

Instrukcja obsługi
programu antywirusowego
avast!
Home Edition wersji 4.8

SPIS TREŚCI

Wprowadzenie	4
O firmie ALWIL Software a.s.	4
Dalsza pomoc	4
Zagrożenia dla komputera	5
Czym jest wirus?.....	5
Co to jest program szpiegujący?.....	5
Czym są rootkity?.....	5
Kluczowe cechy programu antywirusowego avast!.....	6
Jądro antywirusowe.....	6
Ochrona dostępową (lub ochrona „na-dostęp”)	7
Technologia antyspyware	7
Technologia antyrootkit	7
Silna Samoobrona	7
Automatyczne aktualizacje	7
Kwarantanna.....	8
Integracja systemów	8
Zintegrowany program czyszczący z wirusów	8
Skanowanie z linii wiersza (Jedynie w wersji avast! Professional).....	9
Blokada skryptów (Jedynie w wersji avast! Professional).....	9
Wymuszone aktualizacje PUSH (Jedynie w wersji avast! Professional).....	9
Rozszerzony interfejs użytkownika (Jedynie w wersji avast! Professional)	9
Wymagania systemowe	10
Jak zainstalować program antywirusowy avast! Home Edition?.....	11
Uruchamianie	16
Ochrona przy pomocy hasła	18
Jak się zarejestrować aby uzyskać klucz aktywacyjny?.....	18
Wpisywanie klucza licencyjnego	19
Podstawowe informacje dla użytkownika program antywirusowego avast!.....	20
Ochrona dostępową	20
Jak ustawić ręczne skanowanie – Prosty interfejs użytkownika	24
Wybór obszaru skanowania ręcznego	26
Ustawienie procesu i czułości skanowania	28
Uruchamianie skanowania oraz praca z wynikami skand.....	29
Zmiana wyglądu prostego interfejsu użytkownika.....	30
Co zrobić, jeśli został wykryty wirus?	32
Wyniki skanowania	36
Ustawienia zaawansowane.....	37
Ustawienie automatycznych aktualizacji	37
Jak ustawić Skanowanie podczas rozruchu?.....	38
Wykluczanie ze skanowania.....	40
Jak stworzyć raport ze skanowania?.....	41
Alerty.....	44
SMTP.....	45
Szukanie wirusów w bazie danych	46
Praca z plikami w Kwarantannie	48
Log podglądu	50
Konfiguracja osłony dostępowej.....	52
Inne ustawienia programu avast!	65

Ustawienia współdzielone	65
<i>Rozszerzenie eksploratora</i>	65
Wygląd	66
Potwierdzenia	66
Zmiana języka programu	68
Dźwięki	69
Aktualizacje (połączeń)	70
Rozwiązywanie problemów	71
Jak aktywować antywirusowy wygaszacz ekranu avast!	73
Jak dokonać aktualizacji do wersji Home Edition	79
Jak odinstalować program antywirusowy avast!	80

Wprowadzenie

Zapraszamy do przeczytania instrukcji obsługi programu antywirusowego avast! Home Edition w wersji 4.8.

Program antywirusowy avast! to wielokrotnie nagradzana, wysokiej klasy technologia, działające w idealnym połączeniu. Posiada jeden cel: chronić Twój system i cenne dane przed wirusami komputerowymi. avast! Home Edition to najlepsze w swojej klasie rozwiązanie dla każdej stacji roboczej z systemem operacyjnym Windows.

Program antywirusowy avast! posiada technologię anti-spyware i anti-rootkit, certyfikowaną przez West Coast Lab Process, jak również doskonale działający system Samoobrony, gwarantujący, że cenne dane i programy pozostają pod ciągłą ochroną.

O firmie ALWIL Software a.s.

Od 1988 r. ALWIL Software opracowuje rozwiązania antywirusowe, oferując w chwili obecnej wielokrotnie nagradzaną linię produktów antywirusowych avast!. Dzięki temu avast! jest jednym z najlepszych i sprawdzonych produktów w branży.

ALWIL Software z siedzibą w Pradze w Republice Czeskiej, rozwinęła linię produktów antywirusowych avast!, chroniących wszystkie najważniejsze systemy operacyjne i wszystkie ważniejsze typy urządzeń. Więcej szczegółów na temat firmy i jej produktów można znaleźć na naszej stronie www.avast.com.

avast! ® jest zarejestrowanym znakiem towarowym w Stanach Zjednoczonych Ameryki i innych krajach. Firma ALWIL Software as posiada na niego wyłączną licencję.

Dalsza pomoc

Jeśli wystąpią jakiegokolwiek trudności z programem antywirusowym avast!, których nie jesteś w stanie rozwiązać nawet po przeczytaniu tej instrukcji, spróbuj znaleźć odpowiedź w Centrum pomocy technicznej na naszej stronie internetowej na <http://support.avast.com>

- W sekcji **Wiedza** można znaleźć odpowiedzi na najczęściej zadawane pytania
- Polecamy również nasze Forum wsparcia technicznego avast!. Tutaj możesz porozmawiać z innymi użytkownikami avast! o swoich doświadczeniach. Wielu z nich miało ten sam problem i znalazło już rozwiązanie, które znajdziesz prawie na forum. Aby korzystać z niego, należy się zarejestrować. Jest to bardzo szybki i prosty proces, w tym celu należy wejść na <http://forum.avast.com/>

Jeśli nadal nie możesz rozwiązać swojego problemu, możesz **“Wysłać bilet”** do naszego zespołu pomocy technicznej. W tym celu również należy się zarejestrować. Prosimy napisz nam jak najwięcej informacji.

Zagrożenia dla komputera

Wirusy, spyware, rootkity i wszelkie formy złośliwego oprogramowania są znane pod jedną nazwą jako malware (skrót od złośliwego oprogramowania). Złośliwe oprogramowania są także czasami określane jako „szkodliwe oprogramowania”.

Czym jest wirus?

Wirus komputerowy to typ programu, zwykle o złośliwym charakterze, który jest wykorzystywany do rozpowszechniania lub rozprzestrzeniania innych tego typu programów z komputera na komputer. Same wirusy mogą powodować uszkodzenie systemu, utratę cennych danych, lub mogą zostać użyte do instalacji programów szpiegujących, rootkitów lub innego złośliwego oprogramowania w systemie.

Głównym sposobem zapobiegania infekcjom jest posiadanie aktualnego rozwiązania antywirusowego zainstalowanego na wszystkich komputerach w sieci. Dodatkowo użytkownik powinien upewnić się, że wszystkie najnowsze zabezpieczenia dla systemu operacyjnego komputera zostały również zainstalowane. Użytkownicy powinni także upewnić się, że mogą mieć zaufanie, co do pochodzenia oprogramowania pobieranego z Internetu, ponieważ wiele typów złośliwego oprogramowania jest instalowanych wraz z innymi legalnie wyglądające oprogramowaniami.

Co to jest program szpiegujący?

Spyware to oprogramowanie zainstalowane często bez zgody lub wiedzy użytkownika, na jego komputerze. Celem programu jest zbieranie informacji o komputerze i jego użytkowniku. Może dojść do tak zwanej kradzieży tożsamości użytkownika i cennych danych (tak jak na przykład dane banku, karty kredytowej) lub danych firmy.

W obecnych czasach tego typu działalność prowadzą przede wszystkim zorganizowane grupy przestępcze a nie osoby indywidualne.

Czym są rootkity?

Rootkity to programy, które, pomimo że zainstalowane w systemie, działają w ukryciu i pozostają niewidoczne dla użytkownika. Stanowią one znaczne zagrożenie dla bezpieczeństwa komputerów domowych i firmowych sieci oraz są niezwykle trudne do wykrycia i usunięcia.

Rootkity są zazwyczaj instalowane za pośrednictwem innego złośliwego oprogramowania (na przykład Trojan). Dlatego jest wysoce zalecane, aby komputer użytkownika posiadał aktualny system broniący przed złośliwym oprogramowaniem. Jednym z takich systemów jest program antywirusowy avast! 4.8.

Kluczowe cechy programu antywirusowego avast!

avast! to wielokrotnie nagradzana i posiadająca certyfikat laboratorium ICSA linia produktów antywirusowych wyprodukowana przez ALWIL Software as. Program antywirusowy avast! regularnie otrzymuje ocenę 100% od Virus Bulletin, ze względu na umiejętność wykrywania 100% wirusów na wolności. Jest również wielokrotnym laureatem nagród Secure przyznawanych przez Computing Award.

Program antywirusowy avast! jest używany w ponad 75 milionach domów i biur na całym świecie. Posiada niskie wymagania systemowe. Aktualizacje: zarówno programu jak i bazy wirusów są automatycznie i przyrostowe.

avast! stanowi zbiór high-end technologii zaprojektowanych tak, aby chronić Państwa komputery przed wszelkimi formami złośliwych oprogramowań. Główne cechy programów antywirusowych avast! Home Edition i Home Edition są porównane i opisane poniżej.

Kluczowe ustawienia	Home Edition	Home Edition
Jądro antywirusowe oparte na wysokiej wydajności silniku antywirusowym	Tak	Tak
Silna ochrona dostępu	Tak	Tak
Ochrona przed programami spyware	Tak	Tak
Ochrona przed programami rootkit	Tak	Tak
Silna Samoobrona	Tak	Tak
Automatyczne aktualizacje przyrostowe	Tak	Tak
Kwarantanna do przechowywania podejrzanych i zarażonych plików	Tak	Tak
Integracja systemu	Tak	Tak
Zintegrowany program czyszczący z wirusów	Tak	Tak
Skaner z wiersza poleceń	Nie	Tak
Blokowanie skryptów	Nie	Tak
Aktualizacje push	Nie	Tak
Udoskonalony interfejs użytkownika oraz możliwość tworzenia oraz określania harmonogramu zadań	Nie	Tak

Jądro antywirusowe

Jądro antywirusowe, to trzon programu. Najnowszą wersję jądra programu antywirusowego avast! wyróżnia wyjątkowa zdolność wykrywania wirusów oraz wysoka wydajność. Użytkownik może się spodziewać niemal 100% wykrywalności wirusów „na wolności” (wirusów już rozprzestrzeniających się między użytkownikami) oraz doskonałej wykrywalności koni trojańskich.

Jądro antywirusowe uzyskało certyfikaty laboratorium **ICSA Labs**; Bierze również udział w testach Virus Bulletin, często zdobywając nagrodę VB100.

Ochrona dostępową (lub ochrona „na-dostęp”)

Ochrona dostępową (w czasie rzeczywistym ochrony systemu komputerowego), jest jedną z najważniejszych cech programu antywirusowego. Ochrona dostępową avast! jest kombinacją kilku elementów lub tzw. „modułów dostępowych”, które są w stanie wykryć wirusa zanim zainfekuje komputer.

Technologia antyspyware

Program antywirusowy avast! ma teraz wbudowaną technologię anti-spyware, której jakość poświadczą certyfikat West Coast Labs, oferując jeszcze większą ochronę cennych danych i programów.

Technologia antyrootkit

Technologia antyrootkit w oparciu o wiodącą klasę technologii GMER jest również standardowo zainstalowana w program. Jeśli rootkit zostanie wykryty, zostanie wyłączony, a następnie usunięty, jeśli go można bezpiecznie usunąć bez wpływu na wydajność komputera. Program antywirusowy avast! zawiera bazę danych wirusów, która jest automatycznie aktualizowana w celu zapewnienia ciągłej ochrony przed rootkitami.

Silna Samoobrona

Niektóre wirusy mogą próbować wyłączyć oprogramowanie antywirusowe. Aby chronić komputer nawet przed najnowszymi zagrożeniami, które mogą starać się wyłączyć zabezpieczenia, avast! posiada najlepszą w swojej klasie silną Samoobronę. Stanowi ona dodatkową warstwę ochronną w celu zapewnienia bezpieczeństwa danych i programów.

Automatyczne aktualizacje

Automatyczne aktualizacje są kolejnym kluczowym punktem ochrony przed wirusami. Zarówno baza wirusów i samego programu jest automatycznie aktualizowana. Aktualizacje są przyrostowe. Oznacza to, że do bazy wirusów i programu dodawane są jedynie nowe lub brakujące dane, co znacząco skraca czas pobierania. Typowy rozmiar aktualizacji bazy wirusów to kilkadziesiąt KB. Aktualizacja programu zazwyczaj nie zabiera więcej niż setki KB.

Jeśli masz stałe łączenie z Internetem (połączenie szerokopasmowe), aktualizacje wykonywane są całkowicie automatycznie w ustalonych odstępach czasu. Jeśli łączysz się z Internetem tylko sporadycznie, avast! monitoruje połączenia i próbuje wykonać aktualizację, gdy jesteś online. Funkcja ta jest opisana dalej na **stronie 37**.

Kwarantanna

Kwarantanna może być traktowana jako specjalny folder na dysku, posiadające specjalne właściwości, które czynią z niego bezpieczne, odizolowane miejsce nadające się do przechowywania potencjalnie szkodliwych plików. Można pracować z plikami w kwarantannie, choć przy zachowaniu odpowiednich środków ostrożności.

Kwarantanny to fakt, że wirusy są w pełnej izolacji od reszty systemu operacyjnego. Programy takie jak wirusy, mogą uzyskać dostęp do plików wewnątrz. Jednak w wewnątrz Kwarantanny plik nie może być uruchamiany. Oznacza to, że nie grozi niebezpieczeństwo magazynowania wirusów. Aby uzyskać więcej informacji, patrz [strona 48](#)

Integracja systemów

Program antywirusowy avast! posiada w pełni zintegrowany system. Rozszerzenie Explorer umożliwia skanowanie, które można uruchamiać bezpośrednio przez kliknięcie na folder lub plik prawym przyciskiem myszy i wybranie odpowiedniej opcji z menu.

Zastosowaliśmy również specjalny wygaszacz ekranu, który jeśli jest aktywny skanuje w poszukiwaniu wirusów. Program antywirusowy avast! współpracuje z Twoim ulubionym wygaszaczem ekranu. Aby z niego nadal korzystać, nie trzeba więc zmieniać ustawień osobistych. Aby skonfigurować wygaszacz ekranu programu antywirusowy avast! zobacz [strona 73](#).

W 32-bitowych wersjach systemu Windows NT/2000/XP/VISTA, możliwe jest również uruchomienie „skanowania z rozruchu”, który pozwala na przeprowadzenie skanowania podczas uruchamiania systemu przed wirusami i mogą być aktywowane. Jest to przydatne, jeśli podejrzewasz, komputer może już zainfekowany przez wirus.

Zintegrowany program czyszczący z wirusów

Podstawowym zadaniem programu antywirusowego avast! jest zasadniczo ochrona komputera przed wirusami lub innymi formami złośliwego oprogramowania. Dlatego podstawową funkcją programu jest zapobieganie zarażeniu a nie leczenie. Jednak teraz avast! zawiera specjalnego czyściciela wirusów, który jest w stanie usunąć niektóre z popularniejszych wirusów z zainfekowanych komputerów. Niestety, liczba wirusów w obiegu stale rośnie, a w przypadku, gdy komputer zostanie zainfekowany przez wirusa, które nie mogą być usunięte przez Czyściciela, może być niezbędna pomoc eksperta.

Więcej informacji na temat programu czyszczącego wirusa można znaleźć na naszej stronie www.avast.com

Skanowanie z linii wiersza (Jedynie w wersji avast! Professional)

Dla doświadczonych użytkowników wersji avast! Home Edition przygotowaliśmy opcję skanowania z wiersza poleceń. Skanowanie można uruchomić z wieloma parametrami i skorzystać z wielu filtrów, oraz specjalnego modułu STDIN/STDOUT. Moduł jest przeznaczony do użytku w programach wsadowych tzw. BATCH. Wyjście programu jest takie samo jak dla zadań przeprowadzonych z poziomu zaawansowanego interfejsu użytkownika (włącznie z raportami z działania programu).

Blokada skryptów (Jedynie w wersji avast! Professional)

Ochrona dostępową oprogramowania Home Edition zawiera dodatkowy moduł, tak zwaną Blokadę skryptów. Moduł ten skanuje wszystkie skrypty znajdujące się w systemie operacyjnym (tak zwane skrypty WSH Windows Scripting Host) i skanuje skrypty jako część strony WWW bez użycia przeglądarki (Internet Explorer, Netscape Navigator i Mozilla). Zdarzają się luki bezpieczeństwa w przeglądarce, które mogłyby zostać wykorzystane przez wirus, co może spowodować zarażenie komputera. W związku z tym avast! przeprowadza kontrole na stronach, które odwiedzasz, dbając o to, żeby nie przedostały się żadne podejrzanym skrypty, które mogą być potencjalnie niebezpieczne.

Wymuszone aktualizacje PUSH (Jedynie w wersji avast! Professional)

Specjalną opcją, którą posiada avast! Home Edition jest aktualizacja wymuszona PUSH. To miły krok w filozofii aktualizacji. Najczęściej każdy zainstalowany program okazjonalnie kontroluje najnowsze dostępne wersje. System oparty jest na protokole SMTP (przeznaczonym do Twoich wiadomości e-mailowych). Aktualizacja sama w sobie jest kontrolowana przez dostawcę rezydentalnego Poczta avast! (MS Outlook oraz Internet Mail).

Cały system jest chroniony przez asymetryczne kody i jest odporny na niewłaściwe użycie.

Rozszerzony interfejs użytkownika (Jedynie w wersji avast! Professional)

Dodatkowo oprócz prostego interfejsu, wersja avast! Professional Edition posiada tzw. Rozszerzony interfejs użytkownika, który umożliwia dostęp do wszystkich ustawień i kontroli nad skanowaniem. W przeciwieństwie do Prostego interfejsu użytkownika, skanowanie można ustawić przy pomocy poleceń tzw. "Zadań". Najpierw należy zdefiniować polecenie, łącznie z parametrami, obszarem i sposobem skanowania. Ustawione polecenia, możesz powtarzać. Każde polecenie generuje listę wyników, którą możesz później analizować. Inne kluczowe ustawienie, zbliżone do systemu poleceń to Harmonogram. Ta opcja pozwala na zaplanowanie poleceń w czasie, tak, aby przebiegały jednorazowo lub okresowo. Dodatkowo możliwe jest również ustawienie istniejących opcji skanowania. Takie ustawienie nie jest możliwe w prostym interfejsie użytkownika. Cechy rozszerzonego interfejsu użytkownika są opisane bardziej szczegółowo w instrukcji obsługi programu avast! Professional Edition.

Wymagania systemowe

Konfiguracje sprzętu opisane poniżej stanowią **minimalne** wymagania systemowe, poszczególnych systemów operacyjnych

Dla komputera z Windows 95/98/Me:

PC 486, 32 MB RAM, 50 MB wolnego miejsca na dysku.

Dla komputera z Windows NT 4.0:

PC 486, 32 MB RAM, 50 MB wolnego miejsca na dysku, zainstalowany Service Pack 3 lub wyższy.

Dla komputera z Windows 2000/XP (stacji roboczej, nie dla serwera):

PC Pentium, 64 MB RAM (zalecane 128 MB), 50 MB wolnego miejsca na dysku.

Dla komputera z Windows Vista:

PC Pentium 4, 512 MB RAM, 50 MB wolnego miejsca na dysku.

Pentium 4 procesor, 512MB RAM oraz 50 MB wolnego miejsca na twardym dysku
AMD Athlon64, Opteron lub Intel EM64T-enabled Pentium 4 / Xeon procesor, 128MB RAM (polecane 256MB) oraz 50 MB wolnego miejsca na twardym dysku

(Sam program **wymaga 20 MB**. Reszta jest zarezerwowana dla pliku bazy odzyskiwania danych po ataku wirusa oraz jej indeksu. [Baza VRDB, określana także w poprzedniej wersji jako "baza integralności"])

Funkcjonalny **MS Internet Explorer 4** lub nowsza wersja wymagana jest do pracy tego programu.

Dla systemu Windows® XP® 64-bit Edition:

Pentium 4 procesor, 512MB RAM oraz 50 MB wolnego miejsca na twardym dysku

Uwaga: w wyniku instalacji więcej niż jednego produktu zabezpieczającego na tym samym komputerze mogą powstać różne problemy. Jeśli masz zainstalowane inne oprogramowanie zabezpieczające zaleca się jego odinstalowanie, przed zainstalowaniem programu avast!

Jak zainstalować program antywirusowy avast! Home Edition?

W tej części instrukcji obsługi zostało opisane, jak należy pobrać i zainstalować program antywirusowy avast! Home Edition na komputerze i jak wpisać klucz aktywacyjny do oprogramowania po zakończeniu procesu instalacji. Zrzuty ekranu pokazane na następnych stronach pojawią się w systemie Windows XP i mogą się nieznacznie różnić od innych wersji systemu Windows.





Program antywirusowy avast! Home Edition można pobrać z www.avast.com.

Polecamy zamknąć wszystkie inne programy systemu Windows przed rozpoczęciem pobierania.

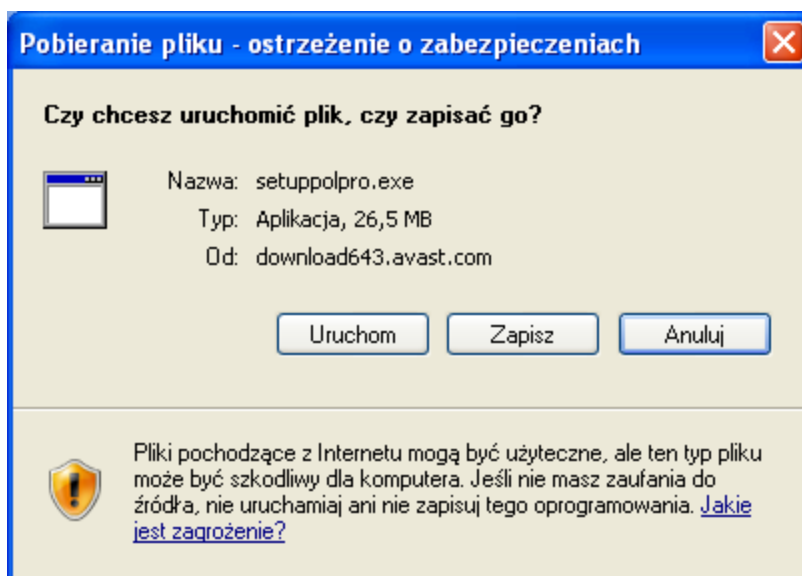
Kliknij przycisk "Pobierz", następnie "Pobierz programy", a następnie wybierz wersję językową, którą chcesz pobrać.

Z listy, wybierz odpowiednią wersję językową i kliknij na szary przycisk "Pobierz".

Pobierz avast! 4 Home Edition

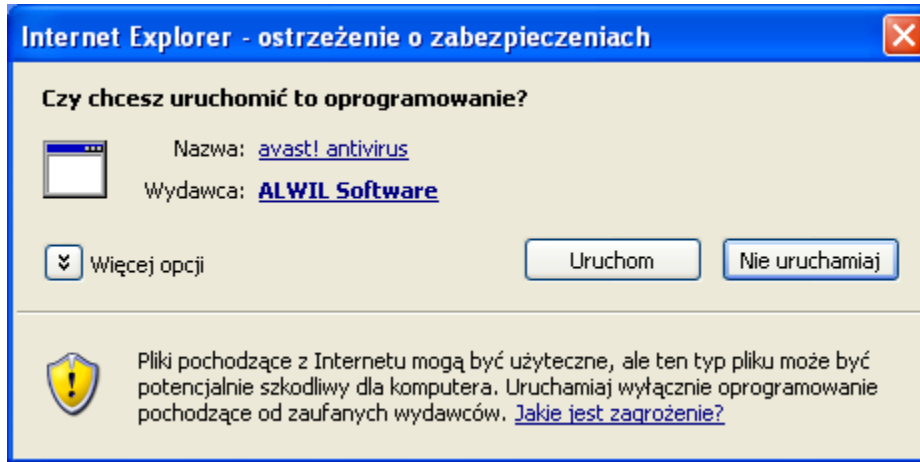
 Download	avast! 4 Home – wersja angielska (length 21.70 MB)
 Download	avast! 4 Home - wersja arabska (length 21.50 MB)
 Download	avast! 4 Home - wersja bułgarska (length 21.54 MB)
 Download	avast! 4 Home - wersja katalońska (length 21.80 MB)

Jeśli korzystasz z programu Internet Explorer jako przeglądarki internetowej, pojawi się następujący obrazek:



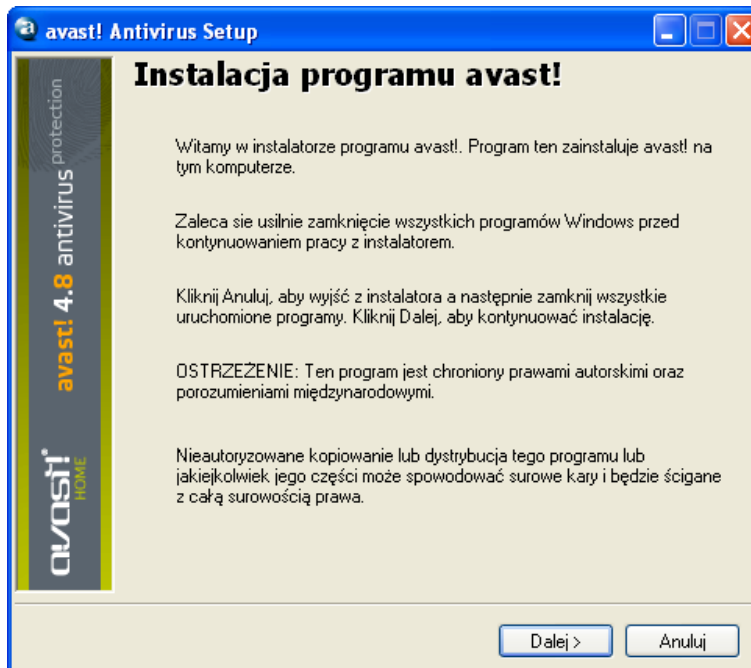
Kliknij przycisk "Uruchom" lub "Zapisz". Następnie rozpocznie się pobieranie pliku instalacyjnego "Setupeng.exe".

Jeśli chcesz aby program antywirusowy avast!, został od razu uruchomiony po zakończeniu instalacji, kliknij przycisk "Uruchom". Po zakończeniu pobierania pliku instalacyjnego pojawi się następujący obrazek:



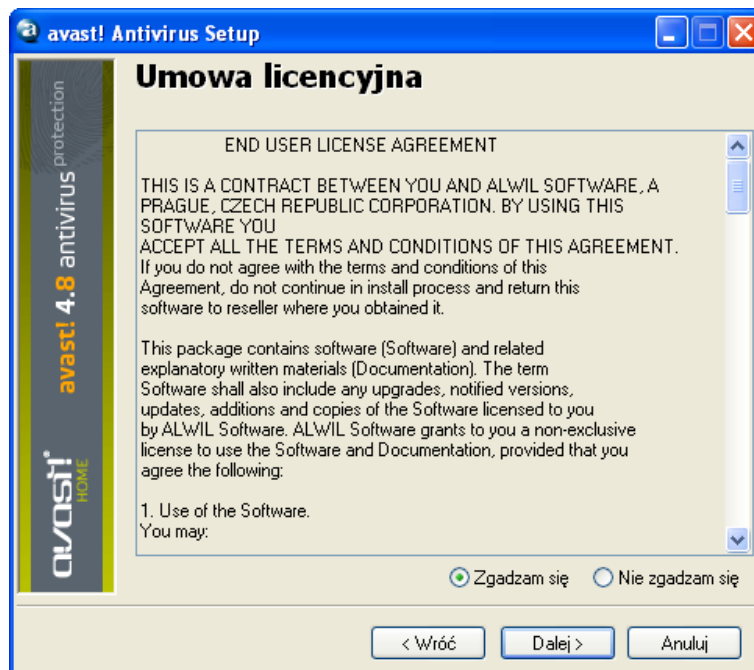
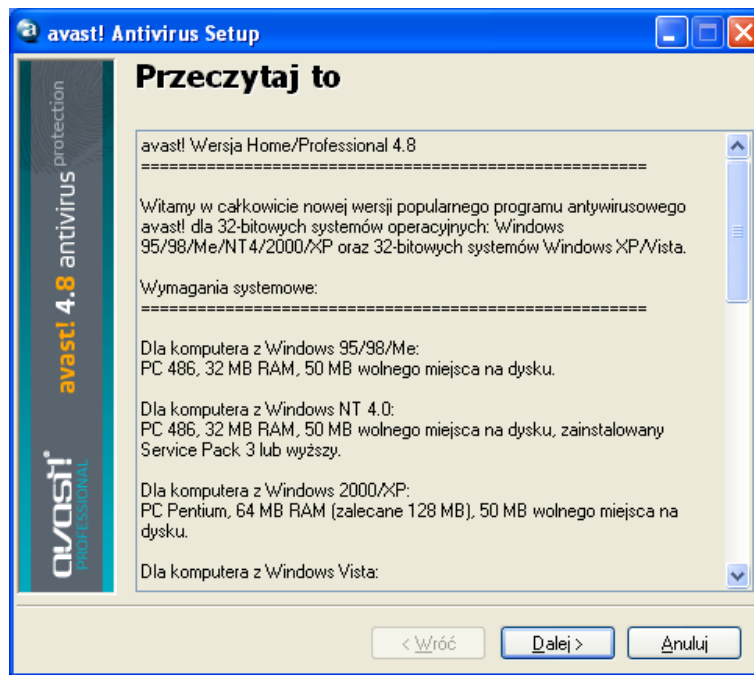
W innych przeglądarkach internetowych, może pojawić się jedynie opcja "Zapisz" plik. Klikając na "Zapisz" rozpoczniesz pobieranie oprogramowania, ale nie zostanie on natychmiast zainstalowany. Aby dokończyć proces instalacji należy uruchomić plik instalacyjny "Setupeng.exe" który będzie pamiętać, gdzie został zapisany! Dwukrotnie kliknij na plik, aby go uruchomić.

Klikając ponownie "Uruchom" przejdziesz do „ustawień” avast!:



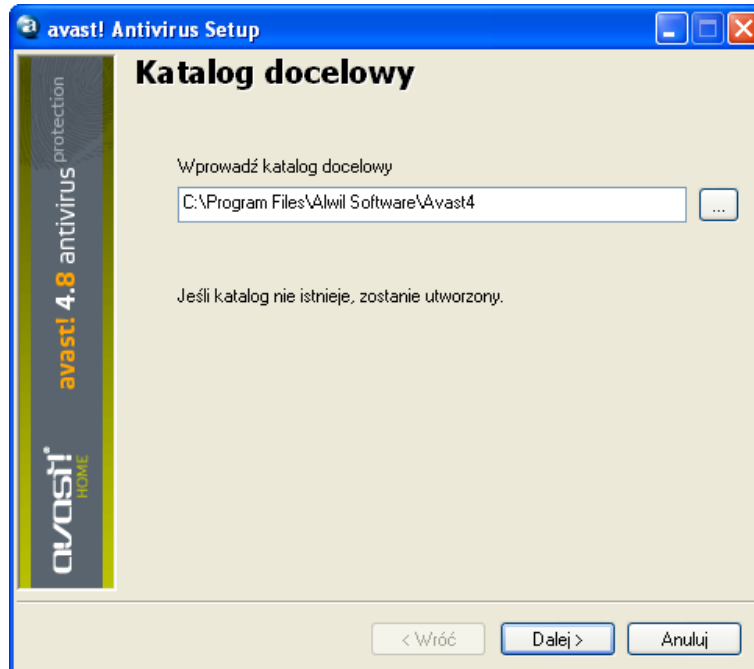
Kliknij przycisk "Dalej", a kreator instalacji poprowadzi Cię przez resztę procesu instalacji.

Po pierwsze zostaniesz poproszony o przeczytanie informacji dotyczących minimalnych wymagań systemowych, a następnie o potwierdzenie, że zgadzasz się z warunkami licencji dla użytkownika końcowego - patrz poniżej na następujące dwa obrazki

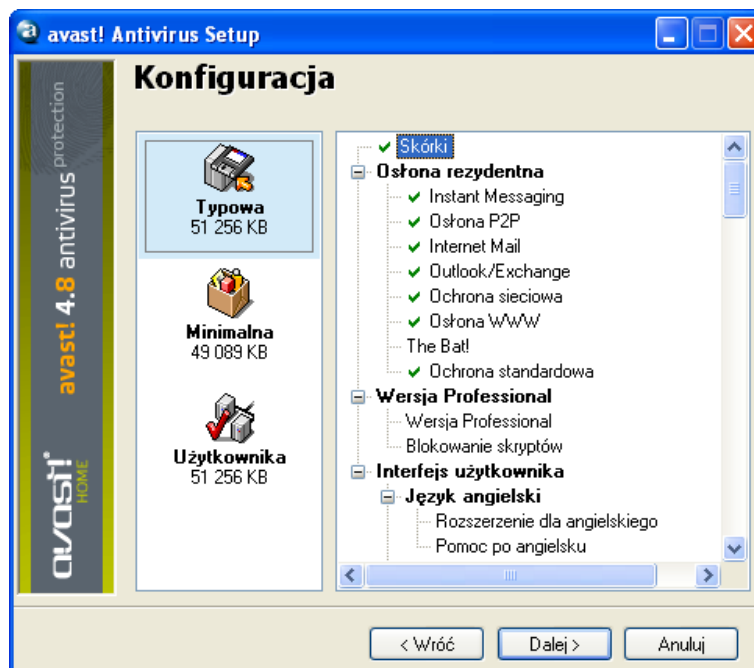


Aby kontynuować, należy kliknąć przycisk "Zgadzam się", i „Dalej”

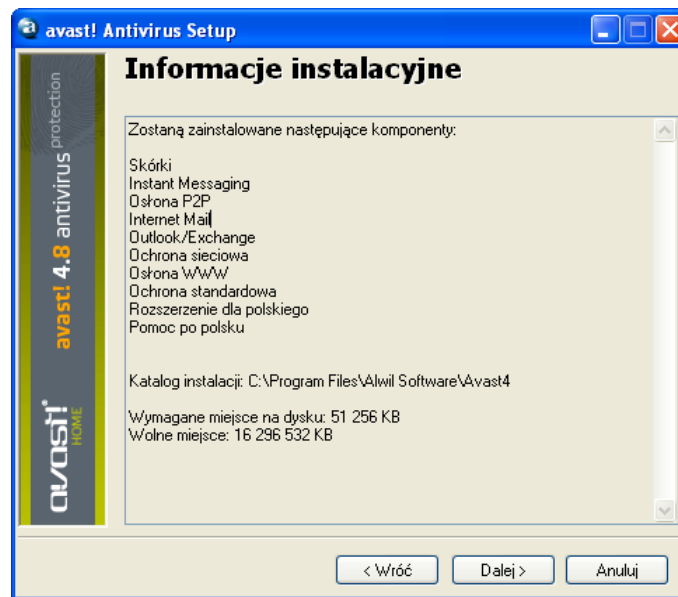
Zostaniesz poproszony o potwierdzenie katalogu docelowego, tzn. gdzie pliki programu powinny zostać zapisane. Program wybierze go automatycznie lub utworzy nowy katalog, jeżeli ten jeszcze nie istnieje. Polecamy zaakceptować domyślny katalog docelowy i kontynuować klikając "Dalej".



W następnym oknie, użytkownik zostanie poproszony o potwierdzenie konfiguracji. Opcje odpowiednie dla większości użytkowników są wybierane automatycznie. Jeśli jednak chcesz zmienić jakiegokolwiek z ustawień domyślnych, np. wybrać inny język, wystarczy kliknąć przycisk "Dalej", aby kontynuować.



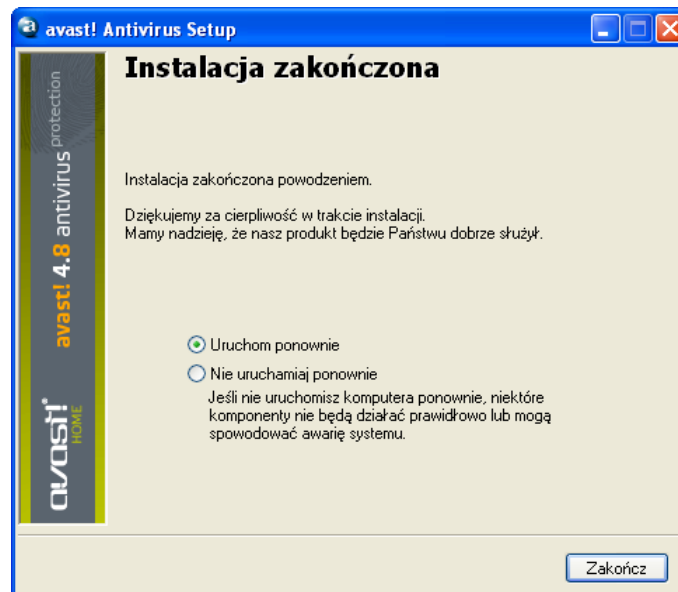
Program będzie się dalej pytać co ma zostać zainstalowane, gdzie, oraz poinformuje jest ilość wolnego miejsca na dysku jest wymagana. Kliknij przycisk "Dalej", aby kontynuować.



Zostaniesz poproszony o potwierdzenie, czy chcesz zaplanować skanowanie w czasie rozruchu - patrz [strona 38](#).

Końcowy obrazek powinien potwierdzić, że instalacja została pomyślnie zakończona. Jednak, aby dokończyć proces instalacji konieczne będzie ponowne uruchomienie komputera.

Należy wyprać opcję "Uruchom ponownie", kliknij przycisk "Zakończ" i komputer zostanie automatycznie uruchomiony ponownie.



Instalacja została zakończona.

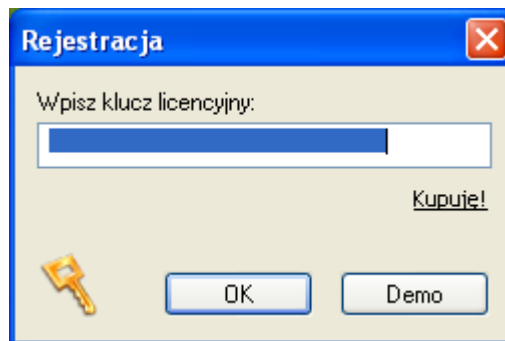
Uruchamianie

Po ponownym uruchomieniu komputera, powinieneś ujrzeć niebieską "a-ikonę " w prawym dolnym rogu ekranu komputera.



Program antywirusowy avast Home Edition może być wykorzystywany bezpłatnie przez pierwszych 60 dni. Jednak po upływie tego okresu próbnego, jeżeli chcesz go nadal używać, musisz dokonać rejestracji i wpisać klucz aktywacyjny w program.

Dlatego też, kiedy po raz pierwszy uruchomisz program, pojawi się następujący obrazek i komunikat:



Nie jest wymagane wprowadzenie klucza licencyjnego natychmiast. Jeśli chcesz uruchomić program na okres do 60 dni bez ubiegania się o klucz aktywacyjny, po prostu kliknij na wersję "Demo". Jednakże, możesz ubiegać się o klucz aktywacyjny od razu, kliknij na "kup teraz" i postępuj zgodnie z procedurą opisaną w następnym akapicie.

Po wybraniu wersji demo do uruchomienia, pole to nie zostanie wyświetlone po następnym uruchomieniu programu. Jednakże, możesz ubiegać się o klucz aktywacyjny w dowolnym momencie - patrz następna strona "Jak się zarejestrować w celu uzyskania klucza licencyjnego" .

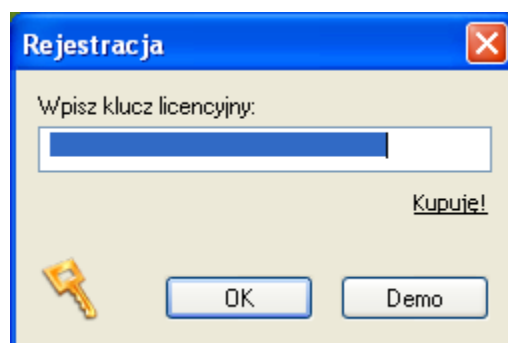
Po upływie 60 dni, jeśli klucz aktywacyjny nie zostanie wpisany, w prawym dolnym rogu ekranu komputera pojawi się, następujące ostrzeżenie:



Następujący komunikat będzie się pojawiał za każdym razem, gdy uruchomisz program:



Klikając przycisku "OK" spowodujesz, że pojawi się okno:



Procedura uzyskiwania i wpisywania klucza licencyjnego jest opisana na następnych stronach.

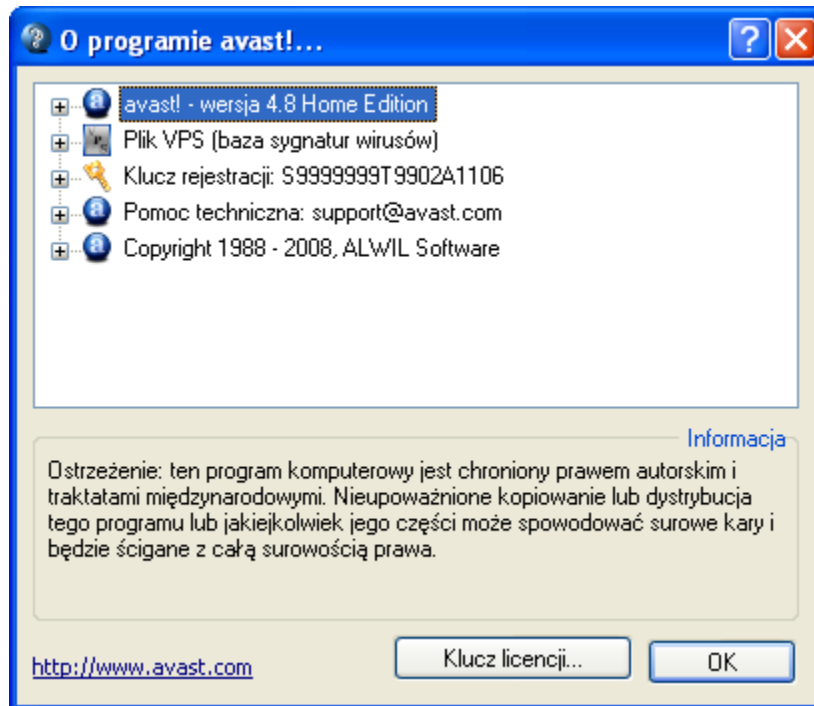
Ochrona przy pomocy hasła

Klikając prawym klawiszem na niebieską "a- ikonę" w prawym dolnym rogu ekranu i zaznaczając opcję "Ustaw / zmień hasło" można utworzyć hasło, aby chronić swój program antywirusowy przed nieautoryzowanymi zmianami.

Jak się zarejestrować aby uzyskać klucz aktywacyjny?

Jeśli chcesz nadal korzystać z programu po upływie bezpłatnego, 60 dniowego okresu próbnego, należy zarejestrować się i wpisać ważny klucz aktywacyjny w program.

Aby zakupić klucz aktywacyjny, kliknij na „Wsparcie” i wybierz opcję "Darmowa rejestracja avast!" na stronie www.avast.com, a następnie wypełnij krótki formularz rejestracyjny. Jeśli masz już pobrany i zainstalowany program, kliknij prawym klawiszem myszy na niebieskim "a-ikonkę" w prawym dolnym rogu ekranu i wybierz opcję "O avast! ..."



Pojawi się okno rejestracyjne, kliknij na „rejestracja programu”

Po ukończeniu instalacji klucz aktywacyjny zostanie wysłany na Twój adres mailowy w ciągu 24 godzin.

Wpisywanie klucza licencyjnego

Po otrzymaniu klucza aktywacyjnego (który zostanie wysłany pocztą elektroniczną na adres podany podczas procesu zakupu) należy go wpisać w program. Umożliwi to automatyczne aktualizacje programu i bazy wirusów oraz dzięki temu unikniesz dalszych ostrzeżeń o wpisaniu klucza aktywacyjnego.

Uwaga– program antywirusowy avast! musi zostać pobrany przed wprowadzeniem klucza aktywacyjnego.

Aby obejrzeć instrukcje video, jak włożyć klucz aktywacyjny bez uruchamiania programu, kliknij **tutaj** lub przejdź na stronę www.avast.com i kliknij na "Wsparcie" na górze ekranu. Z menu wybierz "Pomoc techniczna". Następnie w lewym dolnym rogu ekranu, znajdź "Instrukcję video" i kliknij na "Jak wpisać klucz aktywacyjny".

Ewentualnie wykonaj czynności opisane poniżej.

1. Podkreśl klucz aktywacyjny w e-mailu, który otrzymałeś od avast! Aby to zrobić, przesunij kursor na ekranie tak, że aby najechać nim od razu na lewo od pierwszej litery klucza aktywacyjnego. Kliknij lewym przyciskiem myszy i trzymając nadal wciśnięty lewy przycisk, przesunij mysz w prawo, aż oznaczysz cały klucz aktywacyjny. Zwolnij lewy przycisk myszy, a następnie przesunij mysz do pozycji kursora na zaznaczony klucz aktywacyjny. Kliknij prawym przyciskiem myszy i z menu wybierz "Kopiuj".
2. Kliknij prawym przyciskiem myszy na niebieską "a-ikonkę" w prawym dolnym rogu ekranu, a następnie kliknij lewym przyciskiem myszy "O programie avast!"
3. Kliknij lewym przyciskiem myszy na opcję "Licencja" znajdującą się w prawym dolnym rogu.
4. Umieść kursor w polu klucz aktywacyjny, kliknij prawym przyciskiem myszy i wybierz z listy opcji menu wybierz polecenie "Wklej". Klucza licencyjnego zostanie automatycznie wklejony.
5. Kliknij przycisk "OK". Możesz od teraz używać przez następnych 12, 24 lub 36 miesięcy, w zależności od typu zakupionej licencji. Pod koniec tego czasu, konieczne jest dokonanie zakupu i wstawienie nowego klucza aktywacyjnego.

Podstawowe informacje dla użytkownika program antywirusowego avast!

Program antywirusowy avast! zapewnia ochronę przed wszystkimi typami złośliwego oprogramowania i zawiera potężną "ochronę rezydentalną", również często określane jako "ochronę dostępową", ponieważ sprawdza ona pliki w tej chwili dostępne. (w polskiej wersji programu nazwa została ujednoczona jako ochrona dostępową)

Ochrona dostępową zapewnia całkowitą ochronę komputera i pozwala zapobiegać przed wirusami. Po pobraniu oraz zainstalowaniu programu, ochrona dostępową działa nieprzerwanie w tle, monitorując wszystkie elementy działalności komputera. Jednakże, jeżeli ochrona dostępową została z jakiegokolwiek powodu wyłączona, lub jeśli pozostała nieaktywna przez jakiś czas, nie jest możliwe, aby przeprowadzić ręczne skanowanie z mocą wsteczną (inaczej tzw. skanowanie "na żądanie") wszystkich plików na komputerze.

Program antywirusowy avast! zawiera również specjalny wygaszacz ekranu, który ciągle skanuje Twój komputer, nawet jeśli na nim nie pracujesz, ale jest on wyłączony.

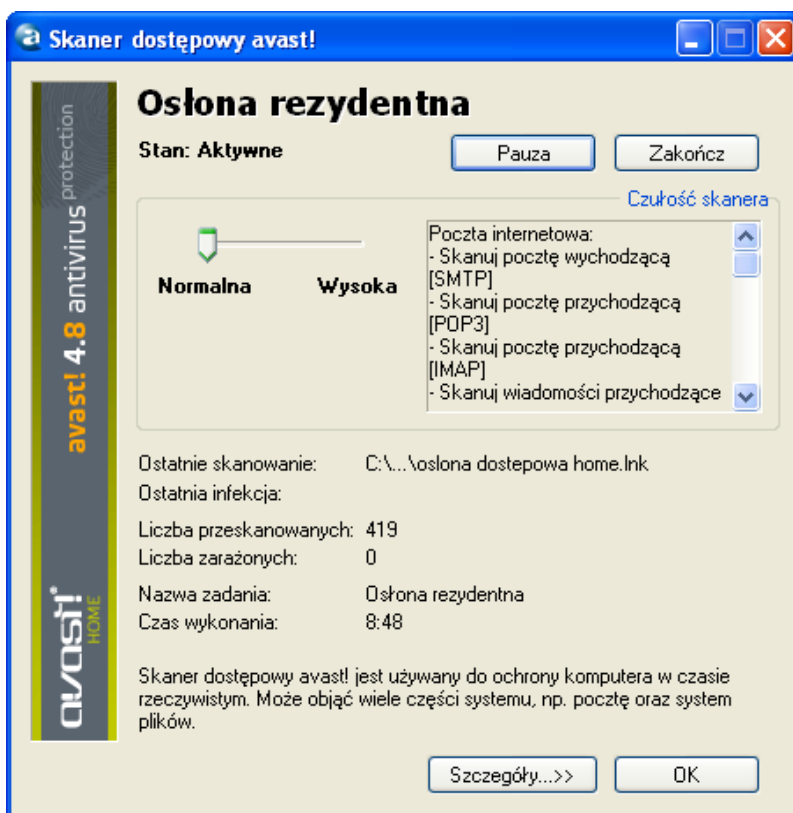
Ochrona dostępową

Ta część programu ciągle monitoruje cały komputer i wszystkie uruchomione programy w celu wykrycia wszelkich podejrzanych działań (np. wirusa), zapobiegając w ten sposób uszkodzeniom plików na komputerze. Ochrona dostępową działa zupełnie niezależnie (uaktywnia się automatycznie wraz z uruchamianiem komputera) i jeśli wszystko jest OK, nawet nie zauważysz, że jest uruchomiona.

Niebieski "a-ikonka" w prawym dolnym rogu ekranu komputera, obok zegara pokazuje aktualny status ochrony dostępowej. Obecności niebieskiej "a-ikonki" wskazuje, że ochrona dostępową jest zainstalowana i aktywnie chroni komputer. Jeśli "a-ikonka" jest przekreślona czerwoną linią, ochrona dostępową jest obecnie nieaktywna, a Twój komputer jest nie jest chroniony. Jeżeli jest szara, oznacza to, że ochrona została wstrzymana - patrz następna strona.

Ochronę dostępową można otworzyć klikając lewym przyciskiem myszy na niebieską "a-ikonkę" w prawym dolnym rogu ekranu, lub klikając prawym przyciskiem myszy i wybierając "Kontrolę ochrony dostępowej".

Pokaże się wówczas następujące okno:



W tej zakładce można czasowo zawiesić ochronę dostępową klikając na "Pauza", lub "Zakończ". Tutaj, obie opcje wywołają taki sam rezultat. Jednakże, ochrona dostępowa zostanie automatycznie przywrócona przy następnym uruchomieniu komputera, w celu upewnienia się, że nie pozostanie on przypadkowo niezabezpieczony.

Możesz również dostosować czułość ochrony dostępowej, poprzez kliknięcie na linii po obu stronach kursora, ustawiając czułości z "Normalnej" lub "Wysokiej". Niemniej jednak, ochrona dostępową składa się z kilku różnych modułów lub tzw. "dostawców", z których każdy został zaprojektowany w celu ochrony różnych części komputera - patrz następna strona. Wszelkie zmiany dokonane na tym ekranie będą miały zastosowanie do wszystkich modułów ochrony dostępowej jednocześnie.

Ochrona dostępową składa się z następujących modułów lub "dostawców":

Komunikatory sprawdzają pliki pobrane przez programy typu "chat" takie jak ICQ i MSN Messenger i wiele innych. Podczas gdy wiadomości błyskawiczne same w sobie nie stanowią poważnego zagrożenia bezpieczeństwa w postaci wirusów, to jednak większość z nich również umożliwia udostępnianie plików - które mogą łatwo prowadzić do infekcji wirusami, jeśli nie są one właściwie monitorowane .

Poczta chroni przychodzące i wychodzące wiadomości, przechodzące przez innych klientów niż MS Outlook i MS Exchange, jak na przykład Outlook Express, Eudora itp.

Ośłona sieciowa chroni przed robakami pochodzącymi z Internetu jak Blaster, Sasser etc. Jest dostępna jedynie dla systemów opartych na systemach Windows NT (Windows NT/2000/XP/Vista).

Outlook/Exchange sprawdza przychodzące oraz wychodzące przechodzące przez MS Outlook i MS Exchange i zatrzymają każdą wiadomość zawierającą potencjalnego wirusa.

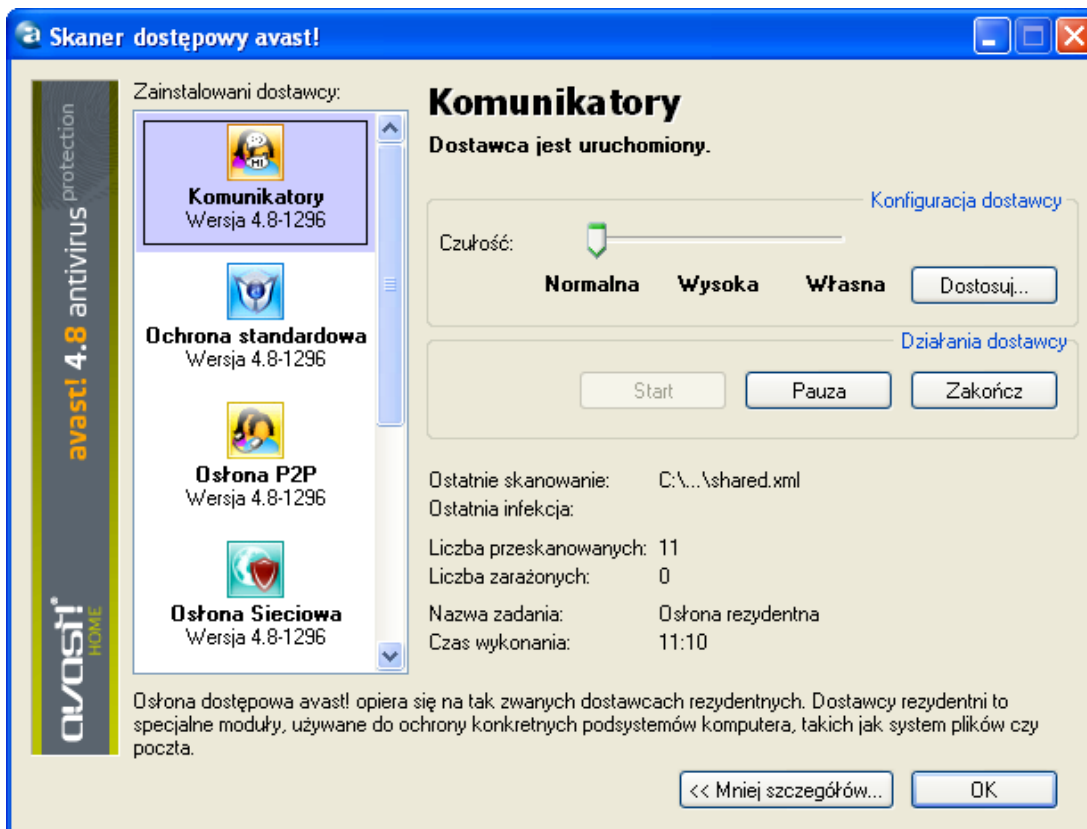
Ośłona P2P służy do sprawdzania plików pobieranych przez sieci P2P (służące do publikowania plików) w programach takich jak Kazaa itp.

Blokowanie skryptów sprawdza skrypty na każdej stronie internetowej, aby zapobiec zarażeniu przez skrypty, które szukają luk w przeglądarce internetowej, aby zarazić komputer.

Ochrona Standardowa sprawdza otwarte i uruchomione programy i dokumenty. Zapobiega uruchomieniu zainfekowanego programu lub dokument i przed otwarciem wirusa, zapobiegając tym samym aktywowaniu wirusa, które może spowodować wiele szkód.

Ośłona WWW chroni komputer przed wirusami podczas korzystania z Internetu (przeglądanie witryn, pobieranie plików itp.). Może również zablokować dostęp do określonych stron internetowych. Jeśli doszło do pobrania zainfekowanego pliku, ośłona WWW zapobiegnie uruchomieniu wirusa nie powodując żadnych szkód. Jednakże, ośłona WWW wykryje wirus nawet wcześniej - w trakcie pobierania pliku, zapewniając jeszcze silniejszą ochronę. Ośłona WWW jest kompatybilna ze wszystkimi głównymi przeglądarkami WWW, w tym Microsoft Internet Explorer, Firefox, Mozilla i Opera. Ze względu na unikalną funkcję o nazwie "Inteligentne skanowanie strumieni", który pozwala pobrać pliki, które mają być skanowane niemal w czasie rzeczywistym, jej wpływ na szybkość przeglądania jest niemal znikoma.

Istnieje możliwość ustawienia intensywności działania każdego dostawcy osobno. Aby zmienić czułość skanowania, włączyć pauzę lub zakończyć wystarczy kliknąć na okno „Szczegóły”, a wtedy pojawi się poniższe okno:



W rozszerzonym polu, poszczególne moduły są wyświetlane w panelu w dół po lewej stronie. Czułość każdego modułu można ustawić przez kliknięcie na odpowiedni moduł po lewej stronie, a następnie przesuwając suwak po linii do lewej do prawej strony. W tym polu możliwe jest również zatrzymanie działania poszczególnych części ochrony dostępowej, czasowo bądź na stałe, klikając odpowiednio albo na "Pauza" albo na "Zamknij". Po kliknięciu przycisku "Pauza", odpowiedni moduł zostanie automatycznie przywrócony po następnym uruchomieniu komputera. Jeśli wybierzesz opcję "Zamknij", program zapyta, czy chcesz aby ten konkretny moduł pozostał wyłączony na zawsze, czy też powinien zostać wznowiony po ponownym uruchomieniu komputera obok - patrz [strona 66](#). Jeśli klikniesz przycisk "Tak", moduł pozostanie wyłączony, nawet po ponownym uruchomieniu komputera, dopóki nie zostanie ponownie ręcznie aktywowany.

Istnieje szereg dodatkowych opcji, które mogą być wybrane dla każdego dostawcy. Na przykład możliwe jest, aby określić typy plików, które powinny być skanowane. Te dodatkowe opcje są dostępne po kliknięciu "Dostosuj" i są opisane na [stronie 52](#) - Konfiguracja ochrony dostępowej.

Jak ustawić ręczne skanowanie – Prosty interfejs użytkownika

Podczas pierwszego uruchomienia programu, pokaże się Ci obrazek przypominający srebrny / szary radio / odtwarzacz CD, który zawiera wszystkie elementy sterujące dla określenia, uruchomienia i przetwarzania wyników skanowania - patrz poniżej. Jest to domyślny wygląd lub tzw. "skóra" programu (może być zmieniony przez wybranie innych "skórek" - patrz [strona 30](#)).

Początkowo odtwarzacz pojawia się za oknem zawierającym „Krótkie wprowadzenie”. Kliknij przycisk "Więcej informacji", aby dowiedzieć się więcej, a następnie "Strona główna", aby wrócić do głównego ekranu. Odpowiednie informacje są podsumowane na następnych stronach. Możesz powrócić do tych kluczowych punktów ponownie i w dowolnym momencie, korzystając z [opcji menu](#) (patrz następna strona) i wybierając „Pomoc - wprowadzenie”.



W środku odtwarzacza, lekko na prawo znajduje się okno dotyczące status informacji:

- **Bieżąca wersja bazy wirusów** – baza wirusów zawiera szczegóły dotyczące obecnej aktualizowanej bazy wirusów oraz jest wykorzystywana przez program do identyfikacji podejrzanych plików.
- **Osłona dostępową** – tutaj możesz zobaczyć bieżący poziom czułości ustawienia
- **Data ostatniego skanowania** – w dniu, w którym ostatnio skanowanie ręczne uruchomienie
- **Baza odzyskiwania danych** – zawiera szczegóły dotyczące plików zainstalowanych na komputerze i jest używana do ich naprawy, jeżeli zostały one uszkodzone przez wirusa. Podana data jest w dniu, w którym doszło do ostatniej aktualizacji bazy odzyskiwania danych.
- **Automatyczne aktualizacje** – pokazują stan aktualizacji odnoszących się zarówno do bazy danych wirusów i samego programu - aby zmienić stan aktualizacji, kliknij na aktualny stan po prawej stronie okna - zobacz [strona 37](#).

Po obu stronach odtwarzacza można zobaczyć trzy przyciski:

- **W lewym górnym rogu** – ten przycisk otworzy **kwarantannę**. Aby uzyskać więcej informacji o plikach znajdujących się w kwarantannie zobacz **stronę 48**.
- **W środku u góry** – Kliknięcie tego przycisku spowoduje, że wyświetli się pasek z suwakiem, które służy do zmiany czułości ochrony dostępowej. Kliknij na suwak i przesun go w lewo lub w prawo, aby zmniejszyć lub zwiększyć czułość. Uwaga - zmiany poziomu czułości będą miały wpływ na wszystkie moduły ochrony dostępowej. Aby dostosować indywidualnie modułów zobacz **stronę 23**
- **W lewym dolnym rogu** – kliknięcie tego przycisku, lub kliknięcie na aktualny stan na odtwarzaczu otworzy okno do aktualizacji bazy wirusów. Baza wirusów może również zostać aktualizowana, poprzez kliknięcie na niebieską „a-ikonkę” w prawym dolnym rogu ekranu komputera oraz wybranie opcji “Generuj VRDB”.
- **Trzy przyciski po prawej stronie** służą do określenia obszarów, które mają być skanowane - dowolna kombinacja lokalnych dysków, twardej dysków, nośników (dyskietek, płyt CD itp.) oraz wybrane foldery - patrz następna strona.
- **Przycisk START**– klikając ten przycisk rozpoczniesz skanowanie wybranego obszaru (ów). Przycisk ten zmienia się następnie w przycisk PAUZA.
- **Przycisk PAUZA** – klikając ten przycisk wstrzymasz skanowanie (tymczasowo).
- **Przycisk STOP** - klikając ten przycisk zatrzymasz skanowanie.
- **MENU** – Klikając strzałkę na przycisku w lewym górnym rogu odtwarzacza otworzysz **OPCJĘ MENU**. Opcję menu można również otworzyć, umieszczając kursor w dowolnym miejscu nad odtwarzaczem i klikając prawym przyciskiem myszy.

Podczas korzystania z programu bez "skórek" (zobacz **strona 30**), opcje menu są dostępne po kliknięciu na "Narzędzia" lub "Ustawienia" u góry ekranu.

Niektóre opcje mogą być dostępne bez uruchamiania programu, klikając prawym przyciskiem myszy na niebieską "a-ikonkę" w prawym dolnym rogu ekranu komputera.

Wszystkie opcje menu zostały opisane dalej w niniejszej instrukcji obsługi.

Wybór obszaru skanowania ręcznego

Przed rozpoczęciem skanowania, musisz wybrać pliki, które chcesz poddać skanowaniu

- **Skanowanie dysków lokalnych**

Jeśli po prostu chcesz skanować wszystko na komputerze (wszystkie pliki na wszystkich dyskach twardych), kliknij na przycisk w prawym górnym rogu. Ekranu informujący o statusie skanowania zastąpiony nowym ekranem - zobacz poniżej. Aby powrócić do stanu informacji, kliknij prawym przyciskiem myszy na odtwarzaczu i wybierz "informacje o statusie".



Na ekranie, pojawi się nowy wiersz "Skanuj dyski lokalne" i status zmienił się z "Wył" na "Wł."

Możesz również zobaczyć nowe okienko nad odtwarzaczem. Możesz w nim ustawić czułość skanowania. Klikając lewym przyciskiem myszy na suwak i przytrzymując przycisk myszy w dół, można przesunąć suwak w lewo, aby zmniejszyć wrażliwość, lub w prawo, co spowoduje zwiększenie czułości. W tym polu można również wybrać, czy chcesz aby archiwum plików zostało poddane skanowaniu. Opcje te zostały opisane dalej w następnej sekcji.

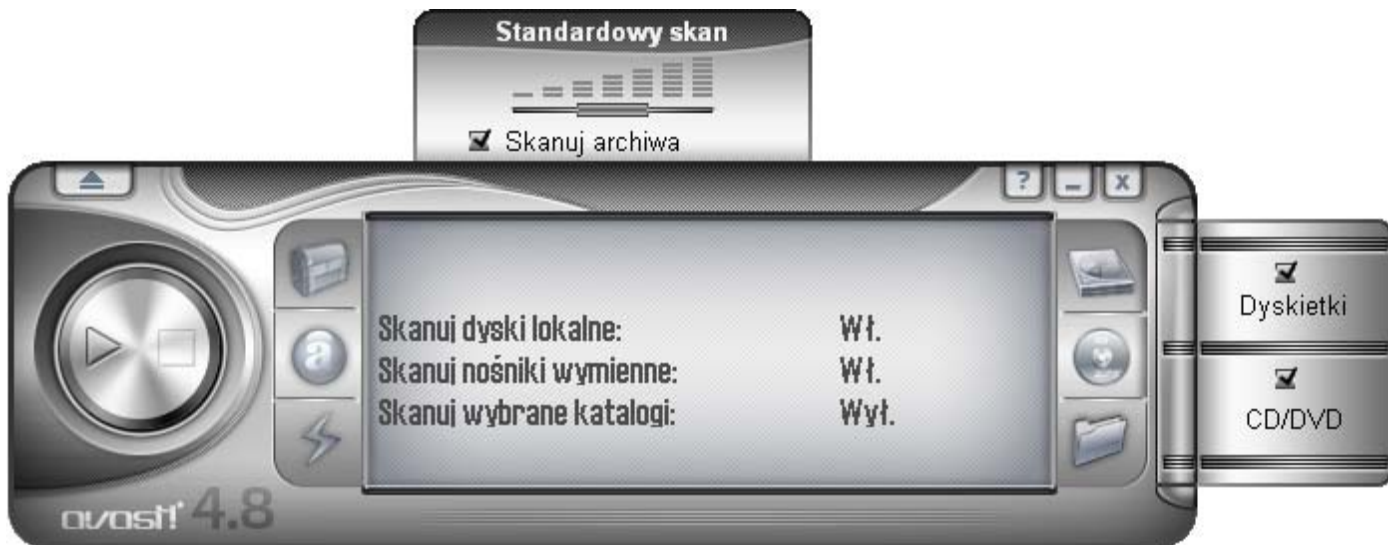
- **Skanowanie nośników wymiennych**

Jeśli chcesz skanować treść niektórych nośników, np. dyskietek lub CD / DVD, kliknij środkowy przycisk po prawej stronie

Kliknięcie tego przycisku spowoduje zmianę statusu "Skanuj nośniki wymienne" z "Wył" na „Wł”.

Dwa okna wyświetlą się dodatkowo po prawej stronie odtwarzacza,. Mogą być one oznaczone lub nieoznaczone, aby pokazać jaki rodzaj nośnika powinien zostać poddany skanowaniu (inne magnetyczne lub magnetyczno optyczne nośniki, takie jak dyski ZIP, traktowane również jako dyskietka).

Okno powyżej odtwarzacza będzie również wyświetlany na której można określić czułość oraz czy chcesz skanować pliki archiwów.



- **Skanowanie wybranych folderów**

To ostatnia opcja - przycisk w prawym dolnym rogu. Należy kliknąć ten przycisk, jeśli chcesz skanować jedynie wybrane foldery. Po kliknięciu tego przycisku, zostanie wyświetlona lista wszystkich folderów na komputerze. Można z niej wybrać foldery, które chcesz poddać skanowaniu. Ustawienie to oferuje największą elastyczność, ale wymaga od użytkownika, określenie dokładnego obszaru skanowania.

Możesz dostosować czułość skanowania i określić, czy pliki w archiwum także powinny być poddane skanowaniu w taki sam sposób jak w przypadku innych obszarów.

Możliwe jest łączenie więcej niż jednego rodzaju skanowania. Na przykład można rozpocząć skanowania wszystkich twardego dysku i klikając zarówno na lokalne dyski oraz nośniki przenośne.

Ustawienie procesu i czułości skanowania

Przy określaniu obszaru (-ów), które mają być skanowane, można także ustawić czułość skanowania i czy program ma skanować zawartość archiwum plików oraz pliki z nazwami, lub z rozszerzeniem. Zip, RAR, ACE, ACJ itp. . Aby skanowanie objęło również te pliki, należy najpierw wybrać obszary, które chcesz poddać skanowaniu (patrz wyżej), a następnie oznaczyć "skanowanie plików archiwum", które pojawia się nad odtwarzaczem. Czułość skanowania określa jak dokładne skanowanie zostanie przeprowadzone. Czułość można ustawić przesuwając suwak w lewo lub w prawo. Można wybrać pomiędzy trzema określonymi poziomami.

- **Szybki skan** ten tryb skanowania, jak sama jej nazwa wskazuje, jest dość szybki. Pliki są badane zgodnie z ich nazwą, a skanowane są jedynie te, które są uznawane za potencjalnie niebezpieczne. Ten typ skanowania może czasami powodować, że niektóre z plików, które zawierają wirusy nie zostaną objęte skanowaniem, jednak zazwyczaj szybkie skanowanie w zupełności wystarcza.
- **Standardowy skan** w tym trybie skanowania plików są analizowane w oparciu o ich zawartość (nie o nazwę, jak w przypadku szybkiego skanowania). Jednak znów jedynie "niebezpieczne" części plików są testowane, a nie cały plik. Ten typ skanowania pomimo, że jest bardziej skuteczny niż Szybki skan, może również nie wykryć pewnych wirusów.
- **Gruntowny skan.** W tym trybie skanowania wszystkie pliki są skanowane w całości i sprawdzone ze względu na wszystkich zakażeń wymienionych w bazie danych. Ten typ skanowania trwa wprawdzie najdłużej ale odznacza się najwyższą wydajnością i efektywnością

Po wybraniu opcji skanowania, jedyne co musisz zrobić, to uruchomić test. Aby to zrobić wystarczy kliknąć na przycisk Start, znajdujący się po lewej stronie odtwarzacza.

Metody alternatywne

Obszar(y) skanowani można określić otwierając **opcje menu** klikając na przycisk "Uruchom skan " a następnie "Wybierz obszar skanowania". Po wybraniu obszaru, który mają zostać poddany skanowaniu, można również określić, czy pliki w archiwum powinny być włączone zaznaczając opcję "Skanuj archiwum plików".

Klikając na "Wybierz poziom skanowania" można również określić, czy skanowanie powinno być Szybkie, Normalne, lub dokładnego jak opisano powyżej.

Uruchamianie skanowania oraz praca z wynikami skanu.

Po kliknięciu na przycisk Start (Uruchom) oraz wybraniu Rozpocznij skanowanie z **opcje menu**, program rozpocznie skanowanie wybranych obszarów. Proces ten może trwać stosunkowo długo, zależy od liczby oraz wielkości testowanych plików oraz szybkości komputera. Warto pamiętać, że opcja Skanowanie gruntowne jest wprawdzie najbardziej czasochłonne, jednakże równocześnie najbardziej efektywne.

Jak tylko program zostanie uruchomiony, możesz pracować normalnie, używając innych programów nawet, jeśli kontynuujesz skanowanie. W tym celu zalecamy zminimalizowanie programu avast! Tak, aby działał on w tle. Jeśli tego nie zrobisz komputer będzie powolny (skanowanie to jedno z bardziej wymagających zadań). Aby nastawić skanowanie w tle, wystarczy wcisnąć przycisk minimalizuj (⏏) w prawym górnym rogu odtwarzacza, w czasie, kiedy proces skanowania jest kontynuowany, a odtwarzacz zniknie z ekranu. Aby go przywrócić należy po prostu kliknąć na okno avast!, które znajduje się na poziomym pasku narzędzi na dole ekranu.

Po zakończeniu skanowania, jeśli nie zostały wykryte żadne wirusy, pojawi się okno przedstawiające takie informacje jak ilość skanowanych folderów, plików oraz czas skanowania itp.

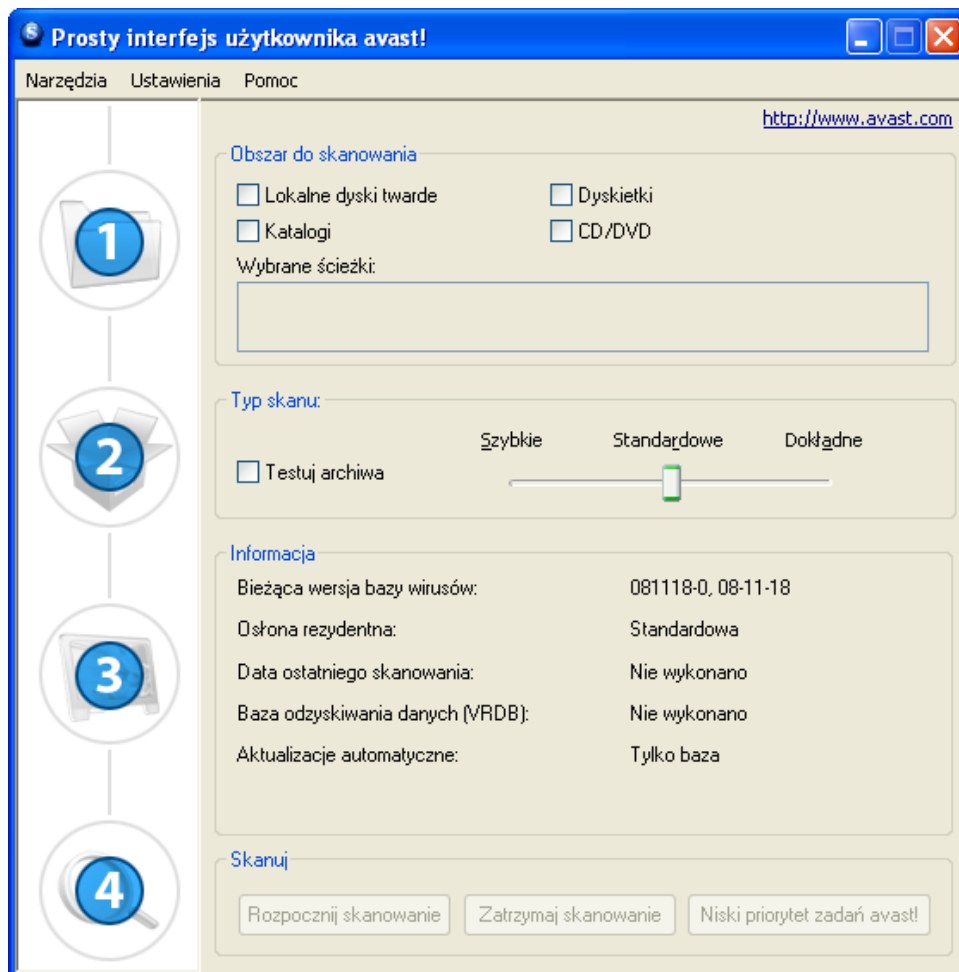


Jeśli zostały wykryte jakiegokolwiek wirusy, program zapyta Cię, co zrobić z zarażonymi plikami. Istnieje kilka możliwości np. Możesz przesunąć pliki do **Kwarantanny**, aby tam je usunąć, zmienić nazwę lub usunąć, a jeśli to możliwe naprawić je. Możesz również pozostawić pliki, aczkolwiek opcja ta może spowodować rozprzestrzenianie się wirusa oraz powodować dalsze szkody. Opcje te zostały omówione szczegółowo w dalszej sekcji **Co zrobić, jeśli został wykryty wirus**".

Zmiana wyglądu prostego interfejsu użytkownika.

Jeśli korzystasz z prostego interfejsu użytkownika, możliwa jest zmiana skórek programu. Do wyboru są trzy różne skórki (wygląd) programu, w wersji standardowej. Pozostałe można pobrać z Internetu, klikając prawym przyciskiem na odtwarzacz avast! A dalej na **opcje menu**, klikając na "Wybierz skórki" a następnie na linka "Wybierz dowolną skórkę przy uruchomieniu aplikacji ...". Możesz również wybrać opcje programu bez żadnych skórek, wybierając, "Ustawienia" z opcji menu, następnie odhaczając "Włącz skórki prostego interfejsu użytkownika". Po następnym uruchomieniu programu, opcja pojawi się w podstawowym formacie. Aby przywrócić skórki, kliknij na "Ustawienia, następnie na Ustawienia ponownie oraz zaznaczyć opcję "Przywróć skórki prostego interfejsu użytkownika". Skórki zostaną przywrócone podczas następnego uruchomienia programu.

Wygląd programu bez żadnych skórek:



Obszar(y) skanowania oraz jego typ, należy ustawić zaznaczając określone okna. Jeśli chcesz skanować jedynie określone foldery, zaznacz foldery, a okno otworzy się pokazując listę wszystkich folderów znajdujących się w Twoim komputerze. Aby wybrać, które z nich chcesz skanować, zaznacz je w okienku obok a pojawią się one w oknie poniżej Wybrane ścieżki.

Intensywność skanowania możesz zmienić przesuwając suwakiem po linii od szybkiego do gruntownego, a jeśli chcesz wybrać skanowanie archiwów, zaznacz opcję Skanowanie archiwów.

Po uruchomieniu skanowania, kontynuuj korzystanie ze swojego komputera, klikając na "Niski priorytet zadań avast!".

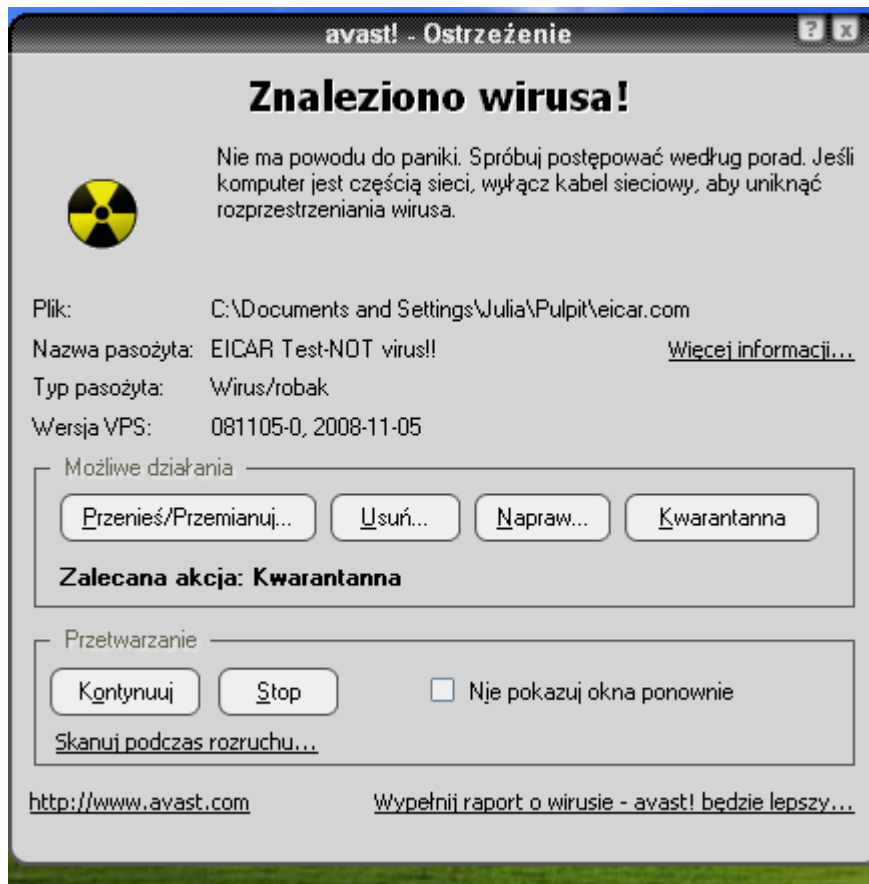
Dodatkowo możesz ustawić czułość ochrony dostępowej, klikając na Ustawienia a następnie na Ochronę dostępową. Skorzystaj z suwaka, zmieniając czułość na Standardową lub Wysoką lub całkowicie wyłączając Ochronę dostępową, klikając na "Zastosuj". Jednakże, jak zostało opisane wcześniej, wszelkie zmiany, jakich dokonasz, zostaną zastosowane do wszystkich dostawców (modułów) ochrony dostępowej. Aby zmienić czułość poszczególnych modułów, zobacz [strona 20](#).

Możesz wejść w inne ustawienia jak na przykład Kwarantanna albo Baza wirusów klikając na Narzędzia I wybierając odpowiednią opcję. Te oraz inne ustawienia zostaną szczegółowo opisane w dalszej części niniejszej instrukcji obsługi.

Dotychczasowy status informacji jest umieszczony w dolnej części ekranu, co zostało opisane w poprzednim akapicie.

Co zrobić, jeśli został wykryty wirus?

Jeśli program wykrył podejrzany plik, skan zostanie przerwany i pojawi się poniższy obrazek, z zapytaniem, co chcesz zrobić z plikiem?

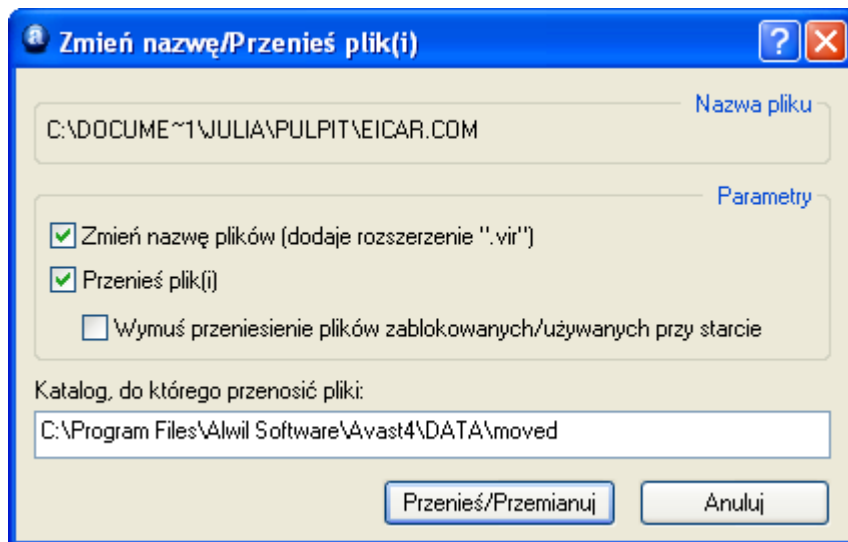


Kliknięcie na "Kontynuuj" będzie oznaczać, że nie zostaną podjęte odpowiednie działania w stosunku do określonych plików i zostanie to zgłoszone na koniec skanowania w wynikach skanowania i podjętych działań - **strona 36**. Klikając na "Stop" zakończysz skanowanie w tym punkcie.

Jeśli wirus zostanie wykryty przez jeden z modułów ochrony dostępowej np. podczas próby otwarcia zainfekowanego pliku, albo przez wygaszasz ekranu, ekran będzie nieco inny - przyciski "Kontynuuj" i "Stop" zostaną zastąpione jednym "Brak działania". Klikając ten przycisk, nie podejmiesz żadnych działań, jednak wirus nie zostanie aktywowany.

Ewentualnie, jeśli chcesz podjąć działania inne działania, istnieją cztery opcje.

Opcja 1: Przeniesienie pliku do folderu znajdującego się w Twoim komputerze. Jednocześnie będziesz miał okazję zmienić jego nazwę. Kliknięcie na "Przenieś / Zmień nazwę" spowoduje w poniższym ekranie są wyświetlane za pomocą "Przenieś plik (ów)" już zaznaczone w tym punkcie.



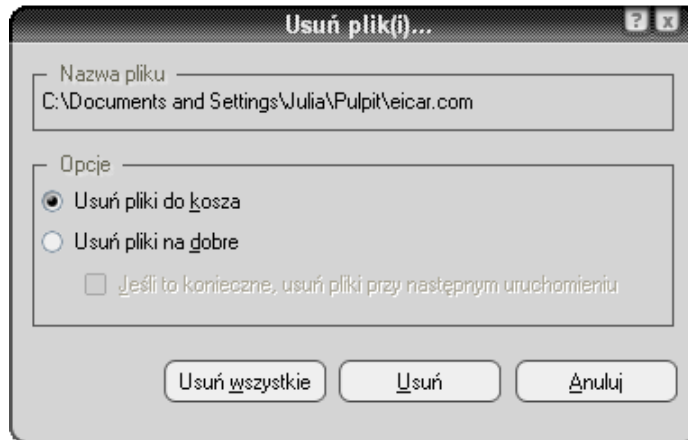
W białej części ekranu, możesz określić, gdzie chcesz, przenieść podejrzany plik. Program automatycznie wybiera odpowiedni folder docelowy, lub można określić inny.

Jeśli również zaznaczysz opcję "Zmień nazwę pliku (-ów)..." należy dodać rozszerzenie „.Vir” na końcu nazwy pliku, tak, aby zidentyfikować go jako potencjalnie niebezpieczny plik oraz aby nie został przypadkowo uruchomiony i nie spowodował szkód na komputerze.

Jeśli jest niemożliwe momentalne przeniesienie pliku, np. Ze względu na to, że jest on używany przez inny program, zaznacz pole u "Wymuś przeniesienie plików zablokowanych / używanych przy starcie " spowoduje plik jest automatycznie przeniesiony w wybrane miejsce po ponownym uruchomieniu komputera.

W przypadku, gdy **pliki systemowe** zostaną zainfekowane to plik, który jest używany do uruchomienia kluczowego programu, przenoszenie plików może spowodować błąd następnym razem komputer próbuje uruchomić program. Jednakże, jeśli plik jest przenoszony do Kwarantanny, będzie chroniony w obszarze kwarantanny, gdzie nie może on spowodować uszkodzenia innych plików i gdzie może zostać naprawiony przed jego ponownym przeniesieniem do pierwotnej lokalizacji - **strona 8**

Opcja 2: Usuń plik, klikając "Usuń" pojawi się następujący obrazek:



W zależności od tego, jakiej wersji Windows używasz, są dwa sposoby jak usunąć pliki.

- Usuwanie plik (ów) do kosza**

W ten sposób przesuń pliki do kosza, ale nie usuniesz ich na zawsze. Istnieje możliwość, że zostaną one później przywrócone. Opcja ta nie jest dostępna w każdej wersji Windows.
- Usuń plik (ów) na dobre**

W ten sposób usuniesz pliki na zawsze swojego komputera, bez możliwości ich przywrócenia. Jednakże w ten sposób jedynie usuniesz zainfekowane pliki. Niektóre wirusy instalują pliki na komputerze i nawet, jeśli nie są one same w sobie wirusa, nie zostaną one wykryte jako podejrzane. Pliki te nie stanowią wprawdzie zagrożenia dla komputera, jednakże zabierają miejsce w pamięci komputera.

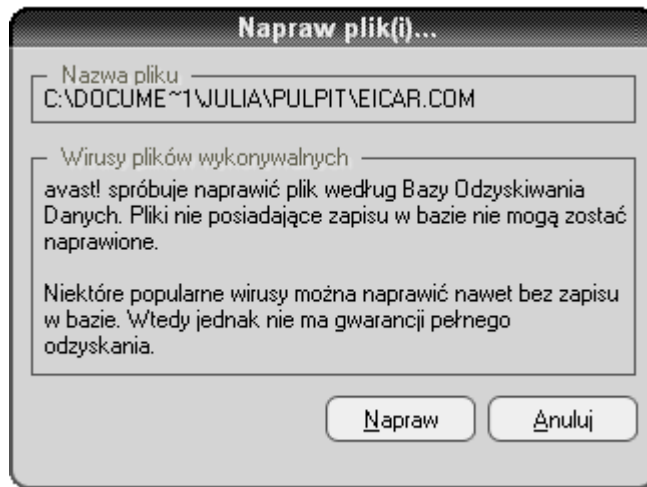
Jeśli wirus został wryty może zostać całkowicie usunięty przez wbudowanego w avast! czyściciela wirusów, włącznie z plikami, które wirus stworzył. W oknie ostrzegającym o wykryciu wirusa może pojawić się dodatkowy przycisk Całkowicie usuń wirus z systemu. Jeśli opcja ta pojawi się, polecamy z niej skorzystać.

Jeśli nie możliwe jest usunięcie pliku w tym momencie, (np. Ze względu na to, że jest on właśnie używany) przez inny program, zaznacz opcję, „jeśli to konieczne, usuń pliki przy następnym uruchomieniu”, dzięki której plik przy następnym uruchomieniu komputera zostanie automatycznie wymazany. Następnie kliknij na „Usuń” ponownie albo potwierdzić usunięcie.

W przypadku, że dojdzie do zainfekowania **plików systemowych** usunięcie pliku, który używany jest do uruchomienia kluczowego programu, może spowodować błąd, przy następnym uruchomieniu pliku przez system. Przed usunięciem pliku, powinieneś się upewnić, że zainfekowany plik nie jest plikiem systemowym lub, że jesteś w stanie zastąpić ten plik. Jeśli nie jesteś pewien, przesuń plik do Kwarantanny. Będzie tutaj bezpieczny i nie będzie zagrażał komputerowi ani innym plikom znajdującym się w komputerze. Może być również naprawiony, a następnie przesunięty do pierwotnej lokalizacji - **zobacz strona 8**

Opcja 3: Napraw plik

Klikając na "Napraw" pojawi się poniższy obrazek:



Klikając ponownie prawym przyciskiem myszy na "Napraw", program ponowi próbę odnowienia pliku w jego pierwotnym stanie.

Aby naprawić plik, program wyśle Cię do bazy danych pozwalających na odzyskanie plików po ataku wirusa..

Jeżeli istnieją wystarczające informacje o programie w bazie danych, istnieje duża szansa, że może on zostać naprawiony. Jeśli nie jedynie pliki, które zostały fizycznie zmieniony przez wirus zostaną naprawione. Jeśli zostały wytworzone nowe pliki, pozostaną nietknięte, o ile czyszciciel wirusów nie jest w stanie ich usunąć - patrz Warian 2.

Jeżeli brakuje informacji w bazie danych, naprawa jest nadal możliwa, ale pełne odzyskanie pliku jest mniej prawdopodobne. Jest zatem bardzo ważne, aby baza wirusów była stale aktualizowana - aby aktualizować bazę danych pozwalających na odzyskanie plików po ataku wirusa. Kliknij prawym przycisk myszy na "a-ikonkę" w prawym dolnym rogu ekranu komputera i wybierz jedną z opcji "Generuj VRDB". Baza danych oraz szczegółowe informacje o wszelkich nowych programach zainstalowanych na komputerze zostaną następnie aktualizowane.

Opcja 4: OPCJA ZALECANA to przeniesienie plików do **Kwarantanny**.

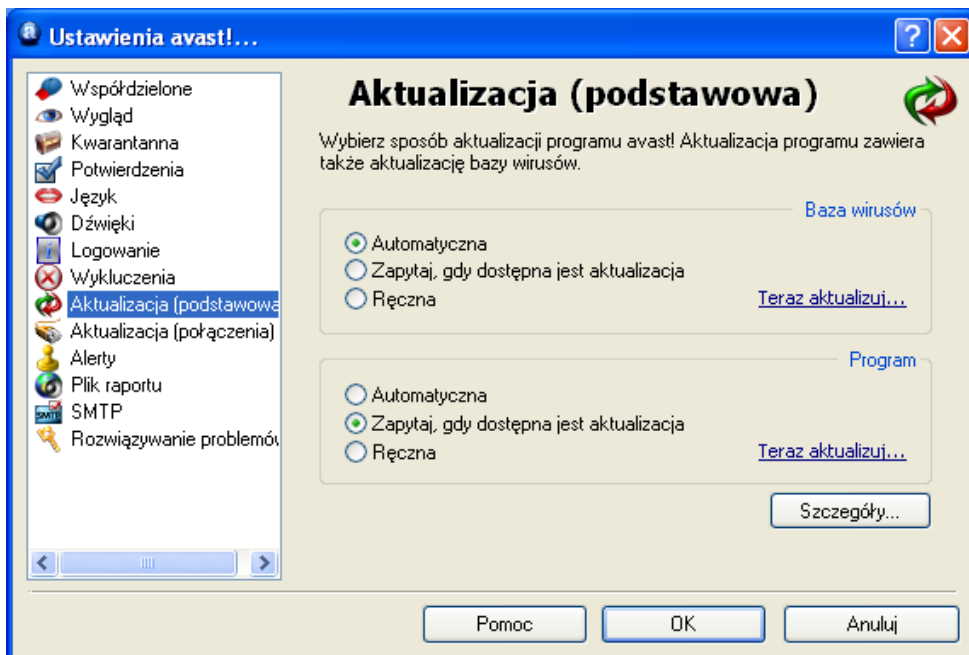
W przypadku, że dojdzie do zainfekowania **plików systemowych** usunięcie pliku, który używany jest do uruchomienia kluczowego programu, może spowodować błąd, przy następnym uruchomieniu pliku przez system. Jednakże, jeśli przesuńiesz go do Kwarantanny będzie w niej bezpieczny i nie będzie zagrażał komputerowi ani innym plikom znajdującym się w komputerze zobacz **strona 8**

Ustawienia zaawansowane

Ustawienie automatycznych aktualizacji

Każdy program antywirusowy jest tak efektywny jak efektywna jest jego baza wirusów, dlatego tak istotne jest pamiętanie o regularnych aktualizacjach program jak również bazy wirusów

Możesz dokonać wyboru, czy program oraz baza wirusów będą aktywowane automatycznie lub ręcznie lub śledząc ostrzeżenia, informujące o tym, że nowe aktualizacje programu avast! są dostępne. Aby zmienić status, możesz kliknąć na dotychczasowy status (tj. Bazy wirusów jedynie) na odtwarzaczu avast! lub po prostu otworzyć **opcje menu** (zobacz **strona 25**), Wybrać "Ustawienia programu", następnie "Aktualizacje (podstawowe)". Następnie wybierz odpowiedni status dla każdej z aktualizacji: bazy wirusów lub Programu (zobacz poniżej).



Kliknij "OK" a status odtwarzacza okna zostanie aktualizowany w następujący sposób:

- **WŁ**, jeśli opcja "Automatyczna" jest wybrana dla obu aktualizacji: bazy wirusów oraz programu
- **JEDYNIĘ PROGRAMU**, jeśli opcja "Automatyczna" jest wybrana dla programu
- **BAZA WIRUSÓW** opcja "Automatyczna" jest wybrana dla bazy wirusów
- **WYŁ.**, jeśli opcja "Automatyczna" jest wyłączona dla obu aktualizacji: bazy wirusów oraz programu

Aby dokonać aktualizacji **ręcznej**: bazy wirusów oraz programu wejdź w **opcje menu** (zobacz **strona 25**) i wybierz opcję "Aktualizuj".

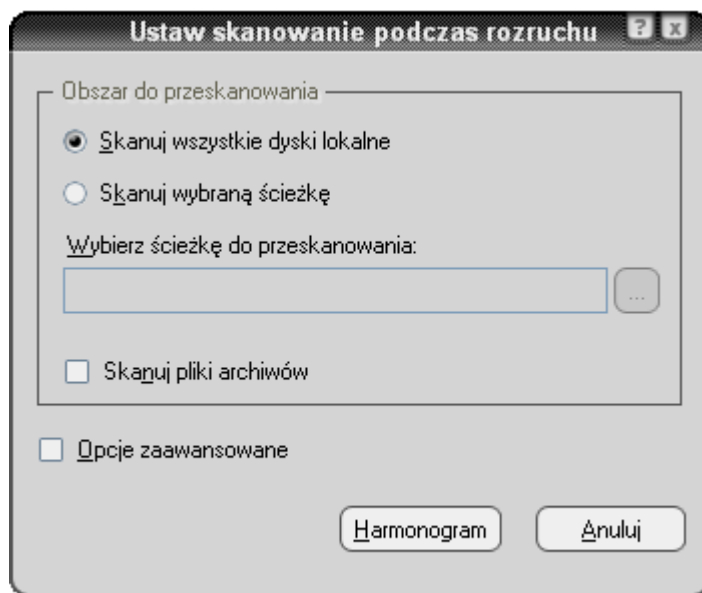
- Aby aktualizować bazę wirusów, wybierz **Aktualizacje iAVS**
- Aby aktualizować program, wybierz **Aktualizacje programu**

Jak ustawić Skanowanie podczas rozruchu?

(Dostępne jedynie dla wersji 32 bit Windows NT/2000/XP/Vista)

Możliwe jest ustawienie harmonogramu skanowania, które ma zostać przeprowadzone automatycznie po ponownym uruchomieniu komputera, tzn. kiedy przed uruchomieniem rzeczywistego czasu systemu operacyjnego. Jest to użyteczne ustawienie, jeśli podejrzewasz, że wirus został zainstalowany na komputerze, ponieważ pozwoli na wykrycie wirusów, które mogą być uruchomione wraz z systemem operacyjnym. W ten sposób nie dostaną one szansy wyrządzić żadnych szkód na komputerze.

Aby ustawić skanowanie podczas rozruchu, wejdź w **opcje menu** (zobacz **strona 25**) i kliknij na "Skanowanie podczas rozruchu". Pojawi się następujący obrazek:



Możesz wybrać, jeśli chcesz skanować cały dysk, lub jedynie wybrane obszary. Aby skanować jedynie wybrane obszary, kliknij "Skanuj wybraną ścieżkę" a następnie albo wpisz nazwę ścieżki w okienko, które się pojawi, lub kliknij na prawo od prostokątnego okna i wybierz obszar skanowania. Jak znajdziesz interesujący Cię obszar, kliknij na niego, a automatycznie pojawi się w on okienku.

Jeśli chcesz włączyć w obszar skanowania pliki archiwów, po prostu zaznacz tę opcję zaznaczając okienko "Skanuj pliki archiwów".

Zaznaczając "Opcje zaawansowane" możesz określić, jakie czynności powinny zostać wykonane w stosunku do zarażonych plików. Możesz wybrać z dostępnej listy:

- Usuń zarażone pliki
- Przesuń zarażone pliki
- Przesuń zarażone pliki do Kwarantanny
- Ignoruj zarażone pliki
- Napraw zarażone pliki

Wybierając "Przesuń zarażone pliki" spowodujesz, że podejrzane pliki zostaną przesunięte do folderu C:/Program Files\Alwil Software\Avast4\DATA\moved. Dodatkowo zostanie dodane przedłużenie ".vir" na koniec nazwy podejrzanego pliku, co zabezpieczy przed jego przypadkowym uruchomieniem i uszkodzeniem komputera.

Jeśli wybierzesz jedną z opcji: Usuń lub przenieś do zarażony plik, zostaniesz poproszony o potwierdzenie, czy rzeczywiście chcesz dokonać tej czynności z jakimkolwiek z zarażonych **plików systemowych**.

Pliki systemowe są wykorzystywane przez komputer do uruchamiania programów usuwanie i przenoszenie ich może doprowadzić do poważnych konsekwencji. Dlatego zostaniesz zapytany o potwierdzenie czynności:

- Zezwól na usunięcie
- Nie usuwaj i nie przesuwasz plików systemowych

Pozwoli uniknąć wszelkich potencjalnych problemów operacyjnych, jednak komputer będzie nadal potencjalnie zagrożony zakażeniem. Jest zalecane przeniesienie wszystkich podejrzanych plików do Kwarantanny, gdzie pozostają bezpieczne i gdzie można z nimi pracować. Po przeniesieniu do Kwarantanny, wirusy nie mogą spowodować uszkodzenia innych plików. Następnie można uporać się z uszkodzonymi plikami, tak jak zostało opisane na **stronie 48** np. mogą one zostać usunięte, jeśli jesteś pewien, że jest to bezpieczne można je przenieść z powrotem do ich pierwotnej lokalizacji, lub po prostu mogą one być przechowywane w Kwarantannie, aż do zdecydowania, co z nimi zrobić.

Po tym, jak potwierdzisz, co należy zrobić ze wszystkimi zainfekowanymi plikami kliknij na przycisk "Tabela", a pojawi się następujący komunikat:



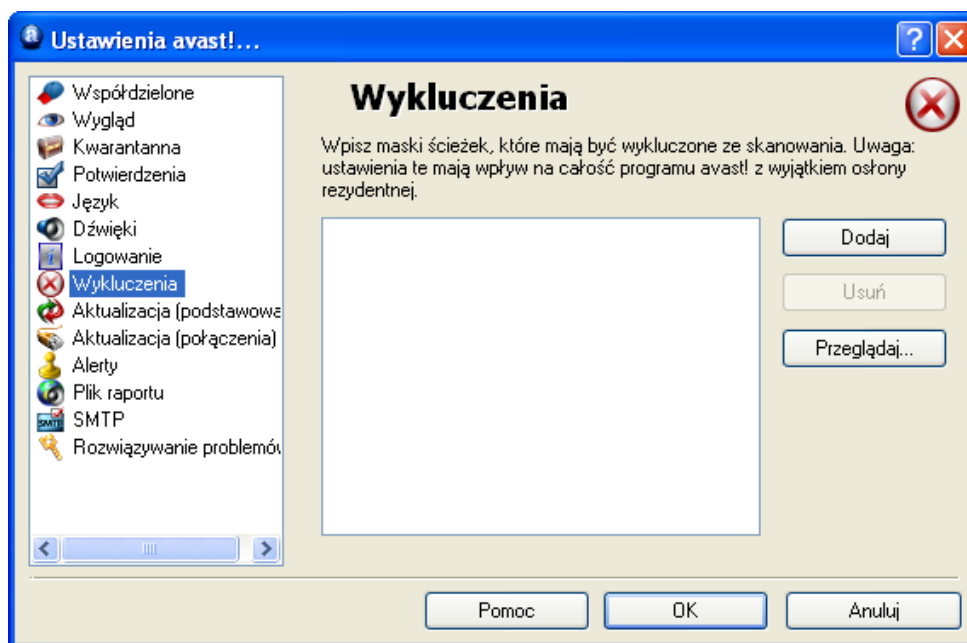
Kliknij "Tak", aby restartować komputer i wybierz Skanowanie podczas rozruchu lub kliknij Nie, a skan zostanie automatycznie uruchomiony po kolejnym restarcie komputera.

Wykluczanie ze skanowania

Istnieje możliwość wykluczenia pewnych plików z testowania, co oznacza, że nie będą one skanowane przed wirusami. Może to być użyteczne w kilku przypadkach:

- **Aby uniknąć tzw. fałszywych alarmów.** Jeśli program zgłasza, że znalazł wirusa, wskazując na plik, o którym jesteś pewien, że nie jest zagrożony, oznacza to fałszywy alarm. Możesz ten plik wykluczyć ze skanowania. Prosimy o poinformowanie działu wsparcia technicznego o takich fałszywych alarmach, a problem zostanie rozwiązany.
- **Aby ustawić proces.** Jeśli folder zapisany na twardym dysku zawiera jedynie obrazki, możesz ten plik dodatkowo wykluczyć ze skanowania, co zredukuje czas skanowania.

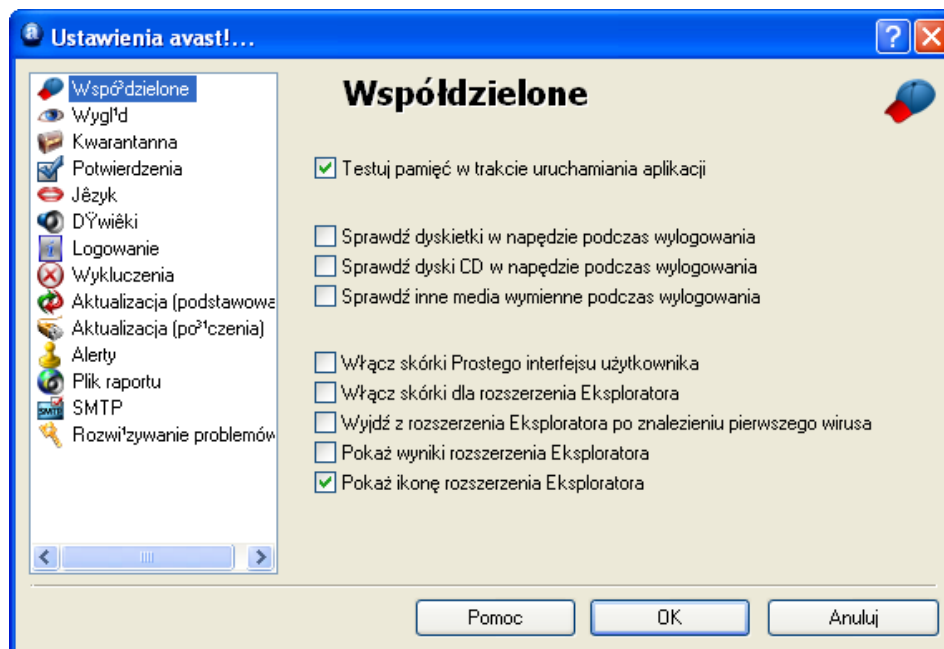
Pamiętaj, że wykluczanie ma wpływ na skanowanie w przyszłości, za wyjątkiem ochrony dostępowej. Aby dokonać wyłączenia określonych plików, wystarczy po prostu kliknąć na „Ustawienia” z **opcji menu** (zobacz **strona 25**), następnie na „Wykluczenia” pojawi się poniższy obrazek:



Aby wykluczyć plik lub folder, kliknij na Przeglądaj a następnie zaznacz folder lub plik, który ma zostać wykluczony. Ewentualnie kliknij na „Dodaj” i ręcznie wpisz lokalizację odpowiedniego pliku lub folderu w okno Wykluczenia. Jeśli chcesz dokonać wykluczenia folderu, łącznie z jego podziorami konieczne jest dodanie „*” na końcu nazwy folderu np. C:\Windows*. Aby usunąć folder lub plik z wykluczeń, kliknij na niego ponownie, podkreśl go i kliknij „Usuń”

Jak stworzyć raport ze skanowania?

Istnieje możliwość stworzenia trwałego raportu ze skanowania, każdego skanowania. Raport ten możesz później prześledzić. Aby stworzyć raport, wejdź w **opcje menu** jak zostało opisane na **strona 25** i wybierz "Ustawienia". Następnie kliknij na "Raporty" i następnym oknie, zaznacz "Stwórz plik raportu" tak jak jest to zaprezentowany poniżej.



Jeśli chcesz stworzyć nowy raport po każdym skanowaniu, a jednocześnie nie chcesz zapisywać wcześniejszych, zaznacz opcję "Napisz istniejący". Jeśli okno to nie jest zaznaczone, wyniki każdego skanowania zostaną dodane do poprzedniego raportu.

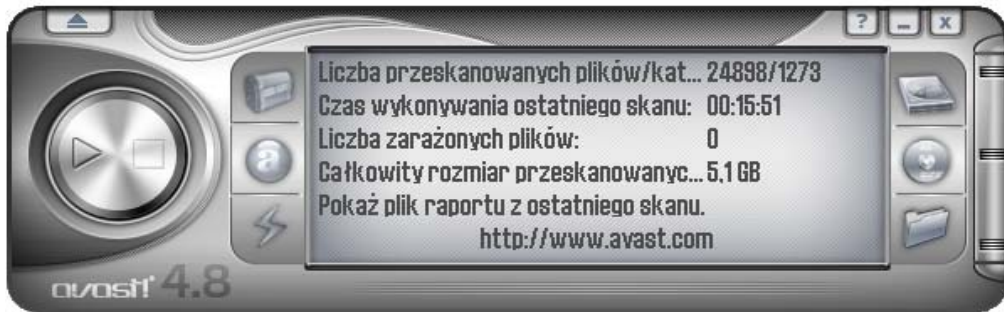
Możesz również dokonać wyboru gdzie chcesz zapisywać pliki raportu – w standardowym folderze programu, gdzie program automatycznie umieści raport, albo wybrać inną lokalizację klikając na "Utwórz plik raportu" i wpisz lokalizację folderu.

Następnie, określ, które informacje powinny zostać zawarte w raporcie:

- Zadanie start – data i czas skanowania zostaną uruchomione
- Zadanie stop – data i czas skanowania zostały zakończone
- Pliki OK – pliki, które zostały poddane skanowaniu, bez wykrycia podejrzanych elementów. Jeśli wszystkie pliki lokalne zostały poddane skanowaniu, zaznaczając to okno, wytworzysz bardzo długi raport, najprawdopodobniej składający się z kilku tysięcy wierszy. Dlatego zalecamy zaznaczyć tę opcję, jedynie w przypadku, kiedy zamierzasz przeprowadzić ograniczone skanowanie i jeśli chcesz uzyskać dokładny raport dotyczący problematycznego obszaru.
- Poważne błędy – pojawią się, w chwili, kiedy program wykryje coś, czego normalnie nie wykrywa. Tego typu błędy wymagają dalszego zbadania.
- Drobne błędy – należą do mniej problematycznych niż tzw. Błędy poważne i najczęściej odnoszą się do plików, które nie zostały poddane skanowaniu, ponieważ były używane podczas skanowania

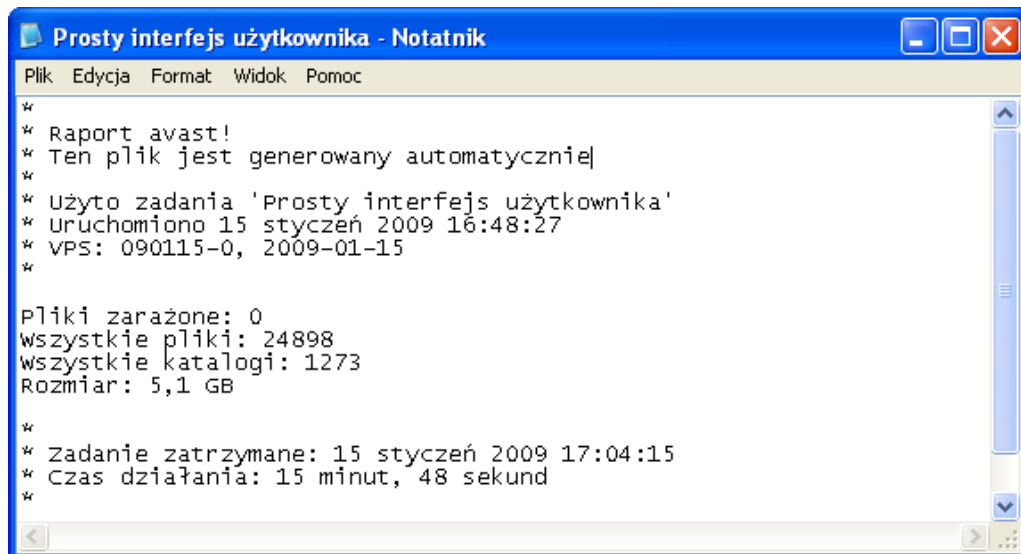
- Pliki pominięte – to pliki, które nie zostały objęte skanowaniem. Na przykład szybki skan skanuje pliki rozszerzone, bez ich przedłużeń. Pliki, które posiadają rozszerzenie nie są traktowane jako niebezpieczne, dlatego nie są skanowane. Wszelkie pliki wyłączone ze skanowanie zostaną wykryte w tym raporcie.
- Pliki zarażone – to pliki, które potencjalnie zawierają wirusa

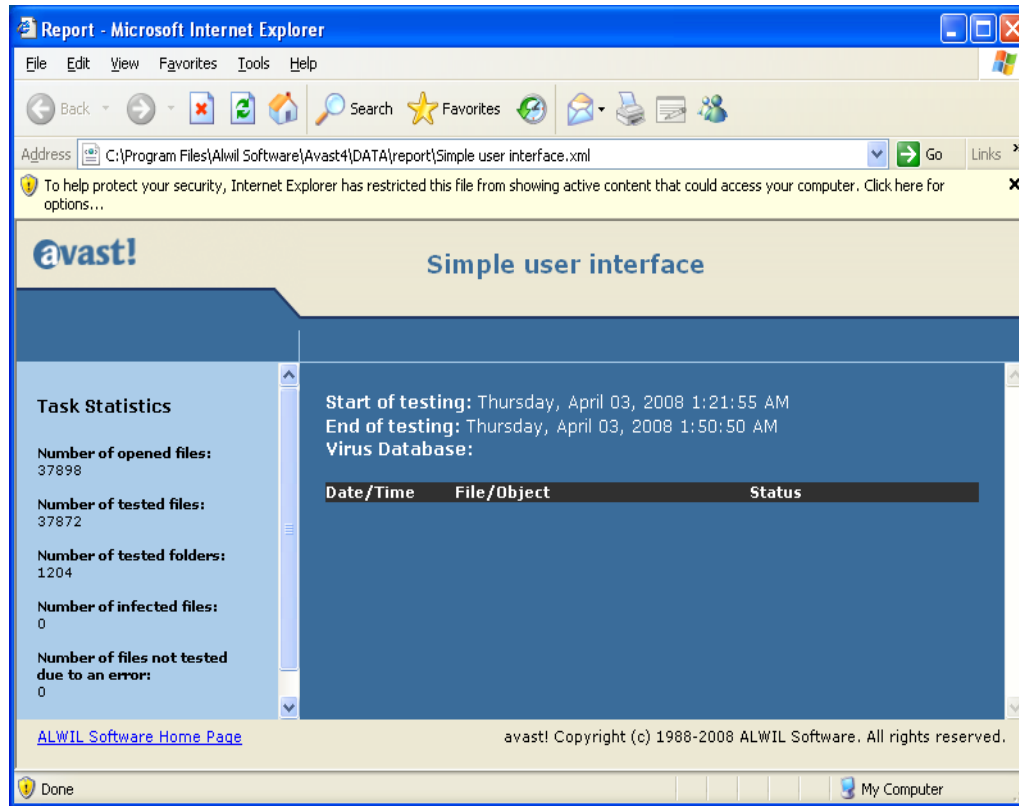
Wreszcie możesz określić, jeśli raport powinien być w formie pliku tekstowego lub pliku XML. Po uruchomieniu skanowania, pojawi się nowy wiersz w oknie statusu informacji– “Pokaż plik raportu z statusu skanowania” jak zostało pokazane poniżej.



Klikając na “Pokaż plik raportu statusu skanowania” wyniki skanowania pojawią się w specjalnym, wybranym formacie. Ewentualnie otwórz **opcje menu** (zobacz **strona 25**) i zaznacz “Pokaż raporty ze skanowania”

Raport w formacie tekstu:



Raport w formacie XML:

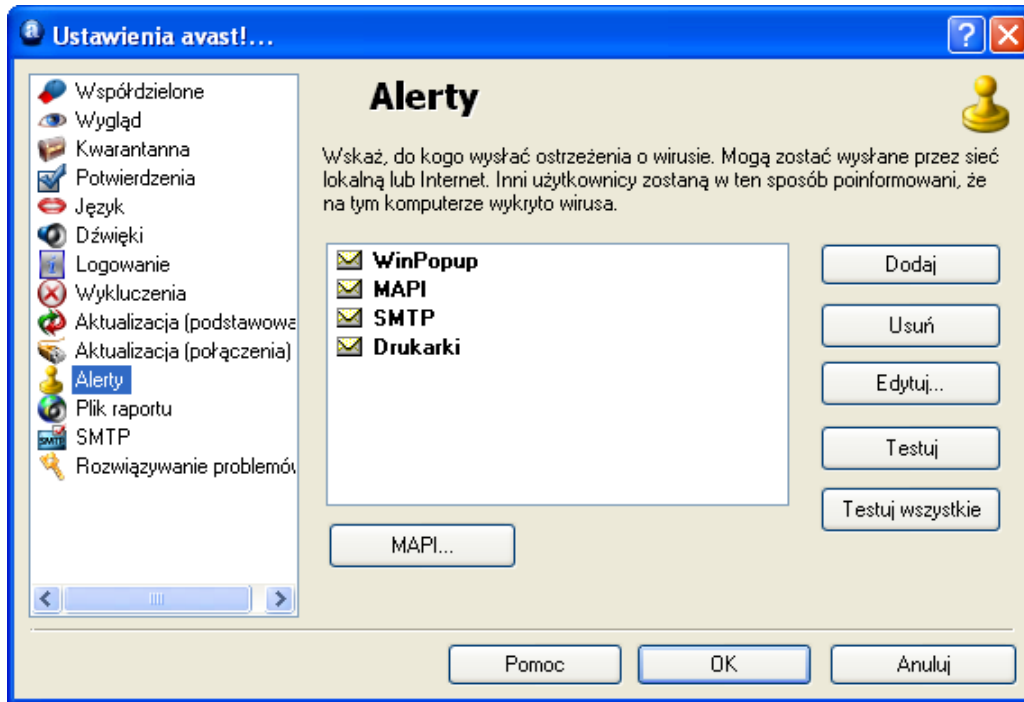
Raporty z poprzedniego skanowania są przechowywane w standardowym folderze programu lub w niestandardowych, określonych przy tworzeniu raportu folderach - patrz poprzednia strona.

Jeśli nie chcesz wytworzyć żadnego dalszego raportu wybierz "Nadpisz istniejący", będziesz miał także możliwość, aby zobaczyć poprzednie raporty za każdym razem, gdy chcesz wejść w podgląd raportu po uruchomieniu nowego skanowania.

Jeśli nie potrzebujesz zapisywać wszelkich następných sprawozdań, które mają być utworzone, wystarczy przejść do opcji „Plik raportu” w **opcji menu** (zobacz **strona 25**) i odznaczyć opcję "Utwórz plik raportu".

Alerty

avast! potrafi wysłać ostrzeżenie dotyczące pojawienia się wirusa. Wybierz “Ustawienia” w **opcji menu**, a następnie “Alerty”. Ustawienie to jest korzystne dla administratora, które zostanie poinformowany o obecności wirusów na którymkolwiek z komputerów w sieci. Pozwoli to na szybką reakcję.



Wszystkie alerty mogą zostać przesłane w następującym formacie:

- WinPopup.**
 Kliknij na “Dodaj” i wybierz WinPopup. Następnie wpisz IP adres lub nazwę sieci komputerowej, które mają być monitorowane i z których mają zostać wysłane ostrzeżenia lub kliknij „Przeglądaj” i wybierz adres z dostępnej listy.
- MAPI.**
 Ostrzeżenie zostanie wysłane drogą mailową, przy użyciu protokołu MAPI. Wpisz adres alerty sieciowego, kliknij na przycisk MAPI na dole ekranu i wpisz nazwę profilu MAPI oraz ważne hasło
- SMTP.**
 Ostrzeżenie zostanie wysłane maile, przy użyciu protokołu SMTP. W oknie, które się pojawi, wpisz adres emaliowy osoby, której chcesz wysyłać ostrzeżenia. Konieczne jest również określenie pozostałych ustawień – zobacz następną sekcja “SMTP”.
- Drukarki**
 Ostrzeżenie zostanie wysłane do specjalnej drukarki. Kliknij na “Dodaj” i na “Drukarka”, a następnie kliknij “Przydaj” oraz wybierz drukarkę z dostępnych opcji.

Aby wytworzyć nowe ostrzeżenie, kliknij na "Dodaj" i wybierz typ wymaganego ostrzeżenia, a następnie wpisz wymagane szczegóły, jak zostało opisane poniżej. Po wykryciu podejrzanego pliku ostrzeżenie zostanie stworzone, a wiadomość zostanie wysłana określönemu odbiorcy.

Aby edytować ostrzeżenie, które zostało stworzone, kliknij na nie, pokreśl, a następnie kliknij "Edytuj" lub "Usuń".

Klikając na "Testuj" prześlesz wiadomość na określony adres, podczas gdy klikając na "Testuj wszystko" wyślesz alerty, wszystkim odbiorcom znajdującym się na liście.

SMTP

Klikając na SMTP na liście po lewej stronie ekranu, możesz określić parametry swojego SMTP serwera. avast! wykorzystuje te ustawienia, aby wysłać wiadomość e-mailem, szczególnie, jeśli:

- Przesyła wiadomość ostrzeżenie (Alerty) po wykryciu wirusa
- Przesyła pliki z Kwarantanny do ALWIL Software.
- Przesyła nieudane raporty avast! do ALWIL Software.

Powinieneś wpisać następujące informacje:

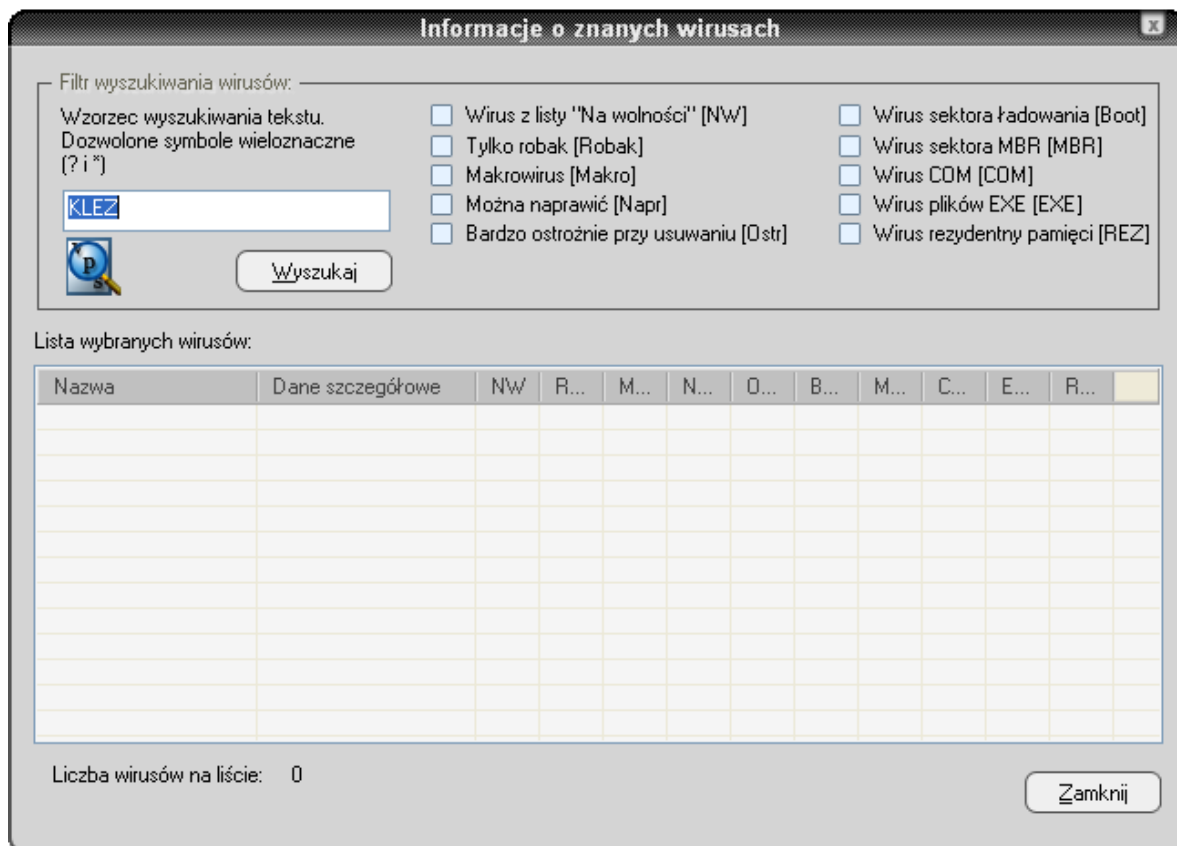
- Adres serwera – adres serwera maili wychodzących (np. smtp.server.com lub 192.168.1.25).
- Port - numer port (domyślny 25).
- Z adresu – adres nadawcy ("Z").

Jeżeli serwer SMTP wymaga uwierzytelniania podczas logowania, należy również zaznaczyć okienko i wprowadzić nazwę użytkownika wraz z hasłem.

Szukanie wirusów w bazie danych

Baza wirusów zawiera szczegółowe informacje dotyczące wszystkich wirusów oraz jest wykorzystywana przez program w celu zidentyfikowania potencjalnych infekcji.

Aby uzyskać dostęp do bazy danych wirusów, otwórz **opcje menu** (zobacz **strona 25**) i kliknij na "Baza wirusów". Pojawi się następujący ekran:



Wirusy można odnaleźć według różnych parametrów. Jeśli znasz nazwę wirusa, po prostu wpisz ją w okienko i kliknij na przycisk „Wyszukaj”. Jeśli znasz jedynie część nazwy wpisz „?” w miejsce nieznanymi liter (bądź cyfr) lub „*” w miejsce kilku nieznanymi liter.

Przykład: Przypuśćmy, że szukasz wirusa "Klez". Jest to rzeczywista nazwa w bazie danych Win32:Klez-H [Wrm]. Powinieneś wpisać: *Klez*. Zostaną odnalezione wszystkie wirusy zawierające słowo "Klez".

Aby zawęzić wyszukiwanie, można również zaznaczyć okienko obok każdego typu wirusa. Aby wyszukać specjalny typ wirusa, zaznacz okienko, klikając na nie dwukrotnie. Kliknięcie na dowolne okienko raz, tak, aby zobaczyć zmiany okienka oznacza, że nie posiadają tej funkcji. Jeżeli którykolwiek pole nie jest zaznaczone, jest niebieskie lub zielone, oznacza to, że nie ma znaczenia, czy istnieje taki typ wirusa czy nie.

Możliwe typy wirusów do wyszukania:

- ***Lista wirusów na wolności (ITW...)***

Wirus znajduje się na liście wirusów na wolności, szerzonych pomiędzy użytkownikami na całym świecie.

- ***Jedynie robaki (Worm)***

To potencjalny typ wirusa, który nie zaraża bezpośrednio, ale wykonuje inne niepożądane działania, jak na przykład rozszerza się drogą mailową, kradnie hasła itp.

- ***Makrowirus (Macro)***

Ten typ wirusa wykorzystuje przede wszystkim język makrowirusa, przede wszystkim produktów Microsoft (np. Word, Excel).

- ***Może zostać naprawiony (Rep)***

Odnaleziony, zarażony plik, może zostać naprawiony przez program avast! oraz odnowiony do pierwotnego stanu.

- ***Bardzo ostrożnie przy usuwaniu (Care)***

Jest niezwykle istotne, aby zachować wszelkie środki ostrożności, podczas usuwania wirusów (w innym przypadku może dojść do wielkich szkód, spowodowanych przez wirusa!).

- ***Wirus sektora ładowania (Boot)***

Typ wirusa, które zaraża sektor ładowania dysku twardego lub dyskietki

- ***Wirus sektora MBR (MBR)***

Typ wirusa, które zaraża główny sektor ładowania dysku twardego

- ***Wirus COM (Com)***

Typ wirusa, który zaraża pliki wykonywalne, z końcówką ".com".

- ***Wirus EXE (Exe)***

Typ wirusa, który zaraża pliki wykonywalne, z końcówką ".exe".

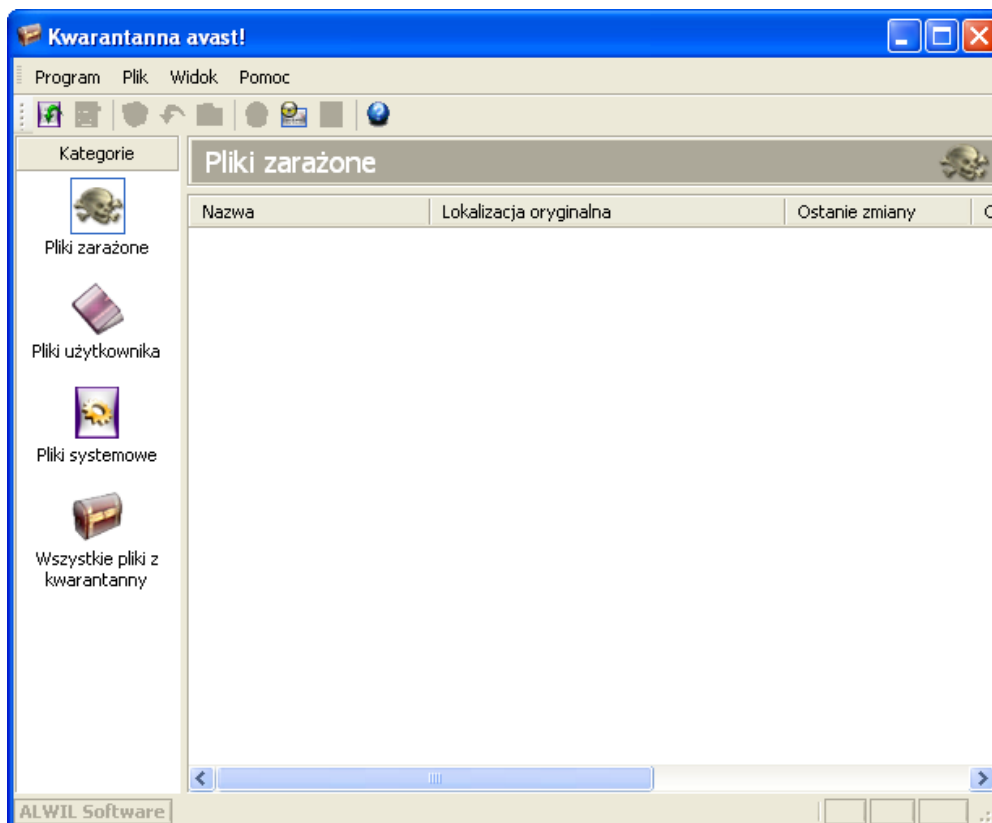
- ***Wirus rezydentalny pamięci (Res)***

Typ wirusów, które pozostają w pamięci RAM i zarażają komputer, kiedy zostanie uruchomiony.

Praca z plikami w Kwarantannie

Wirus w Kwarantannie może być dostępny bezpośrednio z **opcji menu**. Dzięki specyficznym właściwościom tego pliku wirusy pozostają w izolacji w Kwarantannie. Kwarantanna może, więc być wykorzystana do następujących celów:

- Przechowywanie wirusów.**
Jeśli avast! znajdzie wirus, a z jakiś powodów nie zdecydujesz się go usunąć, zostanie Ci zaoferowana opcja przesunięcia go do Kwarantanny. Przechowując wirusy w kwarantannie możesz być pewnie, że nie zostanie on uruchomiony przez pomyłkę.
- Przechowywanie podejrzanych plików.**
Kwarantanna jest odpowiednim miejscem do przechowywania podejrzanych plików w celu ich późniejszego analizowania.
- Tworzenie kopii zapasowych plików systemowych.**
Podczas instalacji, kopie niektórych krytycznych plików systemu są przechowywane w Kwarantannie w folderze "Pliki systemowe" (patrz poniżej). Jeśli główny plik systemowy zostanie zainfekowany przez wirusa, kopie mogą zostać przywrócone z Kwarantanny do ich pierwotnej lokalizacji.



Kliknięcie prawym przyciskiem myszy na dowolny plik otworzy następujące opcje. Ewentualnie kliknij lewym przyciskiem myszy na plik, tak, aby go zaznaczyć, następnie kliknij

na odpowiednią ikonę na górze ekranu lub kliknij na "Plik" i wybierz pożądaną opcję (*UWAGA: Po dwukrotnym kliknięciu pliku, nie uruchomisz go, ale wyświetlisz jego właściwości. Jest to środek bezpieczeństwa w celu zabezpieczenia przed przypadkowym od zakażenia w obrębie Kwarantanny*):

- **Przywróć wszystkie pliki**
Wybierz tę opcję, jeśli chcesz się upewnić, że masz przed sobą pełną listę plików. Program odświeży listę automatycznie, niemniej, jeśli nie chcesz czekać na automatyczne przywrócenie, możesz skorzystać z tej opcji.
- **Dodaj pliki**
Możesz dodać plik jedynie do kategorii "Pliki użytkownika"
- **Usuń plik**
Wybierając tę opcję, plik zostanie bezzwrotnie usunięty, to jest pliki nie zostaną po prostu przesunięte do kosza. Przed usunięciem jakiegokolwiek pliku upewnij się, że nie jest to plik systemowy. Usunięcie pliku systemowego może spowodować poważne konsekwencje.
- **Przywracanie plików**
Plik zostanie przywrócony do swojej pierwotnej pozycji i tym samym usunięty z Kwarantanny.
- **Skrót do pliku**
Plik zostanie skopiowany do wybranego folderu.
- **Skanuj plik**
Plik zostanie poddany skanowaniu w poszukiwaniu wirusów.
- **Pokaż właściwości pliku**
Właściwości pliku zostaną wyświetlone. Możliwe jest dodanie komentarza do pliku.
- **Wyślij e-mail do ALWIL Software.**
Wybrany plik zostanie przesłany (e-mailem) do ALWIL Software. Z opcji tej powinieneś skorzystać jedynie w specjalnych okolicznościach np., jeśli podejrzewasz, że program nie prawidłowo zidentyfikował wirusa. Nie zapomnij zawrzeć jak najwięcej informacji dotyczących przesyłanego pliku, aktualnej wersji bazy wirusów, która jest na twoim komputerze itp. Pomożesz nam w ten sposób ulepszyć nasze usługi.

Klikając na Program i "Ustawienia" a następnie na "Kwarantannę" możesz ustawić Maksymalny rozmiar Kwarantanny i ustawić wielkość, jaką Kwarantanna zajmuje w Twoim komputerze. Możesz określić maksymalną wielkość poszczególnych plików, które powinny zostać przesunięte do Kwarantanny.

Log podglądu

Po zakończeniu każdego skanowania program antywirusowy avast! tworzy kilka plików logów, zawierających informacje o błędach lub podejrzanym plikach wykrytych przez avast! Informacje o instalacji oraz aktualizacjach programu oraz bazy wirusów zostaną tutaj również odnalezione. Aby obejrzeć logi, wystarczy wybrać "Pokaż logi w **opcji menu** (zobacz **strona 25**).

Informacje zapisane w plikach logów są rozdzielone do następujących kategorii:

Informacje	Jedynie informacja, wszystko jest OK.
Uwaga	Ważna informacja, wszystko jest OK. Zawiera informacje oraz aktualizacje bazy danych.
Ostrzeżenie	Pojawił się błąd lub został odnaleziony wirus, ale program może naprawić problem.
Błąd	Pojawił się błąd, program nie działa.
Błąd krytyczny	Krytyczny błąd programu, program zostanie zatrzymany.
Alert	Komputer jest potencjalnie zagrożony
Niebezpieczeństwo	Zagrożenie całego komputera (bezpieczeństwo, usuwanie plików systemowych).

Klikając na „Ustawienia” a następnie na „Logowanie”, możesz ustawić maksymalny rozmiar logu.

W Podglądzie logów, możliwe jest wyszukiwanie konkretnych zapisów, w celu filtrowania rekordów według określonych kryteriów, lub do wywozu do ewidencji lokalizacji.

Znajdź zapis

1. Przyciśnij jednocześnie przyciski "CTRL" i "F" lub
2. Kliknij "Edytuj" w lewym górnym rogu ekranu, a później na "Znajdź" lub
3. Kliknij na lupę w lewym górnym rogu ekranu, lub
4. Kliknij prawym przyciskiem myszy na listę, a następnie kliknij przycisk "Filtruj" w menu

W wyświetlające się pole można wpisać wszystkie lub część nazwy zapisu, który chcesz odnaleźć. Jeśli nie znasz dokładnej nazwy, zaznaczając pole "Dopasuj tylko całe słowa" zapewni tylko wyszukiwanie według ściśle określonych kryteriów. Podobnie się dzieje, jeśli chcesz wyszukać jedynie zapisy przy użyciu wielkich lub małych liter, zaznacz pole "Dopasuj". Klikając przycisk "Do góry" lub "w dół" ustalisz, czy zapisy są wymienione w porządku rosnącym lub malejącym.

Następnie kliknij przycisk "Znajdź następny". Pierwsza płyta zostanie wyświetlona. Wszelkie inne zapisy, które pasują do podanych kryteriów można znaleźć klikając "Znajdź następny", dopóki nie uzyskasz informacji, że zostały odnalezione wszelkie zapisy.

Filtruj listę zapisów. Filtr może być wykorzystywany w celu zawężenia długiej listy zapisów oraz aby wyniki wyszukiwań spełniały konkretne kryteria, np. specyficzne słowo kluczowe lub część słowa.

1. Przyciśnij jednocześnie przyciski "CTRL" i "F" lub
2. Kliknij "Edytuj" w lewym górnym rogu ekranu, a później na "Znajdź" lub
3. Kliknij na żółty kliknij na żółte ścieżki w lewym górnym rogu lub
4. Kliknij prawym przyciskiem na listę zapisów, a następnie kliknij na "Filtruj" w menu.

Pojawi się następnie okno, w którym możesz specyfikować swoje kryteria.

Włącz

Wpisz kluczowe słowo lub części słowa, które powinny być zawarte w zapisach, które chcesz, aby zostały wyświetlone. Można używać symboli wieloznacznych tzn. można wpisać * w miejsce liter, których nie znasz. Wiele słów kluczowych, musi być oddzielone średnikami (;).

Wyklucz

Wpisz kluczowe słowo, albo część słowa, które nie koniecznie musi pojawiać się w rejestrze.

Zakres czasowy

Tutaj możesz określić początek i koniec okresu, dla którego chcesz, aby zostały wyświetlone zapisy.

Wybierz zdefiniowane wiersze

Jeśli wybrałeś tę opcję, zapisy muszą pasować do kryteriów podkreślonych

Pokaż jedynie zdefiniowane wiersze (ukryj resztę)

Jeśli ta opcja jest zaznaczona, tylko zapisy dokładnie pasujące do określonych kryteriów będą wyświetlane. Inne zapisy będą nie będą widoczne. Jest to przydatne, jeśli oryginalna lista jest bardzo długa.

Sortuj zapisy

Klikając na jakąkolwiek z nagłówek kolumn sortujesz zapisy w porządku rosnącym lub malejącym według kryteriów ustawionych w tej kolumnie. Klikając nagłówek kolumny powrócisz do listy pierwotnej kolejności.

Eksportuj zapisy

Znalezione lub wyselekcjonowane zapisy, lub całą listę zapisów można eksportować i zapisać jako nowy plik. Aby znaleźć lub eksportować wyselekcjonowane zapisy, wybierz opcję "Eksportuj wybrane wiersze" lub kliknij na zieloną strzałkę w lewym górnym rogu ekranu. Aby wyeksportować całą listę, wybierz polecenie "Eksportuj bieżącą listę" lub kliknij na zieloną strzałkę w prawo. W nowo wyświetlonym oknie, wybierz folder docelowy dla eksportowanego pliku, a następnie wpisz nową nazwę pliku, a następnie kliknąć przycisk "Zapisz".

Konfiguracja osłony dostępowej

1. Komunikatory

Programy

Możesz tutaj określić, które z plików iM programów (tzw. Komunikatorów) powinny być skanowane. Jeśli korzystasz z Windows 95/98/ME i chcesz chronić programy przed trojanami, musisz wpisać ścieżkę pliku konfiguracyjnego, talk.ini (w tym celu możesz skorzystać z przycisku Przeglądaj). Niektóre z programów są chronione jedynie jeśli korzystasz z Windows NT, 2000, XP, 2003, Vista lub 2008.

2. Poczta

Na stronach "POP", "SMTP", "iMAP" oraz "NNTP" możesz określić czy chcesz aby poczta oraz wiadomości przychodzące i/lub wychodzące powinny być skanowane. Jeśli wirus został wykryty, zostanie wysłana odpowiednia wiadomość. Możesz również określić, co zostanie włączone w pustą wiadomość o tym, że e-maile nie zawierają żadnego wirusa.

Przekierowywanie

Strona ta pozwala na ustawienie transparentnego skanowania e-maili. Każdy e-mail, który przejdzie przez określony port zostanie poddany skanowaniu przed wirusami. Ustawienie to jest dostępne jedynie dla systemów operacyjnych opartych o NT (Windows NT/2000/XP/2003/Vista/2008).

- Przekierowywanie portów.

Porty domyślne to standardowe porty, określone przez cztery podstawowe protokoły mailowe e-mail: jeśli korzystasz z innego portu (lub portów) powinny zostać tutaj wpisane. Nazwa wielocłonowa powinna zostać oddzielone przecinkiem.

- Ignorowanie adresów.

W tym miejscu możesz wpisać adresy serwerów mailowych lub określonych portów które chcesz wykluczyć ze skanowania. Ustawienie to może być użyteczne jeśli chcesz aby avast! skanował jedynie wiadomości z lub do określonych kont (wtedy avast! będzie ignorować resztę wiadomości). Na przykład, jeśli wpiszesz **smtp.server.com**, avast! nie będzie skanował wiadomości wychodzących (SMTP) wysyłanych na ten adres.

- Ignoruj komunikację lokalną.

Opcja ta powinna zostać zaznaczona. Jeśli jest odznaczona, avast! będzie skanował również komunikację lokalną (która zazwyczaj jest bezpieczna), co może spowodować nieznaczne spowolnienie w działaniu komputera. Uwaga: Nie wpisuj żadnego numeru portu niż tego, którego w rzeczywistości używasz do przesyłania poczty. Może to spowodować nieoczekiwane komplikacje.

Zaawansowane

- Pokaż szczegółowe informacje dotyczące wykonywanej akcji.

Jeśli okienko to jest zaznaczone, informacje dotyczące plików, które są momentalnie testowane, zostaną wyświetlone w prawym górnym rogu ekranu.

- Praca w tle

Jeśli akcja określona na stronie wirus jest zaznaczona jako akcja domyślna to jest ona ustawiona jako opcja interaktywna i równocześnie został wybrany tryb cichy, jakkolwiek działania wobec zainfekowanego pliku zostaną podjęte na podstawie poniższych zasad:

- Jeśli została wybrana opcja "z ogólnym założeniem odpowiedzi Tak (OK)", jakkolwiek zainfekowany plik znajdujący się w załączniku e-maila, zostanie automatycznie usunięty.
- Jeśli została zaznaczona druga opcja "z ogólnym założeniem odpowiedzi Nie (Anuluj)" jakiegokolwiek zainfekowane pliki zostaną przesunięte do Kwarantanny.
- Jeśli akcja określona na stronie wirus została ustawiona jako akcja domyślna a pole znajdujące się na lewo jest odznaczone, normalne okno ostrzeżenie o wirusie, zostanie wyświetlone, wraz z zapytaniem, co chcesz zrobić z zainfekowanym plikiem.

Jeśli została określona jakakolwiek inna akcja, na przykład jakakolwiek inna akcja niż domyślna opcja interaktywna, zaznaczenie tego pola nie przyniesie żadnego efektu.

Uwaga, Jednakże jeśli inna akcja, niż domyślna została określona dla Ostrzeżenia standardowej, będzie to miało wpływ na akcję określoną dla dostawcy poczty!

- Czas oczekiwania na komunikację (s).

Czas określony jest w sekundach, wyznacza czas oczekiwania na odpowiedź serwera. Możesz dodatkowo określić czy połączenie powinno zostać zamknięte, jeśli nie została dostarczona odpowiedź w ciągu wyznaczonego czasu lub czy powinien zapytać co dalej.

- Pokaż ikonę w polu systemowym w czasie odsyłania poczty

Jeśli pole to zostało zaznaczone, pojawi się mała ikona w pasku systemowym, w prawym dolnym rogu ekranu komputera, aby pokazać postępy skanowania.

Heurystyka

avast! Potrafi nie tylko skanować przychodzącą pocztę w poszukiwaniu wirusów, ale umie również sprawdzać pocztę, przy użyciu analizy heurystycznej, w poszukiwaniu potencjalnych wirusów, niewystępujących jeszcze w bazie wirusów. W tym oknie możesz dokonać zmian w analizie heurystycznej.

- Czulość - Niska.
 - Sprawdzanie załączników.

Załączniki są sprawdzane w oparciu o ich nazwy oraz w oparciu o to, czy nazwa załącznika posiada rozszerzenie, np. "Patch.jpg.exe", będzie traktowana jako potencjalne zagrożenie. avast! dodatkowo sprawdzi czy rozszerzenie załącznika koresponduje z rzeczywistym typem pliku, np. Czy plik "Pamela.jpg" to obrazek, jak należałoby oczekiwać, lub plik COM ze zmienioną nazwą.
 - Sprawdzanie sekwencji białych znaków.

Niektóre wirusy w ciągu sekundy dodają pewną ilość spacji (lub innych niewyświetlających się "białych" znaków) na końcu, do prawdziwego rozszerzenia pliku, co jest niebezpieczne. Na podstawie długości nazwy pliku, użytkownik może nie zauważyć drugiego rozszerzenia, jednakże analiza heurystyczna umożliwia dostrzeżenie tego triku. Domyślna ilość zezwoleń sekwencji białych znaków to pięć. Jeśli jest ich więcej niż pięć, pojawi się wiadomość z ostrzeżeniem.
- Czulość – Średnia (w porównaniu do powyższej).
 - Gruntowne sprawdzanie załączników.

Tak jak podstawowe sprawdzanie zawartości załączników, ostrzeżenie zostanie również wyświetlone, jeśli załącznik zawiera proste rozszerzenie wykonywalne (EXE, COM, BAT etc.). Uwaga, wszystkie tego typu pliki są niebezpieczne a poziom czulość, będzie w związku z tym generowany jako raczej jako fałszywy alarm, w porównaniu do podstawowego sprawdzania załączników.
- Czulość - Wysoka (w porównaniu w powyższą)
 - Sprawdzanie elementów HTML.

Niektóre wirusy mogą rozprzestrzeniać robaki w określonych programach pocztowych (szczególnie w przypadku niezabezpieczonego programu MS Outlook czy Outlook Express) oraz pozwalają uruchomić wirus, poprzez oglądanie wiadomości w podglądzie. avast! kontroluje, czy kod HTML wiadomości zawiera wirus uniemożliwiający tego typu trik. Jeśli tak jest, pojawi się wiadomość ostrzegająca przed tym

- Wiadomości wychodzące - Test ilości wysłanych (czas).
Większość wirusów rozprzestrzenia się przy pomocy maila oraz przesyłając się na adresy zapisane w książce adresowej Windows. W bardzo krótkim czasie, wiadomość zostaje wysłana do ogromnej ilości adresatów, z tym samym tytułem i/lub załącznikiem. avast! Monitoruje ilość wiadomości w określonym czasie oraz sprawdza tytuł oraz załączniki. Parametry te mogą być również określone w zakładce Heurystyka (Zaawansowane).
- Wiadomości wychodzące - Wysyłka masowa.
Wirusy mogą być również rozprzestrzeniane poprzez wysyłanie ich jako jednej wiadomości do wielu odbiorców. Dlatego avast! monitoruje liczbę absolutną odbiorców wiadomości. Dozwołoną ilość absolutną odbiorców można określić w zakładce Heurystyka (Zaawansowane).

- Czułość - Własna

Klikając na "Dostosuj" możesz określić które z powyższych komponentów analizy heurystycznej powinny zostać zastosowane.

Dodatkowo możesz wybrać "Sprawdzanie struktury tematów". Jeśli opcja ta jest zaznaczona, nagłówek tematu maili zostanie sprawdzony w poszukiwaniu dużej ilości nieesencjonalnych znaków, np., jeśli temat zawiera sekwencje "<?*&\$^(^%#\$\$*_)", pojawi się wiadomość z ostrzeżeniem.

- Dozwołone adresy URL

Klikając na "Dozwołone adresy URL", możesz zdefiniować bezpieczne adresy URL, które nie zostaną poddane analizie heurystycznej. Aby dodać adres URL, kliknij "Dodaj" a następnie ręcznie wpisz nazwę adresu URL. Aby usunąć URL, kliknij na niego raz i zaznacz go, a następnie kliknij na "Usuń"

- Praca w tle

W tej zakładce możesz również określić, jakie działania powinny zostać podjęte w stosunku do zarażonego pliku po pojawieniu się ostrzeżenia o jego wykryciu.

Heurystyka (Zaawansowana)

Strona ta umożliwia modyfikowanie ustawień analizy heurystycznej dla poczty wychodzącej. Ustawienia są wykorzystywane, jedynie, jeśli czułość "Heurystyki" ustawiona jest jako Wysoka lub Własna (a mogą zostać zmienione jedynie, jeśli jest ustawiona czułość Własna).

- Sprawdzany okres.
avast! liczy ile wiadomości wychodzących zostaje przesłanych w określonym czasie. Ustawienie domyślne to 5 wiadomości w ciągu 30 sekund. Oznacza to, że jeśli zostanie wysłanych więcej niż 5 wiadomości w ciągu pół minuty, które posiadają taką samą nazwę lub /i zawartość, zostanie wyświetlone ostrzeżenie.

- **Ostrzeżenie przy liczbie.**
Jest to określona liczba wiadomości posiadających ten sam temat i / lub taki sam załącznik, którą avast! zezwala przesyłać, bez żadnego ostrzeżenia. Gdy ta liczba zostanie przekroczona, będzie wyświetlone ostrzeżenie.
- **Sprawdź temat.**
Jeśli opcja ta jest ustawiona, masowa wysyłka będzie identyfikowana ze względu na temat wiadomości.
- **Sprawdź załącznik.**
Jeśli opcja ta jest ustawiona, masowa wysyłka będzie identyfikowana ze względu na załącznik wiadomości.
- **Liczba absolutna.**

Jest to maksymalna łączna liczba dozwolonych odbiorców wiadomości, tj. adresy w polach Do, Carbon Copy (CC) i Blind Carbon Copy (BCC), przekroczyć ustawienie domyślnie 10, zostanie wyświetlone ostrzeżenie.

3. Ośłona sieciowa

Ośłona Sieciowa chroni Twój komputer przed atakami robaków z Internetu. Działa podobnie do zapory ogniowej (tzw. Firewall), choć nie jest to dokładny substytut tego programu.

Ustawienia

- **Pokaż ostrzeżenie**

Jeśli to pole jest zaznaczone, ostrzeżenie pojawi się w prawym dolnym rogu ekranu, gdy atak robaka internetowego zostanie wykryty.
- **Logowanie**

Jeśli to pole jest zaznaczone, historia ataków robaka będzie rejestrowana i wyświetlana na stronie "Ostatnie ataki". Aby obejrzeć tę stronę, niezbędne jest uzyskanie dostępu do ustawień ochrony rezydenta tj. Należy kliknąć prawym przyciskiem myszy na niebieską "a-ikonkę" w zasobniku systemowym; nie może być ona widoczna podczas uzyskiwania dostępu do ustawień ochrony dostępowej przez wejście w zadania ochrony dostępowej w rozszerzonym interfejsie użytkownika.

Ostatnie ataki

W tej zakładce zostanie wyświetlona informacja dotycząca ostatnich 10 ataków robaka, pod warunkiem, że w poprzedniej zakładce została zaznaczona opcja "Logowanie". Informacja będzie zawierać datę i czas ataku, typ ataku oraz IP adres portu, z którego został on wysłany.

4. Outlook/Exchange

Skaner

Tutaj możesz określić, jakiego typu wiadomości powinny zostać skanowane i czy wiadomości powinny być skanowane również z załącznikami.

Poczta przychodząca

Tutaj możesz określić, co należy zrobić, jeśli zostanie wykryta zainfekowana wiadomość. Może ona być na przykład, dostarczona, odrzucona (usunięta), lub przekierowana na inny adres mailowy. Można również określić, czy operacja powinna dotyczyć wyłącznie czystych i / lub zainfekowanych wiadomości lub również w formacie note, czyli HTML lub TXT. Wszelkie zainfekowane pliki załączone lub zawarte w wiadomości są rozpatrywane zgodnie z ustawieniami w zakładkach "Przechowywanie wirusów" i "Zaawansowane".

Poczta wychodząca

Tutaj możesz określić, czy działania powinny być podjęte w stosunku do czystej wiadomości, oraz formatu note, jak opisano powyżej. Wiadomości zainfekowane nie zostaną w ogóle wysłane. Można również określić, że załączniki będą skanowane podczas ich załączania, a nie podczas wysyłania.

Podpisy

Za pomocą podpisów, możliwe jest znaczne obniżenie liczby wiadomości, które muszą być skanowane. Podpisy można określić jako małe "znaczkki", które są załączone do niezainfekowanej wiadomości, aby potwierdzić, że są one wolne od wirusów. Każdy podpis zawiera datę i czas skanowania.

Podpisy dla dostawcy programu MS Outlook / Exchange są w pełni zgodne z tymi, które posiada avast! np. avast! Exchange Server Edition. Dlatego też wiadomości testowane przez dostawcę Exchange Server nie powinny być ponownie badane przez program Outlook / Exchange, co spowoduje przyspieszenie przesyłania wiadomości

- **Wstaw podpisy do czystych wiadomości.**

To powinno być zaznaczone, jeśli chcesz, aby podpisy zostały dodane do czystych wiadomości.

- **Zawsze ufaj podpisanym**

To pole powinno zostać zaznaczone, w przypadku, że ufasz wszystkim prawidłowo podpisanym wiadomościom i nie muszą one podlegać skanowaniu, bez względu na to jak stary jest podpis (chyba, że zostało zaznaczone pole "Zawsze ignoruj podpisy starsze, niż bieżąca wersja bazy wirusów").

- **Ufaj podpisanym nie starszym niż.**

Tutaj możesz ustawić maksymalny wiek zaufanych podpisów. Wartość ustawienia może być tutaj maskowana przez opcję "Zawsze ignoruj podpisy starsze niż bieżąca baza wirusów" - patrz poniżej.

- **Ignoruj wszystkie podpisy (Brak zaufania).**

Jeśli to pole jest zaznaczone, wszystkie wiadomości zostaną poddane skanowaniu, niezależnie od tego, czy zawierają one prawidłowy podpis.

- **Zawsze ignoruj podpisy starsze, niż bieżąca wersja bazy wirusów.**

Jeśli to pole jest zaznaczone, wiadomość posiadająca ważny podpis zostanie sprawdzona, jeśli podpis jest starszy niż bieżąca baza danych wirusów. Może to być przydatne, ponieważ wiadomość może zawierać nowy wirus, który został dodany do bazy danych wirusów po pierwotnym skanowaniu. Jeśli wiadomość została uznana za zaufaną, nie będzie skanowana i wirus nie będzie mógł zostać wykryty.

Przechowywanie wirusów

W tej zakładce można określić, czy kopia zainfekowanego załącznika powinna być zapisana w danym folderze na twardym dysku komputera. Można użyć przycisku Przeglądaj, aby zlokalizować i wybrać pożądany folder. Jeśli zaznaczysz pole "Nadpisz istniejące plików", każdy plik o tej samej nazwie zostanie zastąpiony przez nowy plik.

Zaawansowane

- Praca w tle

Jeżeli określone działanie wirusa w tej zakładce jest określone jako działanie domyślne, czyli jest zaznaczona opcja interaktywna, zaznaczenie tego pola spowoduje, że wszystkie zainfekowane pliki zostaną automatycznie przenoszone do kwarantanny.

Jeżeli określone działanie w zakładce Wirus jest akcją domyślną to pole na lewo pozostaje niezaznaczone, normalne ostrzeżenie o wirusie zostanie wyświetlone wraz z zapytaniem, jak się chcesz uporać się z zainfekowanym plikiem.

Jeżeli jakiegokolwiek inne działania zostało określony, tj. jakiegokolwiek działanie inne niż opcje interaktywne, zaznaczenie tego pola nie wywoła żadnego efektu.

- Pokaż szczegółowe dane o wykonanej akcji

Jeśli opcja ta jest zaznaczona, informacje dotyczące pliku, który jest w chwili obecnej poddawany testowaniu, zostaną wyświetlone w prawym dolnym rogu ekranu.

- Ikona w polu systemowym podczas skanowania poczty

Jeśli opcja ta jest zaznaczona, mała ikona, zostanie wyświetlona w prawym dolnym rogu ekranu, informując o postępach w skanowaniu.

- Pokaż ekran informacyjny podczas ładowania przez dostawcę
Jeśli to pole to jest zaznaczone, ekran informacyjny avast! zostanie wyświetlony w przypadku, gdy zostanie uruchomiony dostawcy poczty e-mail.

Wreszcie, jeśli podasz swój profil MAPI wraz z hasłem, zostaną one wykorzystane do wyświetlania struktury folderów, po kliknięciu na przycisk Przeglądaj w zakładce Poczta Wychodząca.

Heurystyka

Ustawienia w tej zakładce są takie same, jak w zakładce Poczta

Heurystyka (Zaawansowane)

Ustawienia w tej zakładce są takie same, jak w zakładce Poczta, za wyjątkiem dwóch poniższych ustawień:

- Liczba względna

Jest to dopuszczalna liczba odbiorców pojedynczej wiadomości wyrażona jako procent całkowitej liczby adresów mailowych znajdujących się w książce adresowej. Jeżeli procent ten został przekroczony, ostrzeżenie zostanie wyświetlone.

- Ilość minimalna

Jest to minimalna liczba rzeczywistych odbiorców, odpowiadająca względnej liczbie, poniżej której ostrzeżenie nie będą wyświetlane. Innymi słowy, jeśli liczba względna jest przekroczona, ostrzeżenie nie zostanie wyświetlone, jeśli rzeczywista liczba odbiorców jest mniejsza od liczby minimalnej. Przykład: liczba względna = 20%, ilość minimalna = 10. Jeżeli liczba adresów wynosi 40 i wiadomość jest wysyłana do 9 odbiorców, liczba względna została przekroczona, ale ostrzeżenie nie będzie wyświetlana, ponieważ rzeczywista liczba jest mniejsza niż ilość minimalna.

5. Osłona P2P

Programy

W tej zakładce możesz określić, dla których programów otrzymane pliki powinny zostać poddane skanowaniu. Niektóre programy mogą być chronione jedynie w systemie Windows NT, 2000, XP, 2003, Vista lub 2008.

6. Ochrona standardowa

Skaner (Podstawowy)

W tej zakładce możesz określić, co powinno być skanowane przez ten moduł. Zaleca się, że wszystkie pola na tej stronie powinny pozostały zaznaczone, co umożliwią wykrycie najczęstszych typów wirusa.

Skaner (Zaawansowany)

W tej zakładce można określić które pliki mają zostać skanowane w zależności od ich rozszerzenia, albo gdy są one otwarte, utworzone lub zmodyfikowane.

- Skanuj pliki po otwarciu.

Rozszerzenia dodatkowych plików, które mają być skanowane powinny być oddzielone przecinkiem. Można użyć symbolu wieloznacznego "?" (np. jeżeli chcesz aby zostały poddane skanowaniu wszystkie otwarte pliki htm i. html, albo wpisać "htm", "html" lub użyć symbolu wieloznacznego - "HT?"; w tym ostatnim przypadku. Jednakże wszystkie pliki z rozszerzeniami zaczynające się od " ht ", takie jak " htt ", będą skanowane).

- Zawsze skanuj pliki skryptów WSH.

Zaznaczenie tej opcji pozwala się upewnić, że pliki skryptów (Windows Scripting Host) będą testowane.

- Nie skanuj bibliotek systemowych.

Biblioteki systemowe, które nie są podejrzane, nie będą otwierane i skanowane dogłębnie, ale szybko zostanie sprawdzona ich autentyczność. Opcja ta przyspieszy nieco uruchamianie systemu.

- Skanuj utworzone /zmodyfikowane pliki.

Jeśli pole to jest zaznaczone, pliki zostaną skanowane w momencie ich stwarzania lub modyfikowania. Dodatkowo możesz określić, czy opcja ta powinna odnosić się do:

- Wszystkich plików, lub
- Jedynie plików z określonymi rozszerzeniami

Jeśli pole "Domyślny zestaw rozszerzeń" jest zaznaczone, jedynie te pliki z rozszerzeniami, które są ogólnie postrzegane jako "niebezpieczne" zostaną poddane skanowaniu – kliknij "Pokaż", aby otworzyć listę domyślnych rozszerzeń. Możesz również dodatkowo określić, które rozszerzenia powinny zostać poddane skanowaniu.

Blokada

W tej zakładce możesz określić, które operacje powinny zostać zablokowane dla konkretnych plików z rozszerzeniami. To może być stosowane w stosunku do "Domyślnego zestawu rozszerzeń". Klikając na "Pokaż" zobaczysz listę rozszerzeń domyślnych. Możesz także określić dodatkowe rozszerzenia, które powinny być zablokowane.

Następnie możesz określić dalsze operacje, które powinny zostać zablokowane dla danego typu operacji, tj. otwarcia pliku, zmiana nazwy, usuwanie lub ponowne sformatowanie.

Wreszcie można określić, co należy zrobić, jeśli dotyczy to operacji, którą trzeba zablokować, ale avast! nie jest w stanie uzyskać potwierdzenie, tzn. czy działania powinny być dozwolone lub zabronione.

Zaawansowane

- Pokaż szczegółowe dane o wykonanej operacji

Jeśli to pole jest zaznaczone, informacje o plikach obecnie testowanych będą wyświetlane w prawym dolnym rogu ekranu.

- Praca automatyczna w tle

Jeżeli określone działanie w zakładce wirus jest ustawione jako akcja domyślna tj. Opcja interaktywna, a opcja praca automatyczna w tle jest zaznaczone, wszystkie zainfekowane pliki będą automatycznie rozpatrywane zgodnie z następującymi zasadami:

- Jeśli została zaznaczona opcja "z ogólnym założeniem odpowiedzi Tak (OK)", w stosunku do zarażonego pliku nie zostaną podjęte żadne działania
- Jeśli została zaznaczona opcja "z ogólnym założeniem odpowiedzi Nie (Anuluj)" jakkolwiek wykryty zarażony plik, zostanie automatycznie przesunięty do Kwarantanny.

Jeżeli jakiegokolwiek inne działania są określone, tj. wszelkie działania inne niż domyślne w tzw. interaktywnych opcjach, zaznaczenie tego pola nie spowoduje żadnego efektu.

Wreszcie, można określić konkretne obszary, które powinny być skanowane przez ten moduł. Uwaga, obszary, które zostały wyłączone ze skanowania przez wszystkie moduły nie zostaną pokazane na tej liście.

7. Ochrona www

Ochrona www działa jako lokalny serwer proxy. Dla systemów operacyjnych typu NT (Windows NT/2000/XP/2003/Vista/2008) ochrona jest całkowicie przejrzysta i zwykle nie jest konieczna zmiana jakichkolwiek ustawień. Jeśli korzystasz z systemu Windows 95/98/ME jednak konieczne jest, aby zmienić ustawienia w Opcjach internetowych - w szczególności wpisać zmiany dotyczące adresu i portu lokalnego serwera proxy jak następująco:

Jeśli korzystasz z lokalnej sieci (LAN):	Jeśli korzystasz z połączenia dial-up (modem):
Uruchom Internet Explorer.	Uruchom Internet Explorer.
Wybierz opcje Narzędzia następnie Opcje internetowe ... z menu głównego.	Wybierz opcje Narzędzia następnie Opcje internetowe ... z menu głównego.
Przejdź do zakładki Połączenia	Przejdź do zakładki Połączenia
Kliknij na ustawienia LAN	Wybierz typ połączenia dial-up z listy i kliknij na "Ustawienia".
Zaznacz opcję "Skorzystaj z serwera proxy dla twojego LAN"	Zaznacz opcję "Użyj serwera proxy dla tego połączenia".
Wpisz "lokalnego hosta" w polu adres (ewentualnie możesz wpisać IP adres 127.0.0.1, który jest ten sam jako lokalny host). W polu Port wpisz 12080.	Wpisz "lokalnego hosta" w polu adres (ewentualnie możesz wpisać IP adres 127.0.0.1, który jest ten sam jako lokalny host). W polu Port wpisz 12080.
Potwierdź klikając OK.	Potwierdź klikając OK.

Uwaga: Jeśli korzystasz z wielu połączeń, konieczne jest ustalenie adresu i portu lokalnego serwera proxy dla każdego połączenia osobno.

Podstawowe

- Włącz skanowanie sieci

Odznaczając to pole, możesz wyłączyć funkcję skanowania sieci Web bez wpływu na blokowanie adresów URL, które pozostaną aktywne

- Użyj inteligentnego skanowania strumieniami

Jeśli to pole jest zaznaczone, pliki pobierane skanowane są niemal w czasie rzeczywistym. Części danych są skanowane, jak tylko zostaną dostarczone - i następnie pobierane są jedynie te elementy, które zostały uprzednio sprawdzone i które są wolne od wirusów. Jeśli ta funkcja jest wyłączona, pliki zostaną pobrane w całości do folderu tymczasowego, a następnie poddane skanowaniu.

Inne opcje na tej stronie nie są dostępne w systemie Windows 95, 98 i Millennium:

- Przekierowane porty HTTP

Ustawienie to jest istotne, jeżeli korzystanie z pewnego rodzaju serwera proxy w celu uzyskania dostępu do Internetu i chcesz skanować komunikacji pomiędzy serwerem a komputerem. Jeśli łączysz się z serwerem proxy przy użyciu np. Portu 3128, podaj tę liczbę w tym polu. Program avast! oczekuje, że komunikacja będzie się odbywać w porcie 80 (ustawienia domyślne), a wszystko inne będzie ignorował. Uwaga: Nie wprowadzaj żadnych innych portów niż HTTP (takich jak porty dla ICQ, DC + +, itp.). Wpisane wartości powinny być oddzielone przecinkami.

- Adresy pomijane.

Tutaj należy wpisać serwer nazw lub adresów IP, które będą nie powinny być przekierowane do sieci Osłony www. Wpisane wartości powinny być oddzielone przecinkami.

- Ignoruj komunikację lokalną.

Jeśli opcja ta jest zaznaczona, wszelka komunikacja lokalna, tj. komunikacja pomiędzy programami uruchomionymi na Twoim komputerze będzie ignorowana.

Skanowanie sieciowe

W tej zakładce można określić, które pliki powinny być skanowane, podczas pobierania ich z Internetu. Można określić, że wszystkie pliki powinny być skanowane, lub tylko te, które posiadają rozszerzenia. Jeśli wybierzesz ostatnią opcję, należy wprowadzić rozszerzenia plików, które mają być skanowane, rozdzielając je przecinkami. Można też wprowadzić typy plików MIME, które powinny być skanowane. W obu przypadkach, mogą być używane symbole wieloznaczne.

Wyjątki

Tutaj możesz określić, które obiekty będą nie powinny być skanowane przez Osłonę WWW. Może to być przydatne przy pobieraniu dużej ilości plików z jednego (zaufanego!) portalu

- Wykluczone adresy URL

Użyj przycisku „Dodaj”, aby wprowadzić adresy URL, które powinny być ignorowane. Jeśli chcesz zablokować tylko jedną stronę, konieczne jest, wprowadzenie pełnej ścieżki, np. Jeśli dodasz `http://www.yahoo.com/index.html`, jedynie strona `index.html` zostaną wykluczone z skanowania. Jeśli natomiast wpiszesz `http://www.yahoo.com/ *` żadna ze stron `http://www.yahoo.com` nie będzie skanowane. Podobnie, jeśli chcesz wykluczyć ze skanowania konkretne typy plików, np. pliki z rozszerzeniem `".txt"`, wystarczy wpisać `*.txt`.

Use the Add button to enter the URL addresses that should be ignored. If you want to block a single page only, it is necessary to enter the full path e.g. if you add `http://www.yahoo.com/index.html`, only the page `index.html` will be excluded from scanning. If you enter `http://www.yahoo.com/*`, however, no pages starting with `http://www.yahoo.com` will be scanned. Similarly, if you want a particular file type to be excluded from scanning, e.g. files with a ".txt" extension, simply enter `*.txt`.

- Wykluczane typy MIME

Tutaj możesz określić typy/ podtypów MIME, które mają być wyłączone ze skanowania.

Blokowanie URL

Osłona www może być również wykorzystywana do blokowania dostępu do niektórych stron internetowych. Opcja ta jest wyłączona domyślnie, jednak może zostać wykorzystana, aby uniemożliwić dostęp do "nieodpowiednich" stron internetowych (np. Stron zawierających pornografię, nielegalne oprogramowania, itp.). Jeśli zablokowana strona zostanie uruchomiona w przeglądarce internetowej, pojawi się wiadomość informująca, że dostęp do strony został zablokowany przez program antywirusowy avast!.

Pole "Włącz blokowanie URL" musi najpierw zostać zaznaczone. Następnie możesz wpisać adresy, które mają być blokowane, za pomocą przycisku "Dodaj" i wpisując odpowiednie adresy URL. Symbole wieloznaczne (np. ? oraz *) mogą być wykorzystywane. Na przykład, jeśli wpiszesz `http://www.penthouse.com/*` żadne strony zaczynające się od `http://www.penthouse.com` nie zostaną wyświetlane.

Wpisane adresy URL zostaną ukończone zgodnie z następującymi zasadami:

Jeśli adres nie zaczyna się od `http://` lub symbolu wieloznacznego * lub ?, avast! doda przedrostek `http://` na początku adresu oraz oznaczy gwiazdką na końcu. Jeśli więc wprowadzić `www.yahoo.com`, adres zostanie zmodyfikowany na `http://www.yahoo.com*`.

Zaawansowane

- Pokaż szczegółowe dane o wykonanej operacji

Jeśli to pole jest zaznaczone, informacje o plikach obecnie testowanych będą wyświetlane w prawym dolnym rogu ekranu.

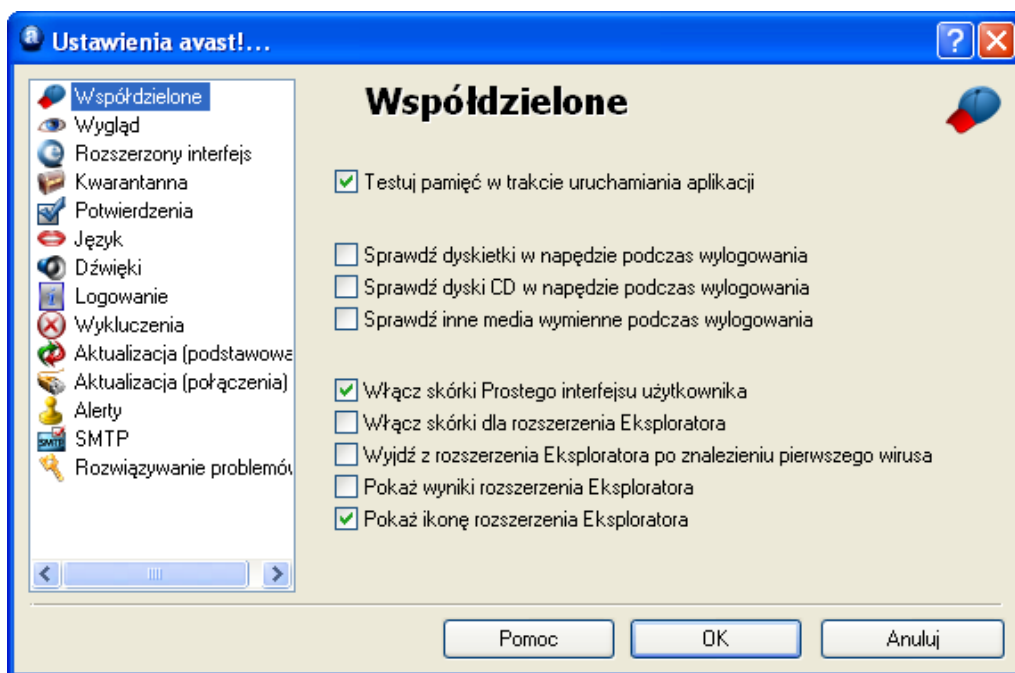
- Praca automatyczna w tle

Jeśli pole to jest zaznaczone, połączenie zostanie przerwane, jeśli dojdzie do wykrycia wirusa

Inne ustawienia programu avast!

Wiele innych elementów programu avast! Może być modyfikowanych w zależności od indywidualnych potrzeb lub preferencji. Niektóre z nich zostały już opisane w poprzednich sekcjach.

Jeśli korzystasz z prostego interfejsu użytkownika i otworzysz **opcje menu** (zobacz [strona 25](#)) oraz klikniesz na "Ustawienia" pojawi się następujący ekran. Jeśli korzystasz z Rozszerzonego interfejsu użytkownika, wystarczy że klikniesz na opcję "Ustawienia" gdzie pojawi się opcja – "Rozszerzony interfejs". inne ustawienia, można zmienić klikając na odpowiedni napis znajdujący się po lewej stronie ekranu:



Ustawienia współdzielone

W oknie tym zostało określone, co jest zaznaczone do sprawdzenia, kiedy włączasz lub wyłączasz komputer. Tutaj możesz również zmienić wygląd programu, zaznaczając lub odznaczając opcję "Włącz skórki...".

Rozszerzenie eksploratora

Ostatnie opcje w tym oknie odnoszą się do "Rozszerzenia eksploratora". Urządzenie to pozwala na skanowanie poszczególnych plików, klikając prawym przyciskiem myszy na niego i wybierając opcję "Skanuj <nazwa pliku>". Jeśli ostatnia opcja jest zaznaczona, obok niej pojawi się niebieska "a-ikonka".

Wygląd

Klikając na "Wygląd" możesz określić czy ikona avast! – niebieska "a-ikonka" – ma być widoczna w prawym dolnym ekranu oraz czy ma się poruszać (kręcić), podczas gdy przebiega skanowanie.

Możesz dodać efekty półprzezroczyste do wyglądu odtwarzacza avast!. Zmiany te zostaną wprowadzone, po tym jak restartujesz komputer.

Potwierdzenia

Okno to umożliwia określenie, czy chcesz zostać poproszony o potwierdzenie, jeśli wybierzesz określoną akcję jak również, jeśli chcesz otrzymywać komunikatory potwierdzające o wynikach, po zakończeniu konkretnych akcji.

Kwerendy potwierdzenia to bezpieczna właściwość programu antywirusowego avast! pozwalająca odwołać akcję, która została wybrana przez przypadek.

Jeśli nie chcesz otrzymywać żadnych konkretnych komunikatorów lub kwerend, po prostu odznacz odpowiednie pola. Jednakże, jeśli kwerendy potwierdzenia są odznaczone, wyniki akcji zostaną pokazane jak tylko odpowiednie akcje zostaną wybrane bez możliwości odwołania ich.

Następujące potwierdzenia / kwerendy są dostępne jako standardowe. Mogą one zostać wyłączone, przez odznaczenie odpowiednich punktów:

- ***Zapytaj przed zamknięciem Prostej interfejsu użytkownika, gdy trwa skanowanie***

Jeśli program jest zamknięty, podczas procesu skanowania, skan zostanie automatycznie zatrzymany w tym punkcie

- ***Zapytaj, czy zachować zmiany w stanie dostawcy rezydentalnego***

Wiadomość ta pojawi się jeśli zdecydujesz się "Zatrzymać" jakkolwiek z poszczególnych modułów – zobacz **strona 23**. Jeśli zaznaczysz "Tak", konkretny moduł pozostanie nieaktywny do momentu aż go ręcznie przywrócisz. Jeśli odpowiesz "Nie", zostanie on reaktywowany, przy następnym restartowaniu komputera.

- ***Zatrzymaj przed zatrzymaniem ochrony dostępnej***

Wiadomość ta pojawi się, jeśli zdecydujesz się "Zatrzymać" osłonę rezydentalną (lub na-dostęp) jako całość – zobacz **strona 20**. Jeśli odpowiesz "Tak", osłona rezydentalna będzie unieruchomiona, jednakże zostanie automatycznie aktywowana przy następnym uruchomieniu komputera.

- **Zapytaj przed usunięciem plików z Kwarantanny**

Jeśli pole to jest zaznaczone, program zawsze zapyta o potwierdzenie, przed usunięciem jakichkolwiek plików. Zabezpiecza to przed automatycznym usuwaniem plików.

- **Komunikat po przetworzeniu wyników z powodzeniem**

Potwierdza, że akcja, która została przeprowadzona w stosunku do określonego pliku, zgłoszona przez program np. Usuń, przesuń do Kwarantanny, została pomyślnie zakończona

- **Komunikat, gdy pojawi się błąd w czasie przetwarzania wyników**

Informuje o tym, że akcja która została przeprowadzona w stosunku do określonego pliku, nie powiodła się. Program zgłasza, że nie może jej dokończyć

- **Komunikat, gdy użyto starego pliku VPS**

Komunikat ten ostrzega, że baza wirusów, nie została aktualizowana. Aby upewnić się, że system jest w pełni chroniony, baza wirusów powinna być regularnie aktualizowana - zobacz [strona 37](#)

- **Ostrzeżenie o wersji BETA programu**

Komunikat ten ostrzega o tym, że wersja którą posiadasz to wersja próbna programu.

- **Pokaż komunikat o udanej wysyłce raportu o błędzie**

- **Pokaż okno stanu w Kwarantannie nawet jeśli akcja zakończona powodzeniem**

Jeśli pole to jest zaznaczone, otrzymasz wiadomość potwierdzającą, że akcja, którą wybrałeś zakończyła się powodzeniem.

- **Komunikat gdy pozytywne wyniki zostały wyłączone podczas konfiguracji.**

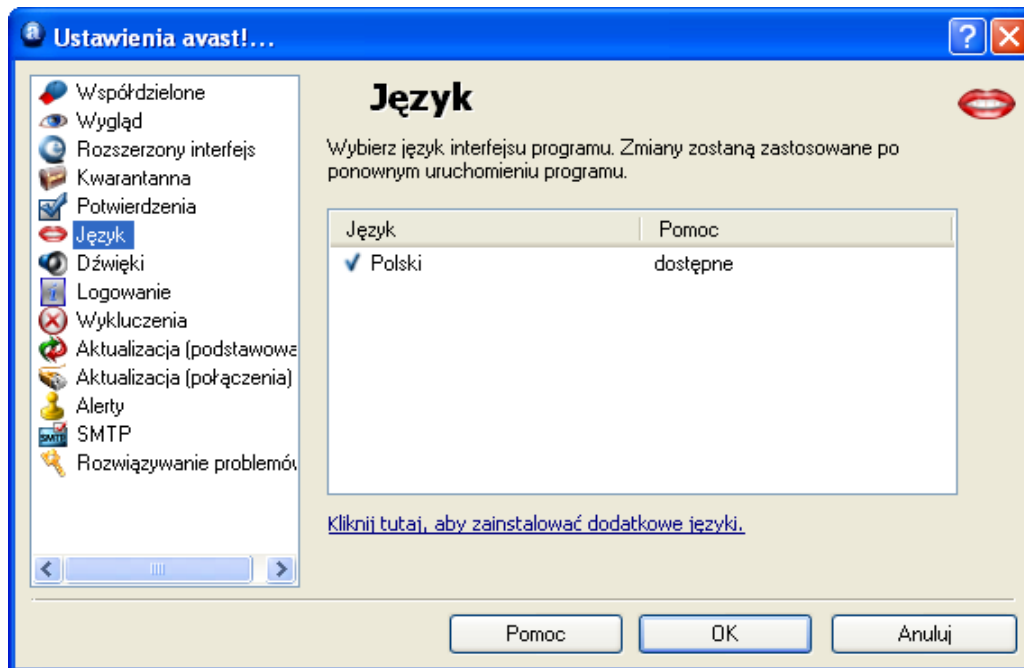
Jeśli pole to jest zaznaczone, otrzymasz ostrzeżenia, jeśli określisz że "OK pliki" powinny być włączone w wyniki skanowania. Uwaga, dotyczy to jedynie tworzenia zadań w Rozszerzonym interfejsie użytkownika.

- **Usuwanie plików z niebezpiecznym rozszerzeniem**

Ostrzega o tym. Że nie jest bezpieczne usuwanie określonych plików lub typów plików, które zawierają ważne dane.

Zmiana języka programu

Jeśli chcesz zmienić język programu, kliknij na "Język", a pojawi się poniższy obrazek:



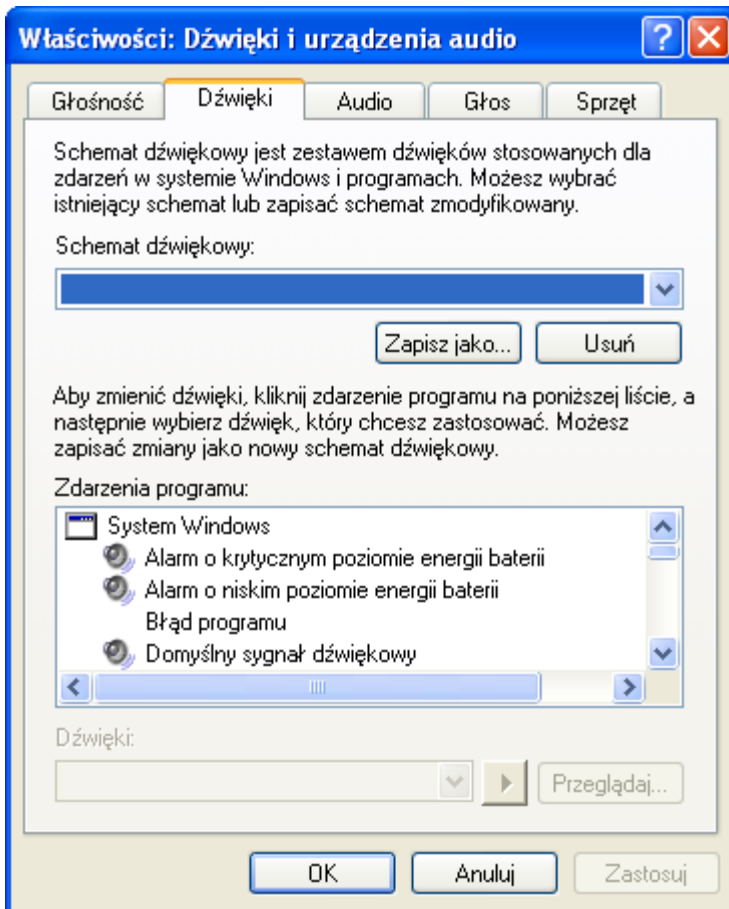
Jeśli wymagany język pojawia się jako "dostępna" opcja w oknie na prawo, kliknij na niego i wybierz go, a następnie kliknij "OK". Następnie zamknij program, a następnym razem jak go uruchomisz język zostanie zmieniony.

Jeśli wymagany język nie pojawia się jako "dostępny", kliknij na "Zainstaluj dodatkowe języki..." poniżej okna, następnie oznacz pole obok języka który chcesz ustawić. Kliknij "Dalej" i dodatkowe pliki programu owe zostaną zainstalowane. Po zakończeniu kliknij "Dokończ".

Dźwięki

W tym oknie możesz ustawić dźwięki audio programu lub wyłączyć zupełnie dźwięk.

Klikając ponownie na "Ustawienia", przejdziesz do okna, w którym możesz zmienić dźwięk dla wszystkich programów Windows. W dolnej połowie ekranu znajduje się okno "Schemat dźwiękowy" – zobacz poniżej



Klikając na strzałkę obok niebieskiego okna, mniej więcej w połowie listy, znajdziesz schemat dźwiękowy programu antywirusowego avast! Do którego mogą zostać przypisane nowe dźwięki. Kliknij na odpowiedni schemat dźwiękowy a następnie "Przeglądaj". Z dostępnej listy, wybierz dźwięk, który Ci się podoba I kliknij "OK".

Następnie wróć w okno poniżej I kliknij na "Aplikuj Użyj" następnie ponownie "OK".

Ponownie wrócisz do głównego okna "Dźwięki", gdzie powinieneś ponownie kliknąć "OK", aby zakończyć.

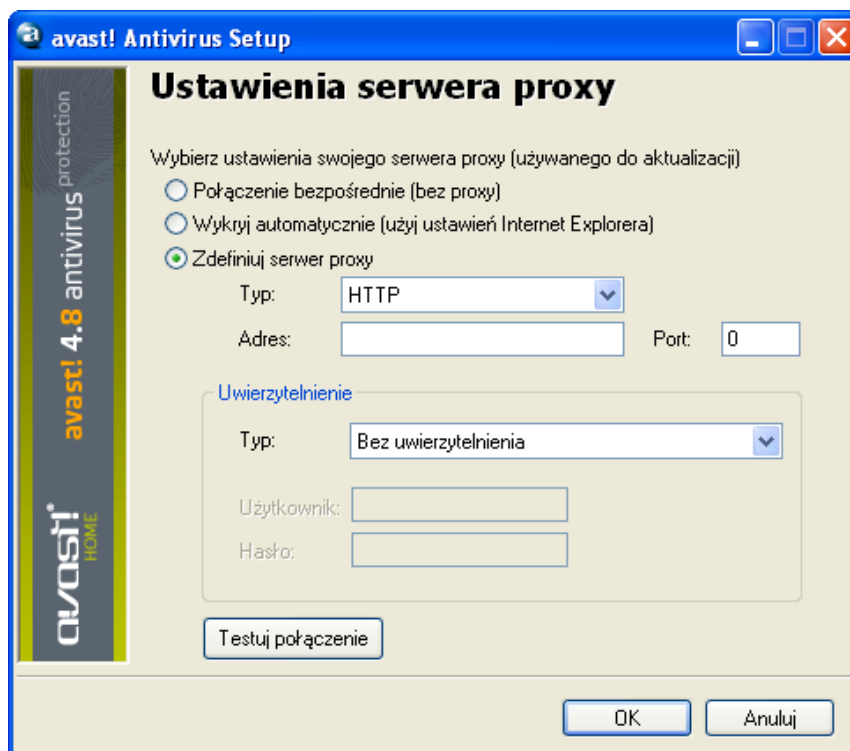
Aktualizacje (połączeń)

W tym oknie możesz określić, tym połączenia internetowego, zaznaczając odpowiednie pole itp.

- Łączę się z Internetem przez modem
- Mój komputer ma stałe łącze z Internetem.

Optymalizuje to sposób, w jaki avast! Sprawdza aktualizacje i spowoduje, że możesz bardziej polegać na automatycznych aktualizacjach.

Jak tylko określisz typ połączenia, kliknij na przycisk "Proxy". W nowym oknie, które zostanie otwarte możesz wpisać ustawienia serwera proxy. Ustawienia serwera proxy są niezwykle istotne, aby avast! Miał dostęp do Internetu podczas np. Aktualizacji.



Jeśli łączysz się bezpośrednio z Internetem (tj. nie przez proxy), co zazwyczaj oznacza, że jesteś użytkownikiem modemu, wybierz opcję "Połączenie bezpośrednie (Nie proxy)"

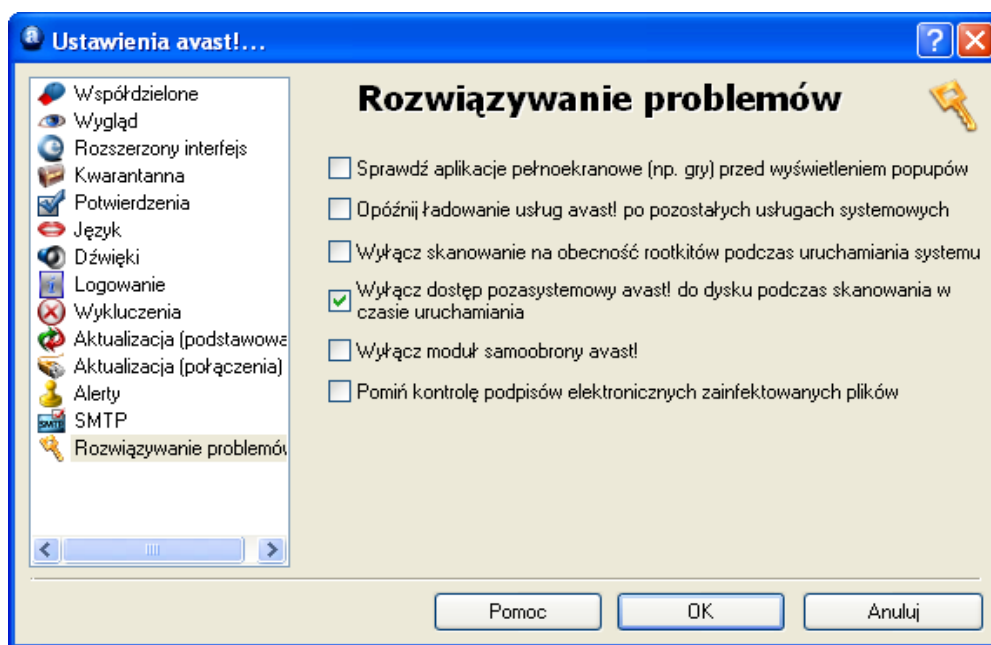
Jeśli nie jesteś pewien czy używasz serwera Proxy lub jakiego połączenia używasz, wybierz "Wykryj automatycznie (użyj ustawień Internet Explorera)", lub zapytaj swojego dostawcy internetowego lub administratora sieci.

Jeśli nie znasz adresu swojego serwera proxy, wybierz opcję "Zdefiniuj serwer proxy" i wpisz wymagane szczegóły, jak zostało podane poniżej:

- **Typ.** HTTP lub SOCKS4
- **Adres.** Wpisz adres swojego serwera proxy
- **Port.** Wpisz nazwę portu swojego serwera proxy.
- **Typ uwierzytelnienia.** W tym miejscu określ, czy dostęp do Internetu przez serwer proxy wymaga uwierzytelnienia użytkownika, a jeśli tak, czy wymaga odpowiedniego typu uwierzytelnienia
- **Nazwa użytkownika i hasło.** To okno powinno zostać wypełnione, jeśli uwierzytelnienie jest wymagane.

Wreszcie, kliknij na "Testuj połączenia" aby sprawdzić jak pracuje połączenie internetowe (na podstawie powyższych ustawień).

Rozwiązywanie problemów



Zmieniając ustawienia w tym oknie, pomożesz rozwiązać niektóre ze specyficznych problemów. Jednakże ustawienia te, nie powinny zostać zmienione, bez ważnej przyczyny. Jeśli pojawią się jakiegokolwiek wątpliwości prosimy o uprzedni kontakt z działem wsparcia technicznego avast!.

Sprawdź aplikacje pełnoekranowe (np. Gry) przed wyświetleniem popupów.

Według ustawień konfiguracji avast!, mogą pojawiać się różne wiadomości, podczas pracy Twojego komputera (np. Kiedy baza wirusów jest aktualizowana, kiedy przychodzące maile skanowane są przed wirusami, itp.). Normalnie, wiadomości pokazują się jedynie, jeśli pojawiają się odpowiednie zdarzenie. Może to jednak powodować, że aplikacje pełnoekranowe (np. gry) będą przerwane - Windows przejdzie z pełnoekranowego modułu na moduł zwykłego okna, w którym zostaną wyświetlone wiadomości. Jeśli zaznaczysz tę opcję avast! wszystkie pełnoekranowe aplikacje uruchomione wcześniej i pokaże komunikat. Jeśli zostanie odnaleziona aktywna aplikacja, nie pojawi się wiadomość avast!.

Opóźnij ładowanie usług avast! po pozostałych usługach systemowych

Program antywirusowy avast! Jest najczęściej uruchamiany wcześniej podczas startu komputera. Może to czasami powodować problemy podczas uruchamiania pozostałych usług systemu - co może powodować tymczasowe zawieszenie (na kilka sekund lub minut) systemu, tuż po jego uruchomieniu. Opcja ta, powoduje opóźnienia w uruchamianiu usług programu antywirusowego avast! do momentu pełnego załadowania pozostałych usług serwisu.

Wyłącz skanowanie na obecność rootkitów podczas uruchamiania systemu.
Program avast! Skanuje na obecność rootkitów, za każdym razem, kiedy uruchamiasz system operacyjny. Zaznacz to pole, jeśli chcesz wyłączyć ten skan.

Wyłącz dostęp pozasystemowy avast! do dysku podczas skanowania w czasie uruchamiania

Podczas skanowania w czasie uruchamiania avast! Korzysta ze specjalnej metody dostępu do dysku, która umożliwia wykrycie wirusa, którego pliki pozostają w ukryciu. Możesz wyłączyć tę opcję - avast! Będzie korzystał z metody dostępu do normalnego dysku.

Wyłącz moduł samoobrony avast!.

Niektóre wirusy są w stanie wyłączyć program lub zatrzymać jego działanie, usuwając pliki krytyczne lub modyfikując je. avast! Zawiera specjalny moduł samoobrony, który zapobiega, przed atakami, blokując niebezpieczne operacje. Aby wyłączyć moduł Samoobrony, zaznacz to pole.

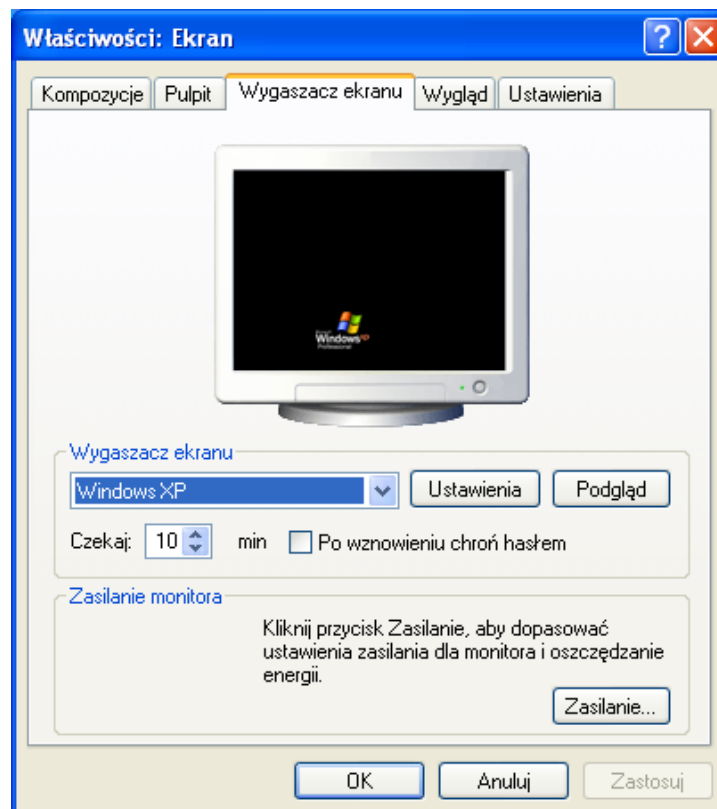
Pomiń kontrolę podpisów elektronicznych zainfekowanych plików.

Aby zapobiec fałszywym alarmom, avast! Sprawdza zainfekowane pliki, w poszukiwaniu podpisów cyfrowych. Jeśli zostanie wykryty plik jako zarażony, ale równocześnie zawiera ważny podpis cyfrowy zaufanego pochodzenia (np. Microsoft), prawdopodobnie jest to tzw. fałszywy, a avast! zignoruje te (fałszywe) wykrycie. Zaznaczając te pole, uniemożliwisz dodatkową kontrolę - avast! zgłosi wszystkie zainfekowane odnalezione pliki.

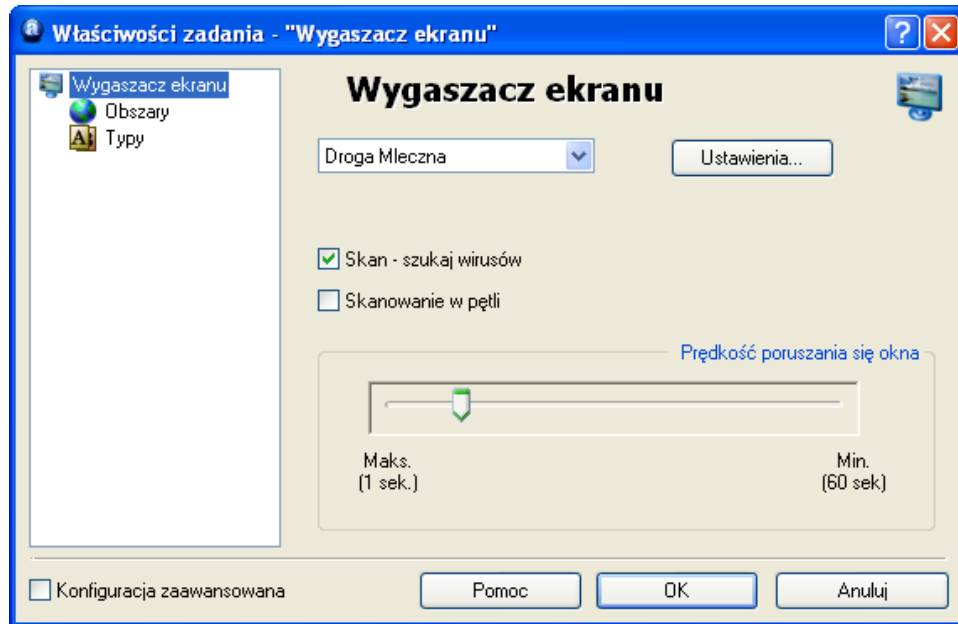
Jak aktywować antywirusowy wygaszacz ekranu avast!

Program antywirusowy avast! potrafi skanować komputer w poszukiwaniu potencjalnych infekcji wirusowych w czasie, kiedy komputer nie jest używany a wygaszacz ekranu jest aktywny. W tym czasie, małe okienko pojawi się na wygaszaczu ekranu, informując o postępach w skanowaniu.

Aby włączyć wygaszacz ekranu, kliknij na "Start" na pasku narzędzi, w lewym rogu wybierz opcję "Ustawienia". Następnie kliknij na "Panel sterowania" oraz podwójnie kliknij na "Ekran" a następnie na pierwszą niebieską strzałkę na dole, aby obejrzyć dostępne opcje. Kliknij na program antywirusowy "avast!" w oknie znajdującym się poniżej, możesz również dokonać zmian w liczbie minut, po których wygaszacz ekranu zostanie aktywowany, używając niebieskiej strzałki, a jeśli jest to konieczne wpisując hasło, aby kontynuować.



Klikając na "Ustawienia", możesz wybrać normalny wygaszacz ekranu, który zostanie polecony w oknie avast!. Następnie pojawi się status ekranu - zobacz następną stronę.



Jeśli chcesz, aby twój komputer był skanowany w poszukiwaniu wirusów, za każdym razem jak wygaszasz ekranu jest aktywny, zaznacz opcję "Skanuj w poszukiwaniu wirusów". Jeśli okno to nie jest zaznaczone, wygaszacz ekranu będzie działał jedynie jako normalny wygaszacz ekranu bez żadnych dodatkowych funkcji.

Zaznaczając opcję "Skanowanie w pętli" upewnisz się, że skan zostanie uruchomiony za każdym razem jak tylko zostaną poddane skanowaniu wszystkie określone obszary skanowania.

Zmiana szybkości ruchu okna, spowoduje zmiany w częstotliwości wyświetlania się okna prezentującego postęp skanowania..

Klikając ponownie na "Ustawienia" uniemożliwisz zmianę ustawień normalnego wygaszacza ekranu.

Poprzez kliknięcie na "Miejsca" można określić, jakie obszary komputera powinny być skanowane. Obszarów, które mają być skanowane automatycznie "Wszystkie dyski twarde". Jeśli nie chcesz wszystkich dysków twardych, które mają być skanowane, usunąć poprzez kliknięcie na nim, a następnie klikając przycisk "usuń". Następnie można określić obszary, które mają być skanowali klikając na przycisk "Przeglądaj" i wybraniu odpowiedniego obszaru (-ów), zaznaczając odpowiednie pola. Klikając przycisk "Dodaj" możesz wybrać jedną z kilku wcześniej zdefiniowanych obszarów.

Po wybraniu obszaru (-ów), które mają być poddane skanowaniu, kliknij na "Typy", aby określić, które pliki powinny zostać objęte skanowaniem. Pliki mogą być uznane za podejrzane w zależności od ich nazwy, treści lub w oparciu o ich rozszerzenie.

Jeśli wybierzesz opcję skanowania w oparciu o zawartości, możesz określić, że wszystkie pliki powinny być skanowane, zaznaczając pole :Skanuj wszystkie pliki ". Jeśli zaznaczysz to

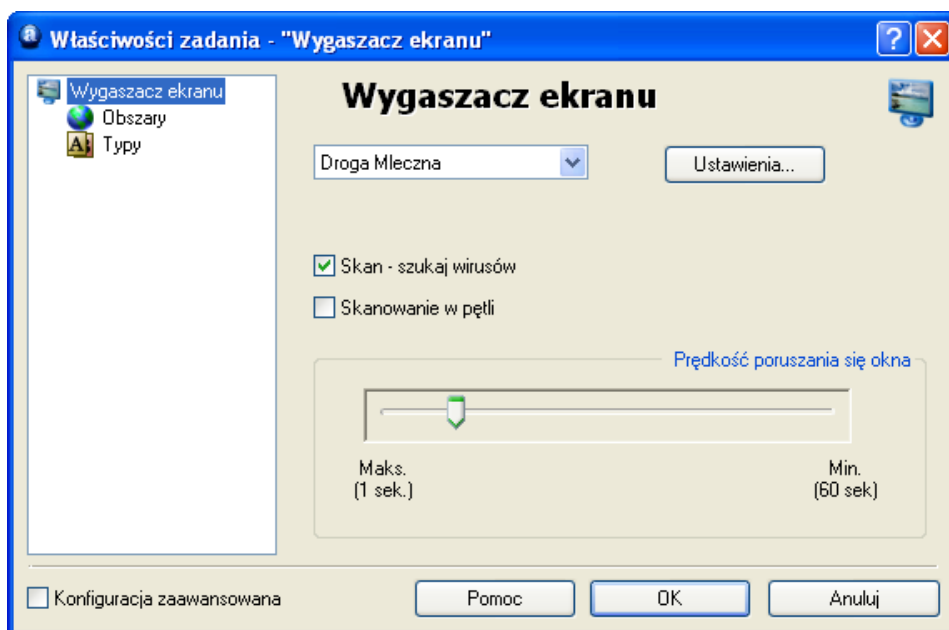
pole, oznacza to, że nawet te pliki, które zazwyczaj nie zawierają wirusów, np. pliki graficzne, również będą skanowane. Jeśli pole pozostanie odznaczone, pliki te nie będą skanowane i będą zgłaszane jako "pomijane pliki".

Jeśli wybierzesz opcję skanowania w oparciu o typ rozszerzenia, to wtedy trzeba określić, które rozszerzenia powinny być uznane za podejrzane.

Aby poddać skanowaniu pliki w oparciu o jeden lub więcej konkretnych rozszerzeń, kliknij przycisk "Przełączaj". Zostanie wyświetlona lista rozszerzeń plików. Jeśli nie możesz znaleźć rozszerzenia, które chcesz dodać, kliknij na nie, a następnie kliknij "OK", aby dodać je do listy. Jeśli rozszerzenie, które chcesz dodać nie znajduje się na liście, można go dodać ręcznie. Kliknij przycisk "Dodaj", a następnie wpisz rozszerzenie pliku, który chcesz dodać. Aby dodać kolejne rozszerzenie, kliknij przycisk "Dodaj" ponownie. Jeśli chcesz usunąć plik z rozszerzeniem listy, po prostu kliknij na jej zaznacz ją i kliknij "Usuń".

Jeśli pole „Skanuj rozszerzenia domyślne” jest zaznaczone, oznacza to, że wszystkie znane niebezpieczne rozszerzenia zostaną automatycznie skanowane. Żadne inne pliki, niż wymienione nie będą skanowane.

Jeśli zaznaczysz pole "Zaawansowane", szereg dodatkowych opcji zostanie wyświetlanych - patrz poniżej.



- **Czułość**

Zaznaczając opcję "Skanuj pliki" (może to być bardzo powolny i długotrwały proces), spowodujesz, że pliki będą testowane w całości, a nie jedynie ich części, które są najbardziej podatne na zarażenie. Większość wirusów zostaje umieszczona na początku pliku lub na jego końcu. Zaznaczenie tej opcji, spowoduje, że pliki zostaną poddane skanowaniu w całości, czyli dokładniej, ale będzie się to wiązało ze spowolnieniem tempa skanu.

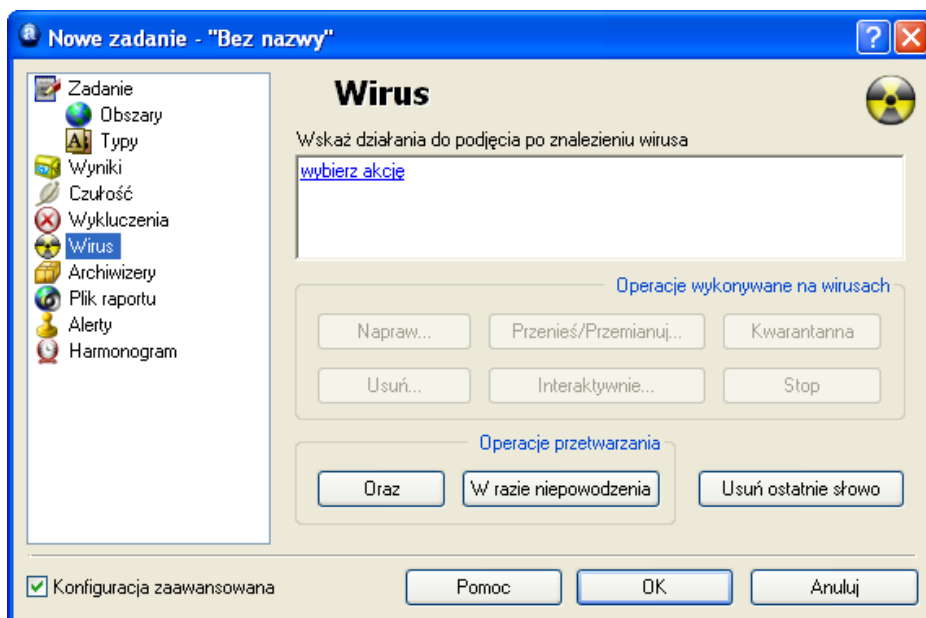
Zaznaczając opcję "Ignoruj wiodącego wirusa" spowodujesz, że pliki zostaną przetestowane, w poszukiwaniu wszelkich wirusów znajdujących się w bazie danych. Jeśli opcja ta nie zostanie zaznaczona, pliki zostaną jedynie przetestowane.

- **Wykluczenia**

Istnieje również możliwość wykluczenia niektórych plików lub folderów ze skanowania. Działa to dokładnie w ten sam sposób, jak zostało wcześniej opisane, za wyjątkiem tego, że ustawione w tym oknie wykluczenia, będą dotyczyły specjalnych zadań. Pliki lub foldery, które są zawarte w „Ustawieniach” w menu zostaną automatycznie wyłączone ze skanowania. Pliki, które zostały wyłączone ze skanowania, pojawią się w raporcie, w wynikach „Pliki pominięte”.

- **Wirus**

Klikając na opcję „Wirus” otworzysz poniższe okno:



W tym oknie możesz określić, jakie działania chcesz podjąć po wykryciu wirusa. „Wybierz akcję” jest ustawieniem domyślnym. Jest to opcja „Interaktywna”.

Jeśli pozostało to jako opcja do wyboru, oznacza to, że jeśli zostanie wykryty podejrzany plik, zostanie zaprezentowana lista opcji, z których możesz wybrać jedną. Oznacza to, że możesz określić, jakie działania powinny być podjęte w stosunku do poszczególnych podejrzanych plików.

Klikając na „Wybierz akcję”: otworzysz listę opcji, które pojawią się w momencie wykrycia podejrzanego pliku tj. Usuń, Napraw, Przesuń do Kwarantanny, Przesuń / Przemianuj lub Zatrzymaj. Jedynie opcje, które są zaznaczone zostaną zaprezentowane jako opcje dostępne. Jeśli jakaś opcja nie została zaznaczona, nie zostanie zaprezentowana jako dostępna, w momencie wykrycia podejrzanego pliku. Wszystkie z tych opcji zostały opisane na **stronie 32** w sekcji, „Co należy zrobić, jeśli został wykryty wirus”.

Wybierając tę opcję spowodujesz, że skan zostanie zawieszony w momencie wykrycia, o ile nie sprecyzujesz, jaką akcję należy podjąć. Dlatego polecamy wybrać jedną lub więcej innych opcji, tak jak na przykład przesuń plik do Kwarantanny, jeśli planujesz, aby zadanie zostało uruchomione w momencie, kiedy nie pracujesz na komputerze.

Aby wybrać inne działanie, kliknij na „Usuń ostatnie słowo”. Ustawieniem domyślnym będzie następnie usunięcie, a 6 możliwych akcji zostanie podkreślonych w środku ekranu. Klikając na jakąkolwiek z nich, dodasz akcję do okna znajdującego się poniżej. Akcja to zostanie później zastosowana w stosunku do wszystkich podejrzanych plików, które zostaną wykryte. Aby ją usunąć, po prostu kliknij ponownie „Usuń ostatnie słowo”.

Pierwsze cztery akcje zostały szczegółowo opisane na [stronie 32](#). Klikając na „Interaktywny” ponownie włożysz „Wybierz akcję”. Klikając stop, po prostu zatrzymasz skan jak tylko zostanie wykryty podejrzany plik.

Można określić więcej niż jedną akcję korzystając z przycisku „Dodaj”. Na przykład możesz określić, że jakkolwiek zainfekowany plik będzie naprawiony i przesunięty w inne miejsce, klikając na „Napraw”, później „oraz” a później „Przenieś/Przemianuj”.

Dodatkowo możesz również określić alternatywne działania, które powinny zostać podjęte, jeśli wcześniejsze akcje nie zadziałały. Na przykład, możesz wybrać opcję „Napraw” jako preferowaną akcję, jednakże, klikając na „W razie niepowodzenia.....” „Przesuń do Kwarantanny” upewnisz się, że każdy plik, który nie mógł zostać naprawiony, zostanie przesunięty do Kwarantanny – zobacz [strona 48](#).

Uwaga, wybierając „Usuń”, będziesz w stanie określić, jeśli plik zostanie usunięty na zawsze (akcja domyślna) lub po prostu przesunięty do kosza. Jeśli zaznaczysz opcję „Usuń pliki na zawsze”, będziesz również mógł określić czy plik (i) powinny zostać usunięte następnym razem, kiedy komputer zostanie uruchomiony, lub czy nie powinny być usunięte – w takiej sytuacji zaznacz opcję, „Jeśli konieczne, usuń plik (i), przy następnym uruchomieniu komputera”.

- **Archiwizery**

W tym oknie możesz określić, które pliki archiwów powinny zostać poddane skanowaniu. W ustawieniach domyślnych znajduje się jedynie samo-wyodrębnianie plików wykonywalnych. Możesz określić, które dodatkowe archiwa powinny zostać poddane skanowaniu, choć należy mieć na uwadze, że proces ten spowolni skanowanie. Zaznacz wszystkie formaty kompresji, jeśli chcesz aby wszystkie archiwa zostały poddane skanowaniu.

- **Plik raportu**

W opcji tej możesz utworzyć plik raportu zawierające kluczowe informacje dotyczące ukończenia zadania. Informacje zawarte w raporcie są kluczowe tak jak informacje zapisane w sekcji wyniki. Różne opcje, dla tworzenia plików raportu zostały opisane na [stronie 41](#).

Uwaga: Nazwa domyślna pliku raportu to task_name.rpt. Plik raportu, to prosty plik tekstowy, który można łatwo przeglądać oraz modyfikować.

- **Alerty**

Alerty mogą być ogólnymi alertami, które zostaną wysyłane za każdym razem, w momencie gdy wirus zostanie wykryty. Mogą zostać wygenerowane tylko wtedy, gdy wirus zostanie wykryty przez poszczególne zadania, z którym jest powiązany.

Alerty, które mogą zostać dodane do zadań, pojawiają się jako „dostępne alerty”. Ogólne alerty tworzą się przez kliknięcie na „Ustawienia” oraz „Alerty”, jak zostało opisane na **stronie 44**, jednakże alerty, które zostały stworzone w ten sposób, nie zostaną powiązane z zadaniem.

Jeśli alert, który chcesz dodać znajduje się tutaj, kliknij na niego, podkreśl go a następnie kliknij na przycisk “→”. W ten sposób alert zostanie przesunięty do pliku „Użytych alertów”, co oznacza, że nie zostanie on powiązany z zadaniem.

Jeśli alert, który chcesz dodać nie pojawia się, kliknij na “Nowy” aby stworzyć nowy alert.

Do alertu możesz przypisać nazwę, na przykład nazwę, która wiąże go z zadaniem. Dodatkowo możesz dodać informacje w oknie “komentarz”. Alert zostanie wtedy stworzony w dokładnie ten sam sposób, jak to zostało opisane na **stronie 44**.

Jak tylko stworzysz nowy alert, kliknij OK, a zostanie on automatycznie umieszczony w oknie „Użyte alerty”.

Aby usunąć alert z okna “Użyte alerty”, kliknij na niego, podkreśl go, a następnie kliknij na przycisk “←”, dzięki któremu przesuńiesz z powrotem do pliku „dostępne alerty”.

Aby zmienić lub usunąć alert, podkreśl go i kliknij „Zmień” lub „Usuń”.

Jeśli chcesz stworzyć SMTP alert, nie zapomnij wpisać również danych dotyczących SMTP, po tym jak dokończysz tworzenia swojego zadania, klikając na “Ustawienia” i “SMTP”.

Uwaga: alerty przyporządkowane zadaniom zostaną wysłane jedynie w momencie wykrycia wirusa, przez określone zadanie. Nie będą wysłane jeśli wirus został wykryty przez inne zadanie. Jeśli chcesz, aby alert został wysłany za każdym razem, jak zostanie wykryty wirus, powinieneś stworzyć generalny alert, tak jak to zostało opisane na **stronie 44**.

W ten sposób stworzony alert można zobaczyć, klikając na plik “Alert” na liście plików. W tym miejscu możesz stworzyć nowy alert, który może być użyty, przy tworzeniu zadań w przyszłości. Aby tego dokonać, kliknij na „Alerty” na górze ekranu, następnie prawym przyciskiem kliknij na plik Alerty na liście plików, następnie wybierz opcję utwórz „Nowy alert”.

Wcześniej wytworzony alert, może być zmieniony oraz wymazany przez podkreślenie i kliknięcie na “Alerty” na górze ekranu, a następnie wybranie “Edytuj alert” lub “Usuń alert”.

Jak dokonać aktualizacji do wersji Home Edition

Aktualizacja z Home Edition do wersji Home Edition jest bardzo prosta.

Nie trzeba odinstalowywać bieżącej wersji programu. Nie jest również wymagane dodatkowe pobranie aktualizacji. Po prostu wystarczy zakupić wersję Home Edition. Po uzyskaniu nowego klucza licencyjnego trzeba go wstawić programowi. Dodatkowe elementy zostaną następnie automatycznie pobierane i Twój program natychmiast zostanie zaktualizowany do wersji Home Edition.

Klucz licencyjny można nabyć na okres 12, 24 lub 36 miesięcy - po prostu przejdź do www.avast.com i kliknij przycisk "Kup".

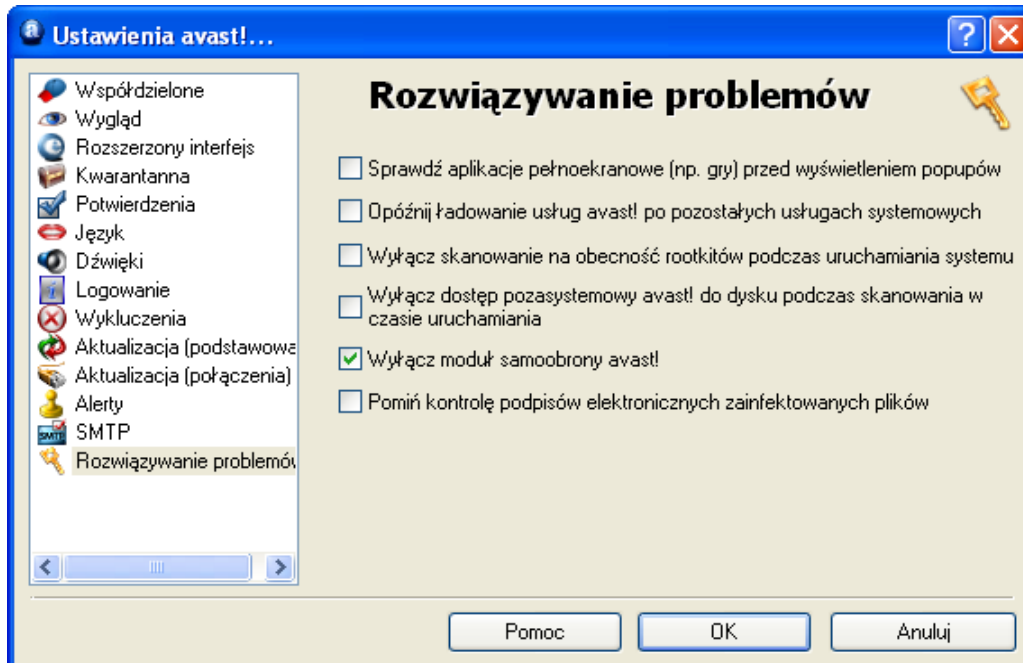
Jak odinstalować program antywirusowy avast!

Niektóre wirusy są zaprojektowane tak, aby umiały wyłączyć oprogramowanie antywirusowe. Dlatego teraz program antywirusowy avast! jest chroniony przez silny moduł samoobrony (SD), który uniemożliwia jego zmianę lub usunięcie przez wspomniane wirusy. Jednak konsekwencją tego jest fakt, że inne ważne programy mogą również napotykać trudności, aby zmienić lub usunąć program avast! w porównaniu do poprzedniej wersji. W celu właściwego usunięcia programu antywirusowego avast!, istotne jest prawidłowe postępowanie.

Przed próbą odinstalowania programu antywirusowego avast!, zalecane jest, aby zamknąć wszystkie inne aplikacje, które mogą być uruchomione na komputerze. Aby odinstalować program antywirusowy avast!, zalecana jest następująca procedura.

1. Wyłącz opcję Samoobrona

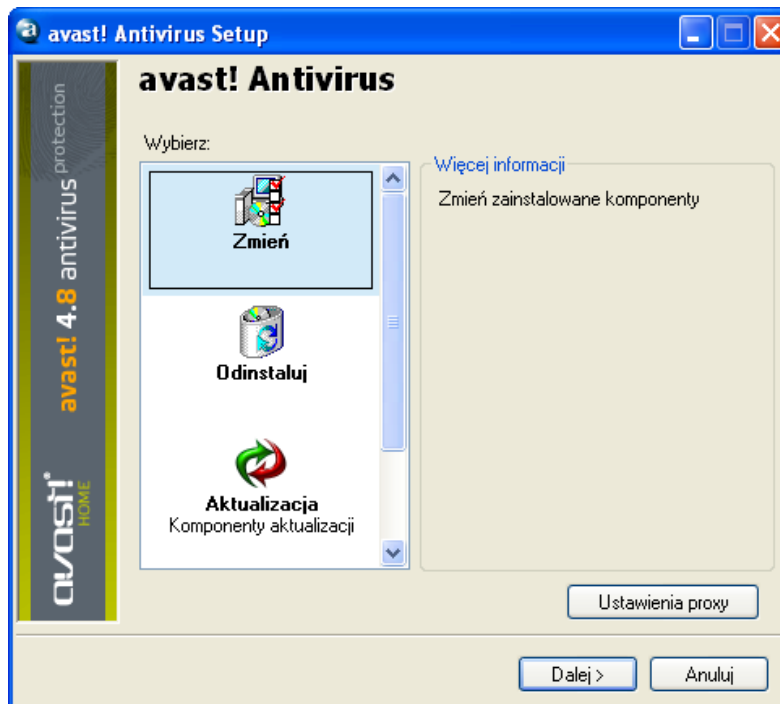
- Prawym przyciskiem myszy kliknij na niebieską "a-ikonkę" znajdującą się w prawym dolnym rogu ekranu komputera i z menu opcje, wybierz "Ustawienia programu".
- Kliknij na opcję "Rozwiązywanie problemów", znajdującą się po lewej stronie ekranu i z menu wybierz opcję, tak jak zostało pokazane poniżej



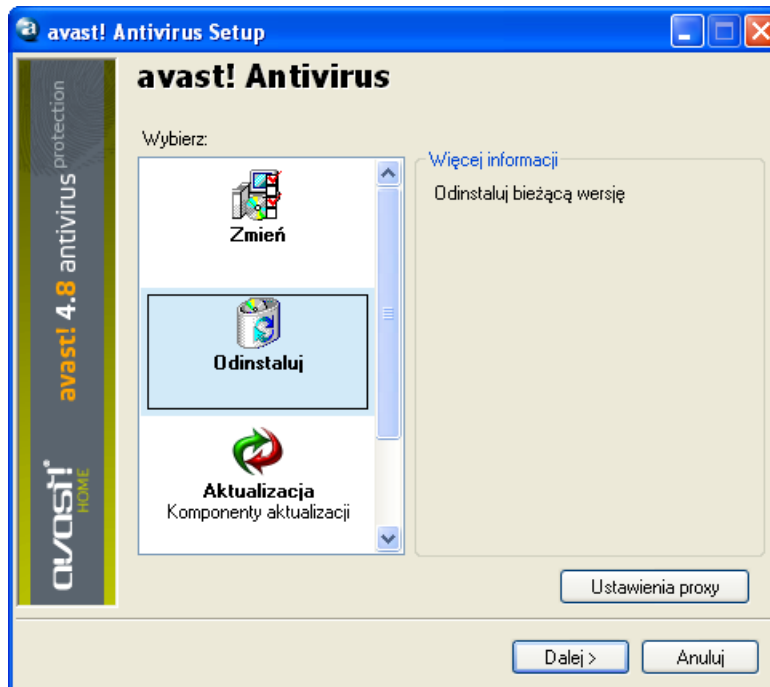
- Zaznacz opcję "Wyłącz moduł samoobrony avast!" i kliknij "OK"
- Moduł Samoobrony jest teraz wyłączony.

2. Usuń program

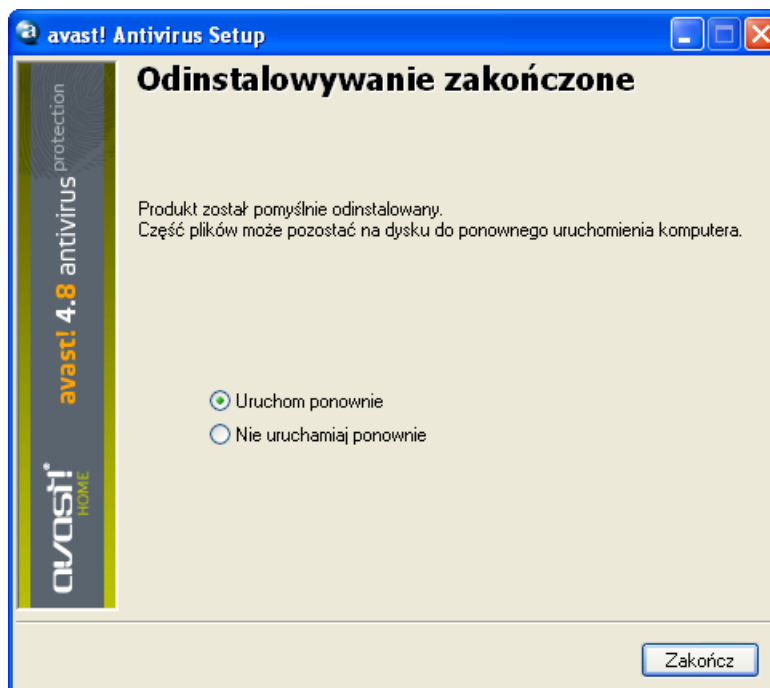
- Kliknij na Start w lewym dolnym rogu twojego ekranu i otwórz opcję Panel sterowania. Jeśli nie widzisz tej opcji w Menu Startu, kliknij na Ustawienia i powinna się ona pojawić jako jedna z opcji
- W Panelu sterowania wybierz opcję "Dodaj lub usuń programy".
- Pojawi się lista dostępnych zainstalowanych programów.
- Zaznacz "avast! antivirus" klikając na niego a następnie klikając na "Zmień/Usuń"



Kliknij na "Odinstaluj" a następnie na "Dalej"



Program zostanie teraz usunięty oraz pojawi się następujący obrazek:



Aby dokończyć proces odinstalowania, niezbędne jest ponowne uruchomienie komputera. Wybierz "Uruchom ponownie", kliknij na "Zakończ", a Twój komputer zostanie automatycznie restartowany.