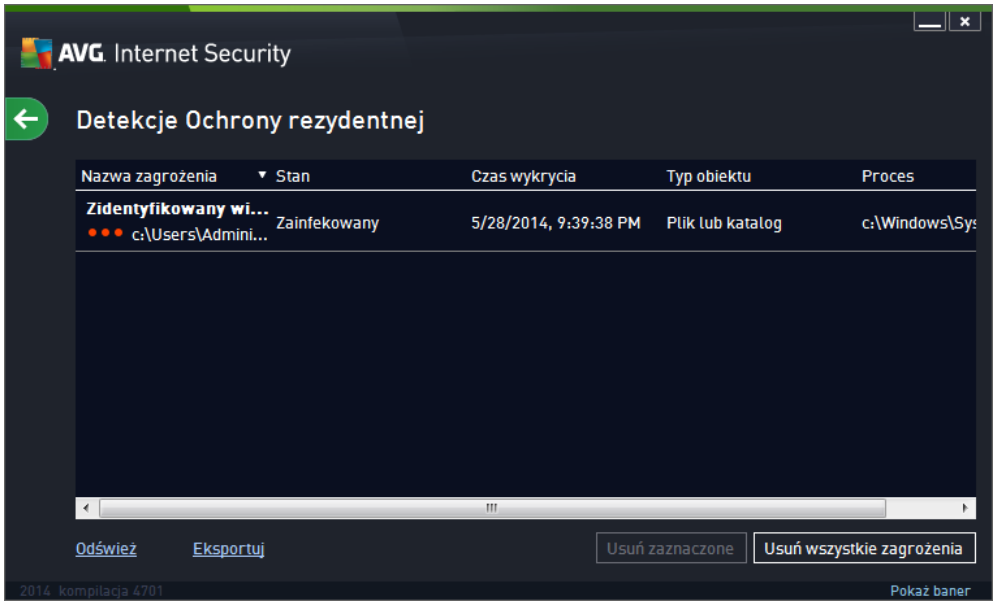
Ochrona rezydentna jest częścią składnika ***Komputer***, odpowiedzialną za skanowanie plików podczas ich kopiowania, otwierania lub zapisywania. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego ostrzeżenia:

To okno ostrzegawcze podaje informacje o wykrytym obiekcie, który został uznany za infekcję (*Zagrożenie*), a także kilka opisowych faktów o samej infekcji (*Opis*). Link Pokaż szczegóły przeniesie Cię do encyklopedii wirusów online, która może udzielić szczegółowych informacji o wykrytej infekcji, o ile są one znane. To samo okno zawiera także przegląd dostępnych rozwiązań w kwestii unieszkodliwienia zagrożenia. Jedna z alternatyw będzie oznaczona jako zalecana: ***Ochroń mnie (zalecane). O ile to możliwe, powinieneś 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 wyświetlony komunikat informujący o problemie. Istnieje jednak możliwość zmiany rozmiaru Przechowalni wirusów. Można to zrobić, określając dostępny procent rzeczywistego rozmiaru dysku twardego. Aby zwiększyć rozmiar Przechowalni wirusów, należy przejść do okna dialogowego Przechowalnia wirusów w sekcji Zaawansowane ustawienia AVG (rozmiaru Przechowalni wirusów).*

W dolnej części tego okna znajduje się link ***Pokaż szczegóły***. Kliknij go, by 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 poprzez menu ***Opcje / Historia / Zagrożenia wykryte przez Ochronę rezydentną*** w górnej części nawigacyjnej głównego okna **AVG Internet Security 2014**. Okno Zagrożenia wykryte przez Ochronę Rezydentną zawiera przegląd obiektów wykrytych i ocenionych przez ten składnik jako niebezpieczne, które następnie wyleczono lub przeniesiono do Przechowalni wirusów.



Podawane są tam następujące informacje:

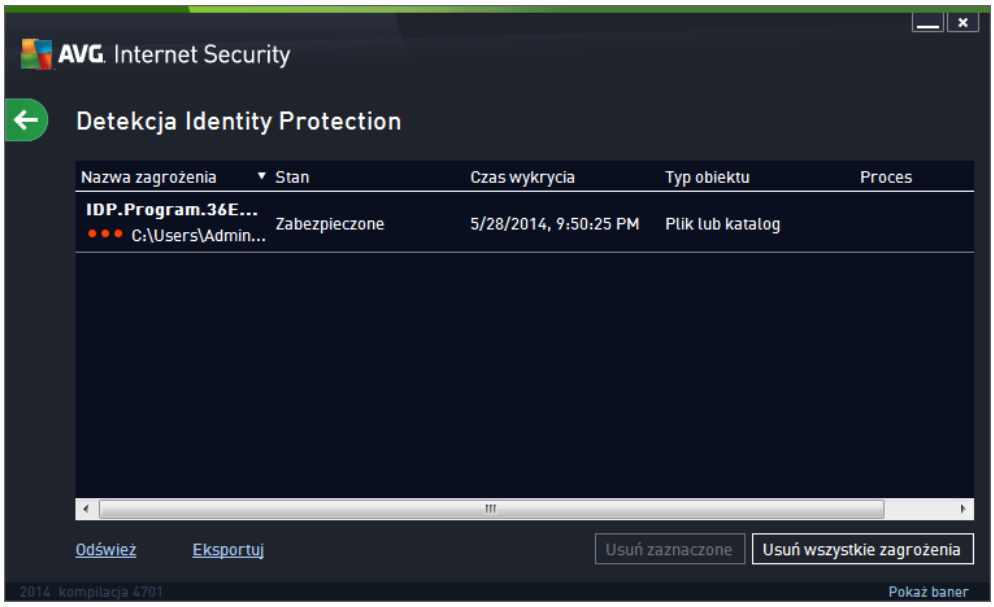
- ***Nazwa zagrożenia*** – opis (*także możliwa nazwa*) wykrytego obiektu oraz jego lokalizacja.
- ***Wynik*** – działanie podjęte w związku z wykryciem.
- ***Czas wykrycia*** – data i godzina wykrycia i zablokowania zagrożenia.
- ***Typ obiektu*** – typ wykrytego obiektu.
- ***Proces*** – akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co umożliwiło jego wykrycie).

Przyciski kontrolne

- ***Odśwież*** – pozwala zaktualizować listę obiektów wykrytych przez składnik ***Ochrona Sieci.***
- ***Eksportuj*** – eksportuje listę wykrytych obiektów do pliku.
- ***Usuń zaznaczone*** – możesz użyć tego przycisku po zaznaczeniu konkretnych pozycj na liście, aby je usunąć.
- ***Usuń wszystkie zagrożenia*** – użyj tego przycisku, by usunąć wszystkie zagrożenia widoczne w tym oknie.
- – by powrócić do domyślnego okna głównego AVG *(przeglądu składników),* użyj strzałki znajdującej się w lewym górnym rogu tego okna.

14.3. Wyniki Identity Protection

Okno ***Wyniki narzędzia Identity Protection*** dostępne jest z menu ***Opcje / Historia / Wyniki narzędzia Identity Protection*** znajdującego się w górnej części nawigacyjnej głównego okna **AVG Internet Security 2014**.



To okno zawiera listę wszystkich obiektów wykrytych przez składnik Identity Protection. Dla każdego wykrytego obiektu podawane są następujące informacje:

- ***Nazwa zagrożenia*** – opis (*a także możliwa 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 liczy 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

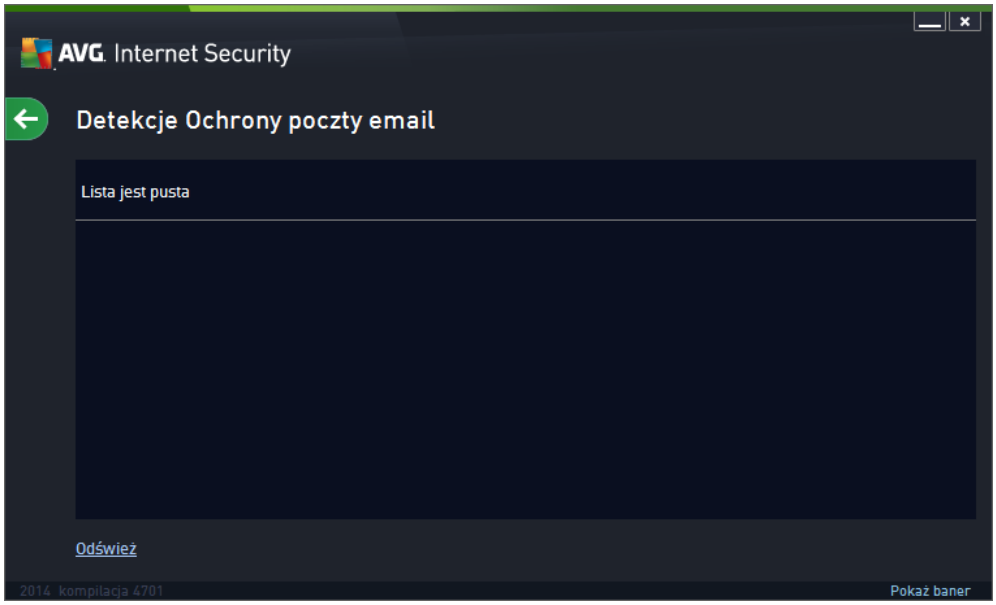
W interfejsie składnika ***Wyniki Identity Protection*** dostępne są następujące przyciski sterujące:

- ***Odśwież listę*** – aktualizuje listę wykrytych zagrożeń.
- – by powrócić do domyślnego okna głównego AVG *(przeglądu składników)*, użyj

strzałki znajdującej się w lewym górnym rogu tego okna.

14.4. Wyniki narzędzia Ochrona poczty email

Okno ***Wyniki narzędzia Ochrona poczty email*** dostępne jest z menu ***Opcje / Historia / Wyniki narzędzia Ochrona poczty email*** znajdującego się w górnej części nawigacyjnej głównego okna **AVG Internet Security 2014** .



To okno zawiera listę wszystkich obiektów wykrytych przez Skaner poczty email. Podawane są tam następujące informacje:

- ***Nazwa detekcji*** – opis (*a także możliwa nazwa*) wykrytego obiektu oraz jego źródło.
- ***Wynik*** – działanie podjęte w związku z wykryciem.
- ***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 liczy 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 e-mail*** dostępne są następujące przyciski sterujące:

- ***Odśwież listę*** – aktualizuje listę wykrytych zagrożeń.

- – by powrócić do domyślnego okna głównego AVG *(przeglądu składników),* użyj strzałki znajdującej się w lewym górnym rogu tego okna.

14.5. Wyniki narzędzia Ochrona sieci

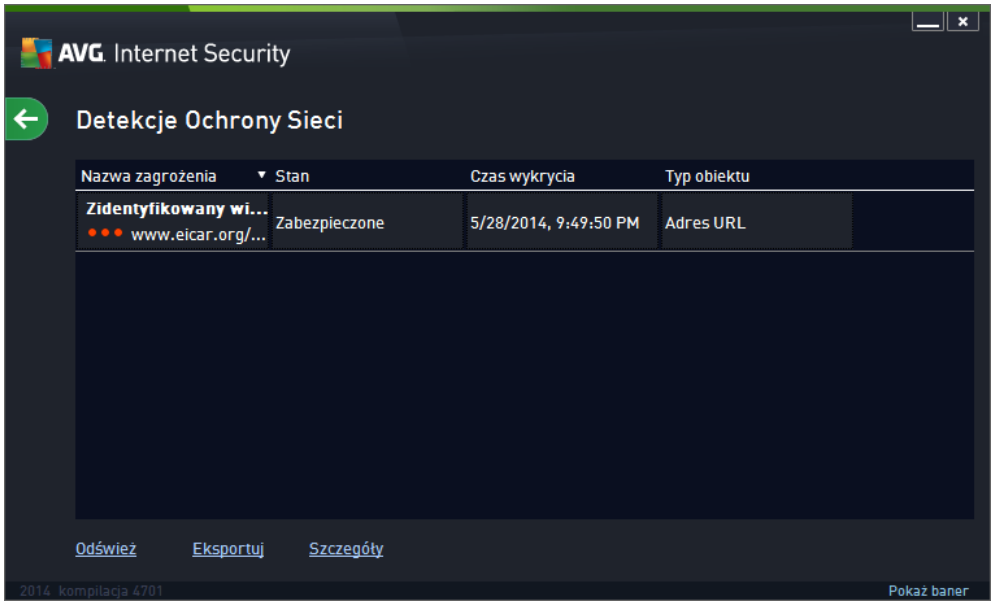
Ochrona Sieci skanuje zawartość odwiedzanych stron internetowych (oraz znajdujących się na nich plików) jeszcze zanim zostaną wyświetlone w przeglądarce lub pobrane na dysk twardy. Wykrycie jakiegokolwiek zagrożenia powoduje natychmiastowe wyświetlenie następującego okna:

To okno ostrzegawcze podaje informacje o wykrytym obiekcie, który został uznany za infekcję (*Zagrożenie*), a także kilka opisowych faktów o samej infekcji (*Nazwa obiektu*). Link Więcej informacji przeniesie Cię do encyklopedii wirusów online, 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 (np. 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***. To okno dostępne jest poprzez menu ***Opcje / Historia / Zagrożenia wykryte przez Ochronę Sieci*** w górnej części nawigacyjnej głównego okna **AVG Internet Security 2014.**



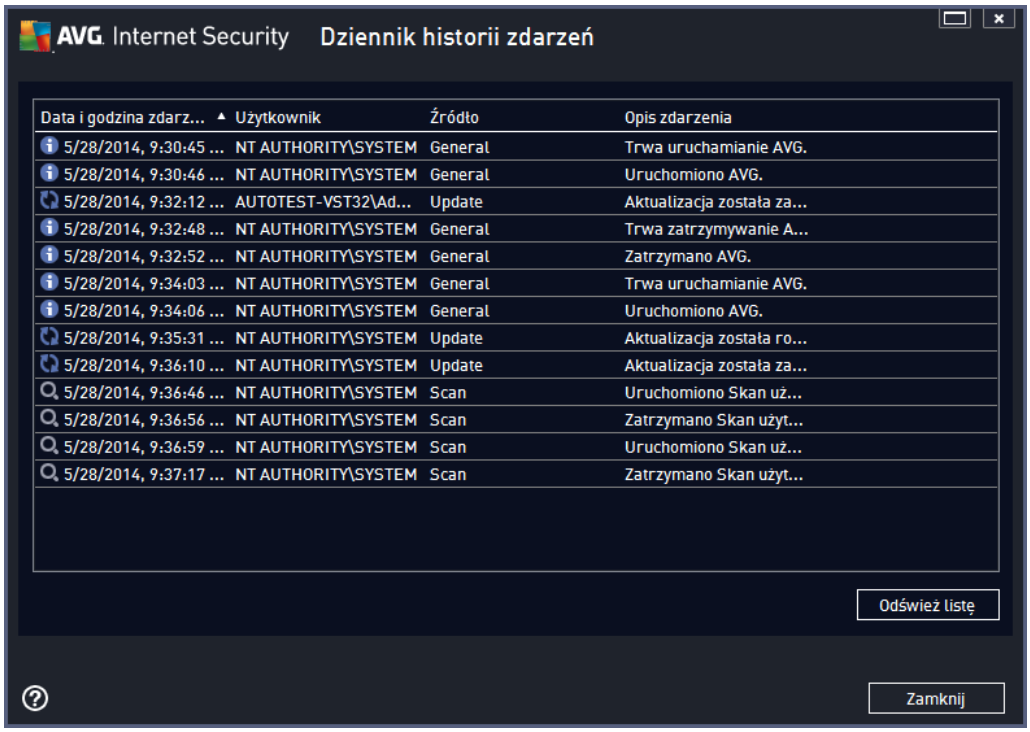
Podawane są tam następujące informacje:

- ***Nazwa zagrożenia*** – opis (*a także możliwa nazwa*) wykrytego obiektu oraz jego pochodzenie (*strona internetowa*).
- ***Wynik*** – działanie podjęte w związku z wykryciem.
- ***Czas wykrycia*** – data i godzina wykrycia i zablokowania zagrożenia.
- ***Typ obiektu*** – typ wykrytego obiektu.
- ***Proces*** – akcja wykonana w celu wywołania potencjalnie niebezpiecznego obiektu (co umożliwiło jego wykrycie).

Przyciski kontrolne

- ***Odśwież*** – pozwala zaktualizować listę obiektów wykrytych przez składnik ***Ochrona Sieci.***
- ***Eksportuj*** – eksportuje listę wykrytych obiektów do pliku.
- – by powrócić do domyślnego okna głównego AVG *(przeglądu składników),* użyj strzałki znajdującej się w lewym górnym rogu tego okna.

14.6. Dziennik historii



Okno ***Dziennika historii zdarzeń*** dostępne jest poprzez ***Opcje / Historia / Dziennik historii zdarzeń*** w górnym menu nawigacyjnym głównego okna **AVG Internet Security 2014**. Okno to zawiera podsumowanie najważniejszych wydarzeń, które wystąpiły w czasie pracy systemu **AVG Internet Security 2014**. Okno to zawiera wpisy na temat następujących typów zdarzeń: informacje o aktualizacjach systemu AVG; informacje o rozpoczęciu, zakończeniu lub zatrzymaniu skanowania (*włączając w to 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 czas wystąpienia zdarzenia.
- ***Użytkownik*** states the name of the user currently logged in at the time of the event occurrence.
- ***Źródło*** podaje nazwę składnika lub innej części systemu AVG, która wywołała zdarzenie.
- ***Opis zdarzenia*** przedstawia krótkie podsumowanie zdarzenia.

Przyciski kontrolne

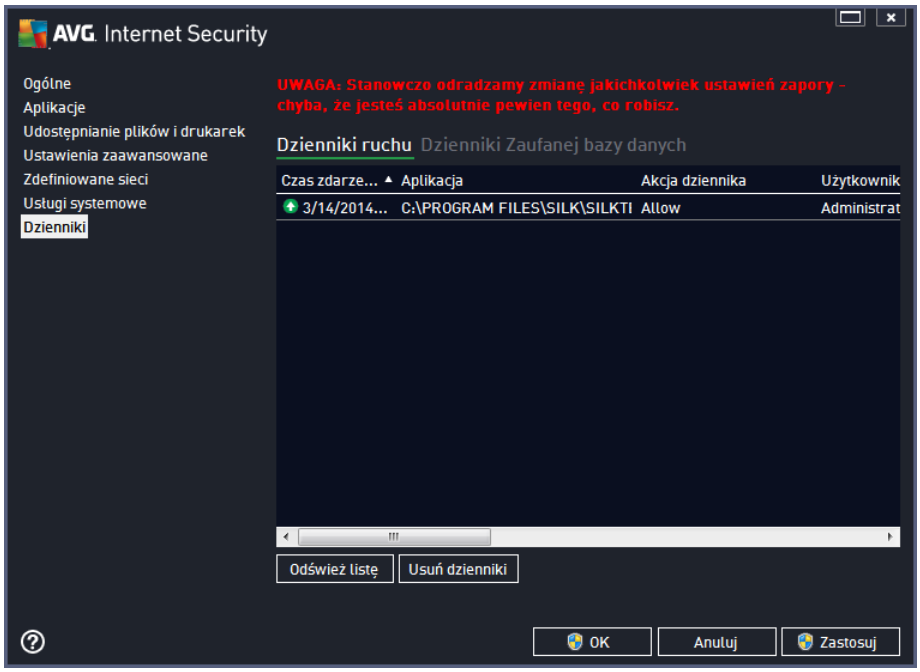
- ***Odśwież listę*** – powoduje odświeżenie całej listy.
- ***Zamknij*** – kliknij, by powrócić do głównego okna **AVG Internet Security 2014**

14.7. 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 zdarzenia, nazwie aplikacji, zarejestrowanej akcji, nazwie użytkownika, numerze PID, kierunku ruchu, typie protokołu, numerze portu zdalnego i lokalnego, a także 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 siecią (*np. gdy jeszcze nie została utworzona reguła Zapory dla tej aplikacji*), konieczna jest decyzja, czy zezwolić na komunikację sieciową. Najpierw system AVG przeszukuje bazę *Trusted Database*. Jeśli aplikacja znajduje się na liście, dostęp do sieci zostanie jej automatycznie umożliwiony. Dopiero gdy 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

- ***Odśwież listę*** – wszystkie zarejestrowane parametry można uporządkować według wybranego atrybutu: chronologicznie (*data*) lub alfabetycznie (*inne kolumny*) – wystarczy kliknąć odpowiedni nagłówek kolumny. Użyj przycisku ***Odśwież listę***, aby zaktualizować wyświetlane informacje.

- ***Usuń dzienniki*** – pozwala usunąć wszystkie wpisy.

15. Aktualizacje systemu AVG

Żadne oprogramowanie zabezpieczające nie może zapewnić realnej ochrony przed różnymi typami zagrożeń bez regularnych aktualizacji. 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 ilość nowo powstających zagrożeń internetowych oraz prędkość z jaką się rozprzestrzeniają, regularna aktualizacja systemu **AVG Internet Security 2014** jest absolutnie niezbędna. Najlepszym rozwiązaniem jest w tym wypadku pozostawienie domyślnych ustawień automatycznej aktualizacji. Przypominamy, że jeśli baza wirusów lokalnego systemu **AVG Internet Security 2014** jest nieaktualna, wykrycie najnowszych zagrożeń może być niemożliwe!

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

15.1. Uruchomienie aktualizacji

Aby zapewnić maksymalną dostępną ochronę, produkt **AVG Internet Security 2014** domyślnie sprawdza dostępność nowych aktualizacji bazy wirusów co 4 godziny. Aktualizacje sytemu 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.

Jeżeli chcesz natychmiastowo sprawdzić dostępność nowych definicji, użyj szybkiego linku Aktualizuj teraz. Jest on widoczny przez cały czas w głównym oknie interfejsu użytkownika. Po uruchomieniu tego procesu program AVG sprawdza, czy dostępne są nowe pliki aktualizacyjne. Jeśli tak, system **AVG Internet Security 2014** rozpocznie ich pobieranie i sam uruchomi proces aktualizacji. Zostaniesz poinformowany o wynikach aktualizacji za pomocą wysuwanego okna nad ikoną AVG w zasobniku systemowym.

Jeżeli chcesz zmniejszyć ilość 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, na następujących ekranach:

- Harmonogram aktualizacji definicji
- Harmonogram aktualizacji programu
- Harmonogram aktualizacji bazy Anti-Spam

15.2. Poziomy aktualizacji

AVG Internet Security 2014 oferuje dwa poziomy aktualizacji:

- ***Aktualizacja definicji*** zawiera uzupełnienia niezbędne do zapewnienia niezawodnej ochrony antywirusowej i antyspamowej. Na ogół nie zawiera modyfikacji programu i aktualizuje tylko bazę definicji. Ta aktualizacja powinna zostać zastosowana, gdy tylko

będzie dostępna.

- ***Aktualizacja programu*** zawiera różne zmiany w programie, poprawki i udoskonalenia.

Podczas planowania aktualizacji można zdefiniować jej parametry dla każdego z poziomów:

- Harmonogram aktualizacji definicji
- Harmonogram aktualizacji programu

Uwaga: *Jeśli zaplanowana aktualizacja programu pokrywa się z zaplanowanym skanowaniem, proces aktualizacji ma wyższy priorytet, więc skanowanie zostanie przerwane. W takim przypadku, użytkownik zostanie poinformowany o niezgodności.*

16. FAQ i pomoc techniczna

Jeżeli masz jakiekolwiek pytania natury technicznej lub handlowej (dotyczące produktów **AVG Internet Security 2014**), 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. Znajdują się tam podstawowe informacje o zainstalowanym systemie AVG (*wersja programu i bazy wirusów*), szczegóły licencji oraz lista przydatnych linków.

- ***Rozwiązywanie problemów przy użyciu plików pomocy***: Nowa sekcja ***Rozwiązywanie problemów*** dostępna jest bezpośrednio w plikach pomocy **AVG Internet Security 2014** *(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*** znajdziesz uporządkowaną strukturę tematów opisujących kwestie handlowe i techniczne.

- ***Często zadawane pytania***: Na stronie AVG (*http://www.avg.com/*) opublikowana jest również obszerna sekcja często zadawanych pytań. Można się do niej dostać poprzez menu ***Centrum Pomocy technicznej / FAQ i poradniki*** . Wszystkie pytania podzielone są w czytelny sposób na sekcje: handlową, techniczną i na temat wirusów.

- ***AVG ThreatLabs***: Specjalna strona AVG (*http://www.avgthreatlabs.com/website-safety-reports/*) 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, zlokalizowanego pod adresem http://forums.avg.com.