

G Data Security 2011

Podręcznik użytkownika

Wszystkie prawa zastrzeżone. Oprogramowanie oraz pisemny materiał informacyjny chronione są prawami autorskimi. Dozwolone jest wykonanie jednej kopii bezpieczeństwa oprogramowania, która nie może być udostępniania osobom trzecim.

G Data Software Spółka z ograniczoną odpowiedzialnością zastrzega sobie wszelkie prawa, a w szczególności do publikacji, powielania, edycji i korzystania z oprogramowania. Żadna część niniejszego podręcznika nie może być w żadnej formie powielana, ani przechowywana w bazach danych lub też jakichkolwiek innych systemach przechowywania danych bez pisemnej zgody wydawcy. Wyjątkiem są cytaty w artykułach recenzujących.

G Data Software Sp. z o.o. nie ponosi odpowiedzialności za szkody spowodowane użytkowaniem programu. Treść podręcznika może ulec zmianie. Aktualna pomoc znajduje się na stronie internetowej www.gdata.pl.

ISBN 978-83-61624-12-7

G Data Software Sp. z o.o.
ul. 28 Lutego 2, 78-400 Szczecinek
tel. 094 3729 650
faks 094 3729 659
e-mail: biuro@gdata.pl
Bank Zachodni WBK S.A.
63 1090 1711 0000 0001 0987 7149

Wydanie pierwsze, Szczecinek 2010
Printed in Poland

G Data Software Sp. z o.o.

Spis treści

Rozdział I Wstęp	1
Rozdział II Pomoc techniczna	2
Rozdział III Instalacja programu	4
Rozdział IV Po instalacji	5
Rozdział V Pierwsze uruchomienie	6
1 Pierwsza aktualizacja	7
2 Pierwsze skanowanie	9
Rozdział VI Centrum zabezpieczeń	11
1 Jak poprawić bezpieczeństwo?	12
2 Co pokazuje Centrum zabezpieczeń?	14
Rozdział VII Skanowanie	17
1 Ostatnie skanowanie	18
Rozdział VIII Strażnik	23
1 Opcje Strażnika	24

II G Data Security

Rozdział IX Porady dotyczące instalacji	30
1 Dostępna jest nowa wersja oprogramowania	30
2 Instalacja nie rozpoczyna się automatycznie	31
3 Inicjatywa G Data Malware Information	32
4 Instalacja pełna czy niestandardowa?	34
5 Nieprawidłowy numer rejestracyjny	35
6 Deinstalacja programu	35
Rozdział X Porady dotyczące aktualizacji	36
1 Co to są aktualizacje sygnatur wirusów?	37
2 Jak uaktualnić sygnatury wirusów?	37
3 Co to jest aktualizacja oprogramowania?	39
4 Nieprawidłowe lub zagubione dane dostępu	39
5 Jak przenieść licencję na inny komputer?	40
6 Jak korzystać z licencji wielostanowiskowych?	40
7 Jak dokupić licencje na kolejne stanowiska?	41
8 Kontynuacja licencji	42
Rozdział XI Porady dotyczące Strażnika	42

1 Jak sprawdzić, czy Strażnik chroni komputer?	42
2 Jak włączyć/wyłączyć Strażnika?	43
3 Jak zmodyfikować ustawienia Strażnika?	43
4 Ikona w zasobniku systemowym	44
Rozdział XII Porady dotyczące skanowania	45
1 Strażnik czy skanowanie?	45
2 Jak uruchomić skanowanie?	46
3 Co się dzieje podczas skanowania?	47
4 Co się dzieje po wykryciu wirusa?	50
5 Wykrycie infekcji z oznaczeniem "not-a-virus"	51
6 Jak działa Kwarantanna?	52
Rozdział XIII Warunki licencji	53

1 Wstęp

Ten podręcznik pomoże Ci zainstalować nowe oprogramowanie G Data Software. Dowiesz się z niego w jaki sposób postępować, aby optymalnie chronić Twój komputer. W kolejnych rozdziałach znajdziesz podstawowe informacje na temat instalacji i funkcjonowania programu, a także odpowiedzi na najczęstsze pytania.

- Instalacja programu: Jak zainstalować program na komputerze?
 - Po instalacji: Co zmieniło się w Twoim systemie po zainstalowaniu programu? Jakie możliwości oferuje program?
 - Pierwsze uruchomienie: Co trzeba zrobić aby program skutecznie chronił komputer? Asystent pierwszego uruchomienia pomoże Ci uaktualnić program i sprawdzić komputer. Możesz wyłączyć asystenta, jeśli wiesz jak wykonać te czynności samodzielnie.
 - Centrum zabezpieczeń: Podstawowy widok okna oprogramowania G Data Software. Umożliwia szybki dostęp do wybranych ustawień i informuje o stanie poszczególnych zabezpieczeń.
 - Porady dotyczące skanowania: Chcesz przeskanować komputer, lub zaplanować automatyczne skanowanie? W tym rozdziale dowiesz się jak to zrobić.
-

- Porady dotyczące Strażnika: Strażnik stale chroni Twój komputer nie wpływając na codzienną pracę. Szczegóły znajdziesz w tym rozdziale.
- Porady dotyczące aktualizacji: Ten rodzaj oprogramowania, jak żaden inny wymaga zwrócenia szczególnej uwagi na temat aktualizacji. Dowiedz się jak postępować aby Twój program był zawsze aktualny.



Jeśli potrzebujesz informacja na temat konkretnej opcji, w każdej chwili możesz kliknąć przycisk Pomoc lub F1 aby otworzyć stronę pomocy odnoszącą się do bieżącego okna.

Odpowiedzi na większość pytań znajdziesz w podręczniku użytkownika lub w pliku pomocy. Warto zajrzeć też na stronę internetową G Data Software i przejrzeć najczęściej zadawane pytania na stronie: www.gdata.pl/pomoc.

2 Pomoc techniczna

Masz problemy z zainstalowaniem programu? Program nie działa? Zgłoś problem do Pomocy technicznej G Data. Aby zgłosić problem do Pomocy technicznej, wyślij wiadomość z opisem problemu. Można również zgłosić

3 G Data Security

problem telefonicznie.

Dobre przygotowanie do rozmowy przyspieszy proces udzielania pomocy i ułatwi kontakt z serwisantem.

- Przygotuj dane klienta (dane dostępu do aktualizacji, Numer rejestracyjny lub Numer klienta)
- Upewnij się, że oprogramowanie G Data Software jest zainstalowane na komputerze
- Zgromadź informacje na temat sprzętu i innego oprogramowania zainstalowanego w komputerze
- Przygotuj kartkę i coś do pisania

e-mail: pomoc@gdata.pl

telefon: 94 3729 650

Odpowiedzi na większość pytań znajdziesz w podręczniku użytkownika lub w pliku pomocy. Warto zajrzeć też na stronę internetową G Data Software i przejrzeć najczęściej zadawane pytania na stronie: www.gdata.pl/pomoc.

3 Instalacja programu

Oprogramowanie G Data Software funkcjonuje prawidłowo na komputerach o następujących parametrach:

- System Windows 7, Vista lub XP (od SP 2)
 - Od 512 MB RAM, dostęp do Internetu
- 1 Aby rozpocząć instalację, włóż płytę z oprogramowaniem G Data Software do napędu komputera. Automatycznie otworzy się okno instalacji. Jeśli nie posiadasz płytki, uruchom plik instalacyjny oprogramowania pobrany przez Internet.
 - 2 Kliknij przycisk Instaluj. Uruchomi się asystent, który przeprowadzi Cię przez cały proces konfigurowania instalacji. Po wybraniu opcji instalacyjnych kliknij przycisk Zakończ. Oprogramowanie zainstaluje się automatycznie. Jeżeli nie posiadasz płytki, asystent instalacji zacznie działać po uruchomieniu pliku instalacyjnego pobranego przez Internet.
 - 3 Jeżeli asystent o to poprosi, pozwól na ponowne uruchomienie komputera przed pierwszym uruchomieniem programu.

Jeżeli chcesz doinstalować lub zainstalować poszczególne składniki programu, uruchom Panel sterowania systemem Windows i skorzystaj z polecenia Zmień dostępne w aplecie Dodaj/Usuń programy (Windows XP) lub Programy i funkcje (Windows 7, Vista).

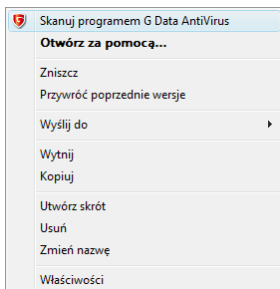
4 Po instalacji



Okno interfejsu oprogramowania G Data Software możesz otworzyć klikając ikonę programu na pulpicie. Widok Centrum zabezpieczeń informuje o stanie poszczególnych modułów zabezpieczających. Szczegóły znajdziesz w rozdziale Centrum zabezpieczeń

Oprócz okna interfejsu programu G Data Software, masz do dyspozycji kilka innych możliwości skorzystania z zainstalowanego oprogramowania:

- **Szybkie skanowanie**
Znalazłeś na dysku podejrzany plik? Chcesz szybko przeskanować plik pobrany z Internetu lub folder? Nie musisz uruchamiać okna programu G Data Software. Kliknij dany plik lub folder prawym klawiszem myszki i wybierz polecenie Skanuj programem G Data AntiVirus.



- Tworzenie płyt startowych
Jeśli Twój komputer jest zarażony wirusami, może się zdarzyć, że nie będziesz w stanie zainstalować oprogramowania antywirusowego w systemie operacyjnym. Niektóre wirusy potrafią do tego stopnia ingerować w system. W takim przypadku możesz skorzystać z opcji skanowania płytą startową G Data. Opis tworzenia i korzystania z płyty startowej znajdziesz w rozdziale: Płyta startowa

5 Pierwsze uruchomienie

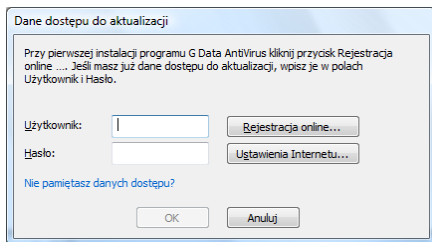
Przy pierwszym uruchomieniu oprogramowania G Data Software otwierają się kolejno dwa okna konfiguracyjne umożliwiające uaktualnienie programu i przeprowadzenie skanowania komputera.

Jeśli nie chcesz oglądać okien konfiguracyjnych przy uruchamianiu programu, zaznacz opcję Nie pokazuj więcej tego okna.

5.1 Pierwsza aktualizacja

Pierwsze okno konfiguracyjne umożliwia przeprowadzenie pełnej aktualizacji oprogramowania G Data Software przez Internet. Aktualizacja jest najważniejszym elementem ochrony wirusowej, gdyż nowe wirusy powstają cały czas. Zadbaj o jak najszybsze przeprowadzenie pierwszej aktualizacji.

- 1 W celu uaktualnienia programu kliknij przycisk Aktualizuj teraz (Zalecane). Pojawi się okno z prośbą o wpisanie danych dostępu do aktualizacji.
- 2 Jeśli jeszcze nie masz danych do aktualizacji, kliknij przycisk Rejestracja online.



Pojawi się okno formularza z prośbą o wpisanie Numeru rejestracyjnego i danych osobowych.

Nie możesz przeprowadzić rejestracji online?

Sprawdź połączenie z Internetem (np. poprzez otwarcie dowolnej strony w przeglądarce internetowej). Jeżeli Twoje połączenie wymaga zmodyfikowania konfiguracji, możesz otworzyć okno ustawień Internetu klikając przycisk Ustawienia Internetu. Szczegóły znajdziesz w rozdziale Problemy z aktualizacją?

- 3 Numer rejestracyjny znajdziesz w opakowaniu z zakupionym oprogramowaniem. Jeżeli dysponujesz licencją zakupioną przez sklep Internetowy, znajdziesz go w wiadomości z realizacją zamówienia.

Wypełnij formularz i kliknij przycisk Rejestracja.

9 G Data Security

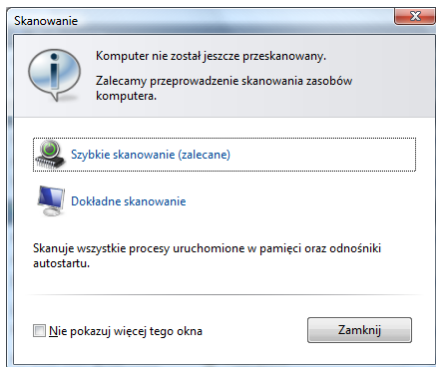
Serwer aktualizacji G Data wygeneruje dane dostępu. Dane zostaną automatycznie wpisane do programu, a także wysłane na podany w formularzu adres e-mail. Kliknij OK, aby zamknąć okno.

- 4 W tym momencie rozpocznie się właściwa aktualizacja danych. Szczegóły aktualizacji można śledzić w oknie aktualizacji. Po zakończeniu procesu kliknij przycisk Zamknij.

Program jest aktualny, ale pamiętaj o regularnych aktualizacjach automatycznych, dzięki którym Twój komputer będzie chroniony. Opis konfiguracji automatycznych aktualizacji w elektronicznej wersji pomocy, w rozdziale Planowanie.

5.2 Pierwsze skanowanie

Skanowanie sugerowane przez asystenta pierwszego uruchomienia umożliwia sprawdzenie, czy w komputerze nie kryją się wirusy. Mogły się dostać do systemu przed zainstalowaniem oprogramowania antywirusowego.



Możesz wykonać Szybkie skanowanie (zalecane) lub Pełne skanowanie komputera. Pełne skanowanie całego komputera może potrwać nawet dłużej niż godzinę, w zależności od ilości danych na dyskach twardej i wydajności komputera.

Szczegóły dotyczące procesu skanowania znajdziesz w rozdziale Co się dzieje podczas skanowania?

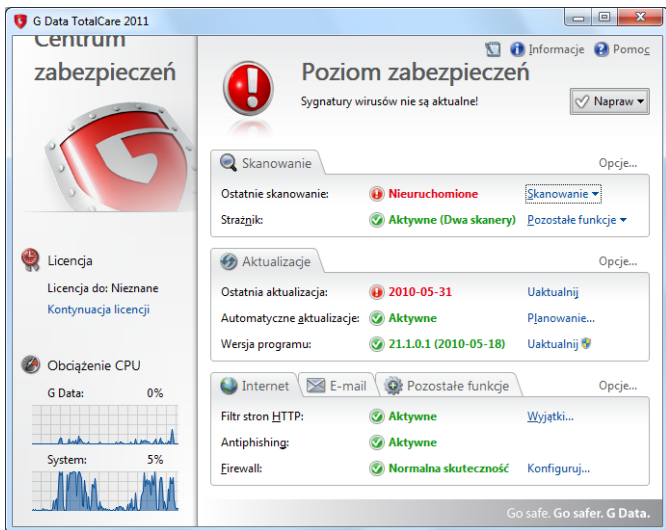
6 Centrum zabezpieczeń

Po zainstalowaniu oprogramowania G Data Software ochrona komputera odbywa się całkowicie automatycznie. Uruchamianie Centrum zabezpieczeń jest niezbędne tylko w celu przeprowadzenia ręcznego skanowania danych lub modyfikacji ustawień.



Warto zajrzeć do Centrum zabezpieczeń jeśli na ikonie programu w zasobniku systemowym pojawi się znak ostrzeżenia, wskazujący na potrzebę ingerencji użytkownika. Szczegóły znajdziesz w rozdziale Ikona w zasobniku systemowym

Widok Centrum zabezpieczeń przedstawia stan poszczególnych składników ochrony w jednym oknie. Odnośniki umożliwiają szybkie przejście do ustawień poszczególnych modułów programu.



6.1 Jak poprawić bezpieczeństwo?

Zarządzanie bezpieczeństwem wcale nie musi być skomplikowane. Często, aby poprawić poziom zabezpieczeń komputera, wystarczy jedno kliknięcie. Ikona Poziomu zabezpieczeń informuje o bieżącym stanie ochrony, a przycisk Napraw umożliwia szybkie podjęcie działań w celu zoptymalizowania ustawień.



Zielony kolor oznacza, że ustawienia zabezpieczeń są optymalne i system jest bezpieczny.



Żółty kolor ikony poziomu zabezpieczeń informuje o potrzebie interwencji w ustawienia. System jest bezpieczny, ale zachodzi konieczność np. uaktualnienia oprogramowania lub przeprowadzenia skanowania.



Czerwony kolor oznacza potencjalne zagrożenie dla systemu operacyjnego. Niezbędna jest natychmiastowa interwencja użytkownika.

Jeżeli wymagana jest ingerencja w ustawienia, przycisk Napraw jest podświetlony. Po kliknięciu przycisku Napraw, oprogramowanie automatycznie zmodyfikuje ustawienia lub podpowie co zrobić, tak aby komputer znów był bezpieczny.

Jeżeli ikona poziomu zabezpieczeń jest w kolorze zielonym, przycisk Napraw wyłącza się i jest wyszarzony.

Po wykonaniu żądanych działań, możesz zamknąć Centrum zabezpieczeń. Najważniejsze funkcje programu dostępne są z poziomu menu kontekstowego ikonki w zasobniku systemowym, bez potrzeby uruchamiania interfejsu użytkownika.

6.2 Co pokazuje Centrum zabezpieczeń?

Centralna część okna Centrum zabezpieczeń podzielona jest na tematyczne sekcje (np. Skanowanie, Aktualizacje). W obrębie każdej sekcji, wyświetlane są informacje dotyczące stanu poszczególnych modułów oprogramowania G Data Software:



Wszystko w porządku.



Zalecana ingerencja w ustawienia.



Bezpośrednie zagrożenie. Niezbędna natychmiastowa interwencja.



Funkcja wyłączona.

Jeśli chcesz zmodyfikować ustawienia dotyczące danej sekcji, kliknij żółtą lub czerwoną ikonkę. Automatycznie otworzy się odpowiednie okno z ustawieniami.

Niebieskie odnośniki w prawej kolumnie umożliwiają szybkie przejście do okien konfiguracji dodatkowych funkcji programu. Dzięki nim możesz szybko ustawić automatyczne aktualizacje, harmonogramy skanowania lub sprawdzić ustawienia wybranych funkcji programu.



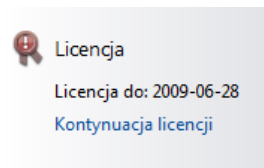
Kliknij przycisk Informacje w prawym, górnym rogu ekranu, aby wyświetlić szczegółowe informacje o zainstalowanej wersji oprogramowania.



Jeśli potrzebujesz informacji na temat konkretnej opcji, w każdej chwili możesz kliknąć przycisk Pomoc lub F1 aby otworzyć stronę pomocy odnoszącą się do bieżącego okna.

6.2.1 Licencja

W lewej części okna znajdziesz informację o czasie pozostałym do końca licencji na oprogramowanie G Data Software. Przed zakończeniem okresu licencyjnego otrzymasz automatyczne powiadomienie mailowe z propozycją wykupienia kontynuacji licencji przez Internet.

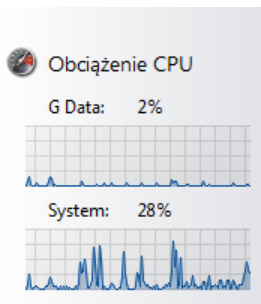


Więcej informacji znajdziesz w rozdziale Kontynuacja licencji

Możesz w każdej chwili odpłatnie rozszerzyć posiadaną licencję na większą ilość komputerów, lub wykupić migrację pakietu do bardziej rozbudowanej wersji. Kliknij odnośnik Rozszerz licencję... aby przejść do strony sklepu internetowego G Data.

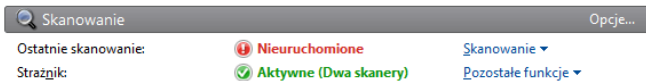
6.2.2 Obciążenie CPU

Wykresy w sekcji Obciążenie CPU obrazują stopień obciążenia komputera przez mechanizmy zabezpieczające. Jeśli obciążenie jest zbyt duże podczas pracy specyficznych, zasobożernych aplikacji (np. baz danych, programów do edycji filmów lub grafiki trójwymiarowej), warto rozważyć ustawienie tych aplikacji jako wyjątków pomijanych przez oprogramowanie antywirusowe. Szczegóły znajdziesz w elektronicznym pliku pomocy, w rozdziale Strażnik.



7 Skanowanie

Sekcja Skanowanie informuje o stanie modułów skanujących. Umożliwia modyfikowanie ustawień związanych z działaniem monitora antywirusowego (Strażnika) i skanowaniem.



Przycisk Opcje... otwiera okno edycji ustawień pogrupowanych w dwóch zakładkach:

- Opcje skanowania
 - Opcje Strażnika
-

7.1 Ostatnie skanowanie

Ten wiersz wyświetla datę ostatnio wykonanego skanowania komputera. Jeśli wiersz jest oznaczony czerwonym symbolem ostrzeżenia, zalecane jest ponowne przeprowadzenie skanowania. Kliknij wiersz z datą ostatniego skanowania, aby uruchomić skanowanie komputera. Po zakończeniu skanowania kolor wiersza zmieni się na zielony.

Szczegóły dotyczące procesu skanowania znajdziesz w rozdziale Co się dzieje podczas skanowania?.

7.1.1 Uruchamianie skanowania

W przypadku podejrzenia infekcji komputera możesz przyprowadzić skanowanie uruchamiając jedno z poleceń sekcji Skanowanie. Jeżeli nie chcesz skanować całego komputera, wybierz jedną z opcji skanowania wybiórczego:

- Skanuj komputer: Polecenie uruchamia skanowanie wszystkich dysków lokalnych oraz obszarów systemowych.
- Pamięć i autostart: Program sprawdzi pliki oraz biblioteki DLL wszystkich bieżących procesów. Pozwoli to usunąć szkodliwe programy z pamięci (jeżeli nie od

razu - zostaną wyeliminowane po kolejnym uruchomieniu komputera). W ten sposób zablokowana zostanie aktywność działających w systemie wirusów, bez potrzeby skanowania całego dysku. Zalecamy regularne przeprowadzanie profilaktycznego skanowania bieżących procesów i autostartu. Proces ten trwa o wiele krócej niż gruntowne skanowanie całego dysku twardego.

- Skanuj foldery pliki: To polecenie umożliwia przeskanowanie wybranych napędów, folderów i plików. Kliknij dwukrotnie tę pozycję aby otworzyć okno wyboru umożliwiające zaznaczenie elementów do przeskanowania.

Po lewej stronie okna wyboru znajduje się drzewo folderów rozwijanych przyciskiem +. Skontrolowany zostanie każdy obiekt zaznaczony haczykiem. Jeśli nie zaznaczysz wszystkich podkatalogów czy plików danego katalogu, wiersz będzie koloru szarego. Czarnymi haczykami oznaczane są foldery skanowane w całości.

- Skanuj nośniki wymienne: Ta funkcja służy do skanowania wymiennych napędów komputera, czyli płyt CD-ROM, DVD-ROM, dyskietek, kart pamięci Flash i pendrive'ów. Uruchomienie tej funkcji spowoduje przeskanowanie wszystkich nośników wymiennych widocznych w systemie. Pamiętaj, że programy nie mogą usuwać wirusów z nośników zabezpieczonych przed zapisem i płyt jednokrotnego zapisu. W przypadku wykrycia wirusa na takim nośniku, program
-

może tylko sporządzić raport z wykrycia.

- Wykrywaj rootkity: Użycie tego polecenia spowoduje uruchomienie narzędzia skanującego system na obecność rootkitów z pominięciem skanowania całego komputera.

Szczegóły dotyczące procesu skanowania znajdziesz w rozdziale Co się dzieje podczas skanowania?.

7.1.2 Opcje skanowania

Okno opcji skanowania pozwala dopasować parametry skanowania danych. Najlepiej przeprowadzać skanowanie komputera w chwili, kiedy nie jest obciążony innymi zadaniami. Umożliwi to wykorzystanie do skanowania wszystkich zasobów systemowych komputera, a tym samym nie będzie przeszkadzać użytkownikowi w pracy.

Do dyspozycji są następujące opcje i parametry:

- Skanery: Program korzysta z dwóch niezależnych skanerów antywirusowych. Optymalne efekty daje zastosowanie obu skanerów. Przy użyciu tylko jednego z nich, proces sprawdzania trwa krócej, ale jest mniej dokładny. Zalecamy ustawienie Dwa skanery. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciąża procesor.

- W razie infekcji: Wybierz reakcję skanera na wykrycie wirusa. Zalecamy wybranie opcji Dezynfekcja (Jeśli niemożliwa: zablokuj dostęp do pliku). Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty ważnych danych lub plików systemowych. Zastosowanie opcji Dezynfekcja (Jeśli niemożliwa: przenieś do Kwarantanny) umożliwi podjęcie decyzji o dalszych działaniach w późniejszym terminie.
- Zainfekowane archiwa: Wybierz reakcję skanera na wykrycie wirusa w archiwach. Wirusy w plikach archiwalnych mogą stanowić zagrożenie dopiero w momencie rozpakowania archiwum. Strażnik wykryje i zablokuje wirusa w momencie uruchomienia dekompresji. Skanowanie archiwów zalecane jest przed przekazaniem lub przesłaniem spakowanych plików innym użytkownikom, jeżeli nie masz pewności, że stosują skuteczne oprogramowanie antywirusowe.
- Wstrzymaj skanowanie na czas aktywności systemu: Ta funkcja spowoduje wstrzymanie skanowanie w momencie przeprowadzania przez system operacyjny innych działań. Skanowanie zostanie automatycznie wznowione w momencie, kiedy komputer znów będzie bezczynny.

Kliknij przycisk Więcej, aby otworzyć okno zaawansowanych ustawień skanowania:

- Rodzaje plików: Strażnik może skanować wszystkie pliki, lub tylko pliki wykonywalne i dokumenty.
-

- **Priorytet skanowania:** Do wyboru są trzy poziomy priorytetu skanowania: wysoki, średni i niski. Skanowanie o wysokim priorytecie przebiega szybciej, ale spowalnia działanie innych aplikacji. Skanowanie o niskim priorytecie trwa dłużej, ale inne aplikacje mogą wtedy swobodnie działać.
- **Heurystyka:** Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmacnia skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.
- **Skanuj archiwa:** Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytyje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.
- **Skanuj pliki e-mail:** Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.
- **Skanuj obszary systemowe:** Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią podstawę systemu operacyjnego, zaleca się skanowanie obszarów systemowych co jakiś czas.

- Wykrywaj dialery / spyware / adware / riskware: To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie może obniżyć poziom bezpieczeństwa systemu.
- Wykrywaj rootkity: Opcja włącza dodatkowy skaner wykrywający rootkity, czyli mechanizmy służące do ukrywania złośliwych programów przed oprogramowaniem zabezpieczającym.
- Skanuj tylko nowe i zmodyfikowane pliki: Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji.
- Twórz raport: Jeśli zaznaczysz pole Twórz raport, program będzie protokołował każdy proces skanowania.

8 Strażnik

Strażnik powinien być zawsze włączony. Tylko wtedy program jest w stanie skutecznie uchronić komputer przed atakami wirusów.

8.1 Opcje Strażnika

Okno opcji Strażnika pozwala skonfigurować sposób monitorowania systemu plików przez Strażnika. W przeciwieństwie do skanowania dysków, opcje Strażnika należy tak dopasować, aby jego działanie jak najmniej obciążało system.

- **Skanery:** Strażnik może korzystać z dwóch niezależnych skanerów antywirusowych. Optymalną ochronę zapewnia zastosowanie dwóch skanerów. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor. Jednak jeśli dysponujesz starszym sprzętem lub mniejszą ilością pamięci, spróbuj wyłączyć skaner dodatkowy. Wydajność pracy komputera na pewno wzrośnie. Sam skaner podstawowy również zapewnia skuteczną ochronę przed wirusami.
- **W razie infekcji:** Wybierz reakcję Strażnika na wykrycie wirusa. Zalecamy wybranie opcji Dezynfekcja (Jeśli niemożliwa: zablokuj dostęp). Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty ważnych danych lub plików systemowych. Zastosowanie opcji Dezynfekcja (Jeśli niemożliwa: przenieś do Kwarantanny) umożliwi podjęcie decyzji o dalszych działaniach w późniejszym terminie.
- **Zainfekowane archiwa:** Wybierz reakcję Strażnika na wykrycie wirusa w archiwach. Zalecamy wybranie opcji Dialog z użytkownikiem. Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty

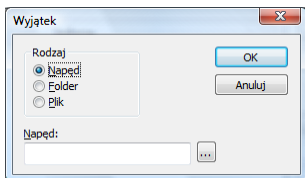
skrzynek pocztowych lub ważnych danych.

Uwaga: Nie należy usuwać ani przenosić do Kwarantanny całych skrzynek pocztowych ani archiwów w przypadku wykrycia wirusa w jednej z wiadomości lub którymś pliku archiwum. Usunięcie pojedynczej wiadomości, można wykonać ręcznie w programie pocztowym.

- Ochrona rejestru i autostartu: Jeżeli opcja chroniąca rejestr jest włączona, oprogramowanie pyta użytkownika o potwierdzenie każdej modyfikacji kluczowych ustawień rejestru lub plików systemowych np. przez instalowane aplikacje. Dzięki włączeniu tej opcji, złośliwe aplikacje nie są w stanie zmodyfikować treści bardzo ważnego pliku systemowego - HOSTS bez wiedzy użytkownika.

Plik HOSTS jest plikiem tekstowym zawierającym zestawienie adresów IP z nazwami komputerów. Zmodyfikowanie tego pliku przez złośliwy program może spowodować przekierowanie przeglądarki na sfałszowane strony internetowe wykorzystujące techniki phishingowe.

W razie potrzeby można wyłączyć spod kontroli Strażnika wskazane napędy, foldery i pliki. Kliknij przycisk Wyjątki aby otworzyć okno wyjątków Strażnika. Aby dodać nowy wyjątek kliknij przycisk Nowy. Wskaż rodzaj obiektu, który chcesz pomijać przy kontroli (napęd, folder lub plik). Przycisk ... otworzy okno wyboru katalogu lub napędu.



Aby utworzyć wyjątek, wykonaj następujące kroki:

- 1 Kliknij przycisk Wyjątki.
- 2 W oknie wyjątków kliknij przycisk Nowy:
- 3 Wybierz rodzaj wyjątku. Można tworzyć wyjątki dla napędów, folderów lub plików.
- 4 W oknie wyboru wskaż obiekt, który chcesz wyjąć spod ochrony Strażnika. Jeżeli tworzysz wyjątek dla pliku, wpisz ręcznie jego nazwę lub zastosuj maskę pliku używając znaków zastępczych.

Dozwolone jest stosowanie następujących znaków zastępczych.

? Symbolizuje dowolny znak.

* Zastępuje dowolny ciąg znaków.

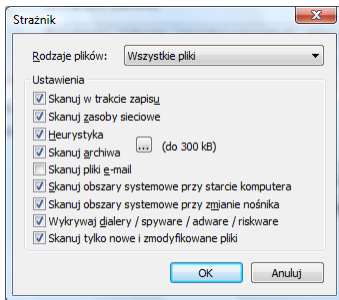
Przykładowo wykluczenie wszystkich plików z rozszerzeniem exe można zdefiniować stosując maskę pliku *.exe. Wyjątki dla różnych plików arkuszy kalkulacyjnych (xlr i xls) można ustawić wpisując tekst *.xl?. Jeżeli nie chcesz, żeby Strażnik skanował pliki, których nazwy rozpoczynają się od konkretnego słowa, np. tekst, wpisz text*.*.

5 Kliknij przycisk OK. Wyjątek pojawi się na liście.

6 Kliknij OK, aby zamknąć okno wyjątków.

Proces można powtarzać wielokrotnie. Można również usuwać i modyfikować zdefiniowane obiekty wyjątków.

Kliknij przycisk Zaawansowane, aby otworzyć okno zaawansowanych ustawień Strażnika.



- Rodzaje plików: Strażnik może skanować wszystkie pliki, lub tylko pliki wykonywalne i dokumenty.
- Skanuj w trakcie zapisu: To ustawienie pozwala wykryć wirusa podczas zapisu lub tworzenia pliku.
- Skanuj zasoby sieciowe: Jeśli komputer jest połączony w sieci z innymi stanowiskami, nie chronionymi przez program antywirusowy, (np. notebook), warto uruchomić opcje kontroli zasobów sieciowych. Strażnik będzie kontrolował zapis i odczyt plików znajdujących się na podłączonych w sieci komputerach. Nie musisz uruchamiać tej opcji, jeżeli Twój komputer nie jest połączony z innymi lub też jeżeli na podłączonych do sieci innych komputerach zainstalowana jest ochrona przed wirusami.
- Heurystyka: Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje

wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmacnia skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.

- Skanuj archiwa: Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.
 - Skanuj pliki e-mail: Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.
 - Skanuj obszary systemowe przy starcie komputera: Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią podstawę systemu operacyjnego, zaleca się skanowanie obszarów systemowych co jakiś czas.
 - Skanuj obszary systemowe przy zmianie nośnika: Obszary systemowe powinny być kontrolowane przy każdej okazji. Mogą być sprawdzane przy starcie komputera, lub przy zmianie nośnika (np. włożenie do napędu nowej płytki CD-ROM).
 - Wykrywaj dialery/spyware/adware/riskware: To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie
-

może obniżyć poziom bezpieczeństwa systemu.

- Skanuj tylko nowe i zmodyfikowane pliki: Skanuj tylko nowe i zmodyfikowane pliki: Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji..

9 Porady dotyczące instalacji

W kolejnych rozdziałach umieszczone zostały praktyczne porady dotyczące instalacji oprogramowania G Data Software.

9.1 Dostępna jest nowa wersja oprogramowania

Jeśli podczas instalowania oprogramowania G Data komputer jest połączony z internetem, instalator automatycznie sprawdza, czy dostępna jest nowsza wersja oprogramowania. Jeśli tak, wyświetla okno z zapytaniem, czy ma pobrać najnowsze pliki przed rozpoczęciem instalacji. Pobieranie odbywa się automatycznie, bez udziału użytkownika.

Istnieje również możliwość uaktualnienia wersji oprogramowania po dokonaniu instalacji, poprzez funkcję dostępną w oknie głównym programu - patrz rozdział Wersja programu.

9.2 Instalacja nie rozpoczyna się automatycznie

Jeśli próbujesz zainstalować program z płyty lub pendrive'a, ale okno startowe nie uruchamia się automatycznie, może to oznaczać, że funkcja automatycznego uruchamiania jest wyłączona lub nie działa prawidłowo.

Uwaga: W systemach operacyjnych Windows Vista i 7 użytkownik musi potwierdzić uruchomienie okna autostartu. W dobrze znanym oknie potwierdzenia, które się pojawi po umieszczeniu nośnika w napędzie, wybierz opcję Uruchom AUTOSTRT.EXE.

Jeśli nie pojawia się żadne okno, przejrzyj zawartość nośnika korzystając z Eksploratora Windows i uruchom plik o nazwie Setup, ew. Setup.exe.

9.3 Inicjatywa G Data Malware Information

Co to jest Inicjatywa G Data Malware Information?

Specjaliści G Data Security Labs rozwijają mechanizmy chroniące Klientów G Data przed złośliwym oprogramowaniem. Skuteczność działania i szybkość tworzenia mechanizmów ochronnych zależy w dużej mierze od posiadanych informacji na temat złośliwego oprogramowania. Informacje na temat szkodliwych programów najlepiej pozyskiwać bezpośrednio z zaatakowanych lub zainfekowanych komputerów. Inicjatywa G Data Malware Information umożliwia przekazywanie informacji na temat zagrożeń. Dzięki przystąpieniu do Inicjatywy, możesz wspomóc zespół specjalistów G Data Security Labs wysyłając informacje o złośliwych programach atakujących Twój komputer. Twój udział w Inicjatywie G Data Malware Information wpłynie bezpośrednio na podniesienie jakości produktów oferowanych przez G Data Software.

Jakie dane zbieramy?

Informacje gromadzone są na dwa sposoby:

1. Użytkownik samodzielnie wysyła szkodliwe oprogramowanie przy pomocy opcji wysyłki plików do Ambulansu G Data. W tym przypadku, wraz z plikami przekazywane są ich oryginalne nazwy, lokalizacje w systemie i daty utworzenia.

2. Automatyczna wysyłka złośliwych plików wykrytych na odwiedzanych stronach internetowych. Do G Data Security Labs wysyłane są następujące informacje:

- Wersja Malware Information
- Numer wersji produktu G Data i używane skanery
- Język systemu operacyjnego
- Adres URL do zablokowanej strony, zawierającej złośliwy kod (malware, phishing itd.)
- Nazwa złośliwego programu

Przesyłane dane nie służą identyfikacji użytkowników zarażonych komputerów. Informacje nie są zestawiane z danymi osobowymi.

W jaki sposób wykorzystujemy dane?

Przechowywanie i obróbka danych odbywa się z poszanowaniem norm dotyczących ochrony danych osobowych, obowiązujących we wszystkich krajach. Szczególny nacisk kładziemy na zabezpieczanie danych przed dostępem osób nieuprawnionych.

Analizowanie danych ma miejsce w pomieszczeniach G Data Security Labs i służy tylko badaniom i wyjaśnianiu zagadnień z zakresu bezpieczeństwa IT. Celem badań jest określenie potencjalnych zagrożeń i rozwijanie mechanizmów ochronnych. Przykładowo, na podstawie

przesyłanych danych tworzone są listy blokowanych stron, statystyki na potrzeby publikacji w fachowej prasie, czy też zestawy reguł stosowane w technologiach zabezpieczających. Udział w Inicjatywie jest dobrowolny, a odmowa udziału nie ma negatywnego wpływu na skuteczność działania produktu G Data. Pamiętaj, że Twój udział w Inicjatywie G Data Malware Information podnosi świadomość zagrożeni, a także skuteczność zabezpieczeń oprogramowania zainstalowanego u wszystkich użytkowników G Data.

9.4 Instalacja pełna czy niestandardowa?

Wybranie pełnej instalacji spowoduje zainstalowanie składników zalecanych dla większości użytkowników. Jeśli chcesz samodzielnie wybrać składniki do instalacji, wybierz instalację niestandardową.



Ta ikonka widnieje przy składnikach, które zostaną zainstalowane.



Ten symbol oznacza, że dany składnik zostanie pominięty.

Program umożliwi zmodyfikowanie składu instalacji także po zakończeniu instalacji. W tym celu wystarczy

rozpocząć instalację ponownie i zaznaczyć pożądane składniki. Nie jest konieczne usuwanie całego pakietu i instalowanie go od nowa.

9.5 Nieprawidłowy numer rejestracyjny

Jeśli masz problem z wpisaniem numeru rejestracyjnego, sprawdź jego poprawność pod kątem typowych podobieństw znaków, np. wielkie I (jak Iza) zamiast cyfry 1, lub małego l (jak lodówka). Inne przykłady to B i cyfra 8, G i cyfra 6, Z i cyfra 2.

9.6 Deinstalacja programu

Najprostszą metodą usunięcia programu z systemu jest skorzystanie z polecenia Usuń w grupie programowej G Data menu Start systemu Windows. Sam proces instalacji przebiega automatycznie.

Alternatywną metodą jest deinstalacja poprzez Panel sterowania systemu Windows.

- Windows XP: Uruchom polecenie menu Start > Panel sterowania. W Panelu sterowania otwórz aplet Dodaj/Usuń programy. Znajdź na liście nazwę zainstalowanego produktu G Data Software, zaznacz ją
-

myszką i kliknij przycisk Usun.

- Windows Vista: Uruchom polecenie menu Start > Panel sterowania. W Panelu sterowania otwórz aplet Programy i funkcje. Znajdź na liście liście nazwę zainstalowanego produktu G Data Software, kliknij ją prawym klawiszem myszki i wybierz polecenie Usun.

Podczas instalacji program zapyta, czy usunąć ustawienia i raporty programu. Jeżeli zamierzasz zainstalować nowszą wersję programu, pozwól na usunięcie tych elementów.

Jeśli w Kwarantannie programu znajdują się zarażone pliki, program zapyta podczas deinstalacji, czy chcesz je usunąć. Jeżeli ich nie usuniesz, będą dostępne w Kwarantannie po zainstalowaniu nowszej wersji programu G Data.

10 Porady dotyczące aktualizacji

Ten rozdział zawiera zestaw porad dotyczących aktualizacji programu.

10.1 Co to są aktualizacje sygnatur wirusów?

Aktualizowanie sygnatur wirusów polega na pobieraniu najnowszej wersji bazy znanych wirusów z serwera aktualizacji do programu antywirusowego. Dzięki regularnie przeprowadzanym aktualizacjom program uczy się rozpoznawać najnowsze szkodliwe programy.

Pracownicy G Data SecurityLabs na bieżąco opracowują najnowsze sygnatury wirusów i przygotowują aktualizacje programu. Z efektów ich pracy korzystasz na co dzień - pobierając uaktualnienia uczące Twój program rozpoznawania najnowszych zagrożeń.

10.2 Jak uaktualnić sygnatury wirusów?

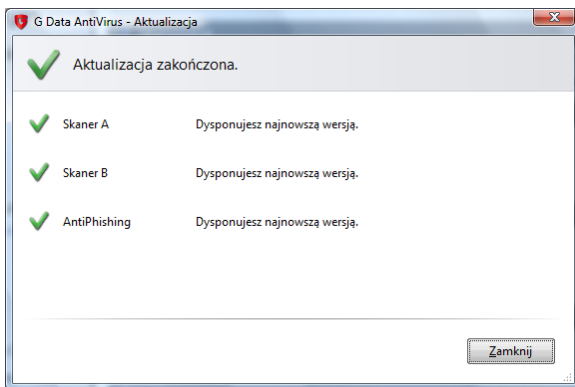
Istnieje kilka sposobów na uaktualnienie sygnatur wirusów.

- Wymuszenie ręcznej aktualizacji: W głównym oknie programu kliknij polecenie Uaktualnij w wierszu Ostatnia aktualizacja sekcji Aktualizacje. Program sam pobierze i zainstaluje pliki zawierające definicje najnowszych wirusów.
 - Automatyczne aktualizowanie sygnatur wirusów: Po zainstalowaniu programu, aktualizacje automatyczne są domyślnie włączone. Jeśli są wyłączone, w wierszu
-

Automatyczne aktualizacje w sekcji Aktualizacje pojawi się czerwony znak ostrzeżenia. Sposób konfigurowania aktualizacji automatycznych opisany jest w rozdziale AktualizacjeAktualizacje.

- Program informuje, że aktualizacja nie została przeprowadzona od dłuższego czasu: Kliknij przycisk Napraw w górnej części okna aby uruchomić aktualizację.

W trakcie przeprowadzania ręcznej aktualizacji otwiera się okno, w którym można śledzić postęp aktualizowania poszczególnych składników programu.



Do przeprowadzenia aktualizacji niezbędne jest połączenie z Internetem.

10.3 Co to jest aktualizacja oprogramowania?

Podobnie jak sygnatury wirusów, można uaktualnić również pozostałe elementy oprogramowania G Data. Do tego służy opcja aktualizacji plików programu.

Uaktualnianie oprogramowania to praktyka stosowana przez wszystkich producentów programów komputerowych. Umożliwia usprawnianie programów, modyfikowanie ich wyglądu, a także poprawianie zawartych w nich błędów.

10.4 Nieprawidłowe lub zagubione dane dostępu

- A Sprawdź dokładnie poprawność danych dostępu. Jeśli dysponujesz wiadomością mailową z danymi, skopiuj je kolejno i wklej do okna programu aby uniknąć potencjalnych błędów przy wpisywaniu. Pamiętaj o zachowaniu pisowni wielkich i małych znaków. Dane dostępu nigdy nie zawierają znaków spacji.

 - B Jeśli nie pamiętasz danych dostępu, lub nie możesz ich odnaleźć, kliknij w programie link Nie pamiętasz danych dostępu?. Link przeniesie Cię na stronę internetową, która po ponownym wpisaniu
-

numeru rejestracyjnego prześle dane dostępu na wcześniej wskazany adres e-mail.

- C Jeśli nie masz dostępu do skrzynki pocztowej (np. z powodu zmiany adresu), skontaktuj się z Pomocą techniczną G Data.

10.5 Jak przenieść licencję na inny komputer?

Po prostu odinstaluj program z jednego komputera i zainstaluj na drugim. Przy próbie aktualizacji program sam zapyta, czy przenieść licencję. Po przeniesieniu licencji poprzedni komputer utraci możliwość pobierania aktualizacji.

10.6 Jak korzystać z licencji wielostanowiskowych?

Licencje wielostanowiskowe umożliwiają korzystanie z jednej licencji na większej ilości komputerów. Rejestracja odbywa się tylko raz - na pierwszym komputerze. Na pozostałych stanowiskach należy wpisać dane dostępu uzyskane w potwierdzeniu rejestracji.

Do czego służy numer rejestracyjny?

Numer rejestracyjny służy do zarejestrowania licencji w celu uzyskania danych dostępu do aktualizacji (Użytkownik i Hasło). Rejestracja danego numeru rejestracyjnego może odbyć się tylko raz.

Dlaczego podczas rejestracji pojawia się komunikat:
Produkt został już zarejestrowany?

Rejestracji można dokonać tylko raz.

Na każdym kolejnym komputerze wystarczy wpisać dane dostępu otrzymane w potwierdzeniu pierwszej rejestracji.

Nie da się zarejestrować danego numeru po raz drugi. Wpisz dane dostępu i kliknij OK, bez otwierania okna Rejestracja online. W razie problemów, skontaktuj się z pomocą techniczną G Data.

10.7 Jak dokupić licencje na kolejne stanowiska?

Aby rozszerzyć licencję skontaktuj się z najbliższym sprzedawcą, kup kolejne licencje w punktach sprzedaży, lub skorzystaj ze sklepu internetowego G Data.

10.8 Kontynuacja licencji

Na niedługo przed upłynięciem licencji na korzystanie z programu, ikonka w zasobniku systemowym pokazuje komunikat o nadchodzącym terminie upływu ważności licencji.

Kliknij dymek, jeżeli chcesz dokonać przedłużenia licencji przez sklep internetowy. Jeśli chcesz zostać przeniesiony na stronę internetową sklepu, kliknij przycisk Zamów.

11 Porady dotyczące Strażnika

Ten rozdział zawiera zestaw porad dotyczących działania monitora antywirusowego.

11.1 Jak sprawdzić, czy Strażnik chroni komputer?



O aktywności Strażnika informuje ikonka programu w zasobniku systemowym. Szczegóły znajdziesz w rozdziale: Ikonka w zasobniku systemowym

11.2 Jak włączyć/wyłączyć Strażnika?

Włączanie i wyłączanie Strażnika możliwe jest z okna głównego interfejsu programu. Prostsza i szybszą metodą jest kliknięcie prawym klawiszem ikonki programu w zasobniku systemowym i wybranie odpowiedniego polecenia z menu kontekstowego ikonki.

Menu kontekstowe ikonki umożliwia wyłączenie Strażnika tylko na określony czas (maksymalnie do kolejnego uruchomienia komputera). Trwałe wyłączenie Strażnika nie jest zalecane, gdyż obniża to w znacznym stopniu skuteczność ochrony komputera.

11.3 Jak zmodyfikować ustawienia Strażnika?

Do normalnej pracy modyfikacja ustawień Strażnika nie jest potrzebna. W szczególnych przypadkach (konfiguracja wyjątków, specjalne zastosowania komputera), modyfikacja ustawień może być konieczna. Aby otworzyć okno ustawień Strażnika kliknij odnośnik Opcje w oknie głównym programu, w sekcji Skanowanie. W oknie opcji kliknij zakładkę Strażnik. Szczegóły na temat ustawień Strażnika znajdziesz w rozdziale Opcje Strażnika.

11.4 Ikonka w zasobniku systemowym

Ikona programu znajduje się w zasobniku systemowym, czyli w prawym, dolnym rogu ekranu (obok zegarka).



Tak wygląda ikonka, jeżeli wszystkie niezbędne funkcje programu są włączone.



Jeżeli któryś z kluczowych składników ochrony jest wyłączony lub nie działa prawidłowo na ikonce pojawia się znak ostrzeżenia.

Dwukrotne kliknięcie ikony powoduje uruchomienie interfejsu programu. Klikając ikonę prawym klawiszem myszy otworzysz menu kontekstowe zawierające kilka podstawowych poleceń.

Menu umożliwia między innymi wyłączenie Strażnika na określony czas. Polecenie Aktualizacja baz wirusów pozwala pobrać najnowsze sygnatury wirusów bez potrzeby uruchamiania okna programu. Z tego miejsca możesz również przejrzeć Statystyki dotyczące wykrytych wirusów, przeskanowanych wiadomości pocztowych i stron internetowych.

Jeśli Twoje oprogramowanie wyposażone jest w składnik Firewall, w menu ikony widnieją dodatkowo polecenia Wyłącz Firewall i Wyłącz autopilota.

Polecenie Wyłącz Firewall pozwala na czasowe wyłączenie zapory sieciowej. Po wyłączeniu zapory komputer nie jest chroniony przed atakami z Internetu. Przy pomocy tej opcji można wyłączyć zaporę maksymalnie do ponownego uruchomienia komputera.

Kliknięcie polecenia Wyłącz autopilota wyłącza mechanizm, który automatycznie zezwala aplikacjom na łączenie się z Internetem. Zapora przełączy się w tryb ręczny i przestanie automatycznie zezwalać programom na łączenie się z internetem.

12 Porady dotyczące skanowania

Ten rozdział zawiera zestaw porad dotyczących skanowania plików.

12.1 Strażnik czy skanowanie?

- Strażnik, czyli monitor antywirusowy skanuje na bieżąco każdy odczytywany lub zapisywany plik na obecność złośliwego oprogramowania. Jest to najważniejszy składnik programu antywirusowego i powinien być zawsze włączony.
 - Skanowanie plików, folderów lub dysków na żądanie to sprawa drugoplanowa. Skanowanie całego komputera zalecane jest po zainstalowaniu programu w systemie,
-

który wcześniej nie był chroniony przez skuteczny program antywirusowy. Warto również przeskanować komputer lub jego foldery systemowe w przypadku, kiedy Strażnik wykryje w plikach wirusa.

12.2 Jak uruchomić skanowanie?

Istnieje kilka sposobów na uruchomienie skanowania danych.

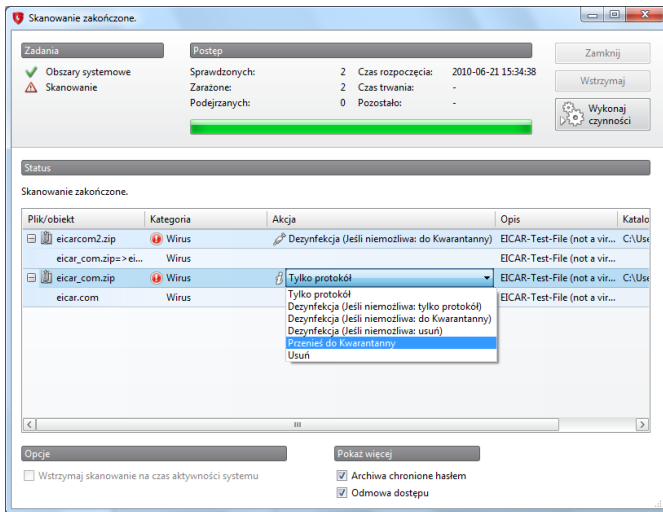
- Ręczne uruchomienie skanowania komputera: Kliknij odnośnik Skanowanie > Skanuj komputer w sekcji Skanowanie głównego okna Centrum zabezpieczeń. Program przeskanuje cały komputer pod kątem obecności wirusów.
- Automatyczne skanowanie według harmonogramu: Jeśli w wierszu Automatyczna aktualizacja w sekcji Aktualizacja widzisz zielone światło, oznacza to, że automat aktualizujący sygnatury wirusów jest włączony. Kliknij odnośnik Planowanie w sekcji Aktualizacja, aby otworzyć okno harmonogramu, umożliwiającego włączanie i wyłączanie automatu, a także dokonywanie ustawień związanych z działaniem automatu.
- Program informuje, że skanowanie nie było wykonywane od dłuższego czasu: Kliknij przycisk Napraw w górnej części okna aby uruchomić skanowanie.

- Skanowanie wybranych zasobów komputera: Jeżeli nie chcesz skanować całego komputera, a jedynie konkretny dysk lub folder, kliknij odnośnik Skanowanie w sekcji dotyczącej skanowania i wybierz jedno z poleceń menu kontekstowego. Opis poszczególnych poleceń znajdziesz w rozdziale Uruchamianie skanowania.
- Skanowanie przy pomocy prawego klawisza myszki: Możesz przeskanować dowolny obiekt (napęd, folder, plik) klikając go w oknie Eksploratora Windows prawym klawiszem myszki i wybierając polecenie Skanuj programem G Data AntiVirus.

12.3 Co się dzieje podczas skanowania?

Skanowanie polega na porównywaniu wszystkich plików objętych skanowaniem z wzorcami wirusów (sygnaturami), którymi dysponuje program antywirusowy. Jeżeli program wykryje w pliku zgodność z jedną z sygnatur, zarejestruje ten fakt jako wykrycie wirusa.

Opis uruchamiania skanowania znajdziesz w rozdziale Jak uruchomić skanowanie?. W trakcie trwania skanowania wyświetlone jest okno skanowania.



W górnej części okna, w sekcji Postęp wyświetlane są statystyki dotyczące procesu skanowania. Pasek postępu wskazuje procent wykonania skanowania komputera. W sekcji status wyświetlana jest ścieżka dostępu oraz nazwa skanowanego w danym momencie pliku. Środkowa część okna przedstawia wyniki skanowania oraz wykryte zagrożenia. Już w tym miejscu masz możliwość podjęcia decyzji, jak postąpić z wykrytymi zagrożeniami.

Przycisk Anuluj umożliwia przerwanie skanowania w dowolnym momencie. Użycie przycisku Wstrzymaj

powoduje tymczasowe wstrzymanie skanowania i pozwala na wznowienie skanowania w dowolnym momencie.

Zaznaczenie opcji Wstrzymaj skanowanie na czas aktywności systemu spowoduje wstrzymanie skanowanie w momencie wykonywania przez system innych działań. Skanowanie zostanie wznowione w momencie, kiedy komputer znów będzie bezczynny.

W sekcji Pokaż więcej możesz zdecydować czy chcesz także oglądać wyniki skanowania dotyczące archiwów, plików, do których program nie ma dostępu i archiwów zabezpieczonych hasłem.

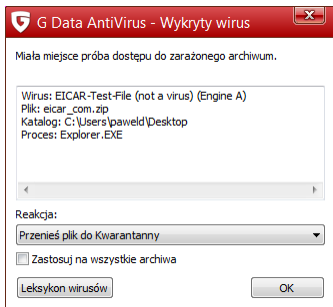
W przypadku wykrycia wirusa program odnotuje ten fakt na liście w oknie skanowania. Po zakończeniu skanowania, można ustalić co program ma zrobić z danym zagrożeniem. Kliknij pole w kolumnie Akcja i wybierz z listy rozwijanej czynność, którą chcesz wykonać. Można ustalić inną akcję dla każdego wykrytego zagrożenia. Po dokonaniu wyboru kliknij przycisk Wykonaj czynności.

Uwaga: Domyślnie dla każdego zagrożenia ustawiona jest reakcja Tylko protokół.

Po wykonaniu wybranych czynności odblokuje się przycisk Zamknij. Kliknij go, aby zamknąć okno skanowania.

12.4 Co się dzieje po wykryciu wirusa?

W przypadku wykrycia wirusa program wyświetla okno zawierające nazwę wirusa, a także lokalizację i nazwę pliku z wykrytym wirusem.



Okno umożliwia podjęcie wybranego działania. W większości przypadków najlepszym rozwiązaniem jest wybranie opcje Przenieś do Kwarantanny). Plik z wirusem zostanie przeniesiony do zaszyfrowanego folderu Kwarantanny. Bezpośrednie usuwanie całego pliku z wirusem może spowodować usunięcie ważnego pliku systemowego lub istotnych danych. Wybranie opcji Zablockuj dostęp do pliku spowoduje że program uniemożliwi uruchamianie i kopiowanie pliku.

Kwarantanna i skrzynki pocztowe

Nie zaleca się przenoszenia do Kwarantanny plików programów pocztowych zawierających całe skrzynki pocztowe (np *.PST, *.DBX). Po przeniesieniu plików poczty do Kwarantanny program pocztowy nie odnajdzie ich w domyślnych lokalizacjach i nie będzie w stanie wyświetlić pobranych wcześniej wiadomości, lub też przestanie działać prawidłowo.

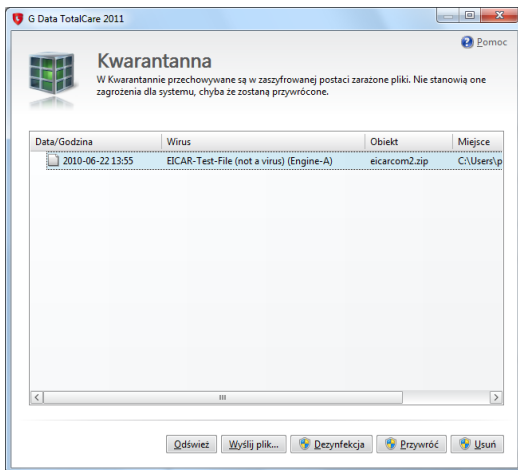
12.5 Wykrycie infekcji z oznaczeniem "not-a-virus"

W ten sposób oznaczane są pliki programów, które choć nie są wirusami, stanowią teoretyczne zagrożenie dla komputera. Same w sobie nie są groźne, ale ich stosowanie może ułatwić przeprowadzenie ataku na komputer. Do takich programów należą między innymi aplikacje do zdalnego zarządzania komputerami przy pomocy protokołu VNC (RealVNC, TightVNC), aplikacje do korzystania z komunikacji IRC, serwery FTP.

Jeżeli są to świadomie używane aplikacje, nie zalecamy usuwania takich plików, ani przenoszenia ich do Kwarantanny, gdyż spowoduje to, że przestaną one funkcjonować poprawnie.

12.6 Jak działa Kwarantanna?

Kwarantanna to zaszyfrowany folder, w którym program przechowuje bezpiecznie zarażone pliki. Nie stanowią one w tej postaci zagrożenia dla systemu. Decyzję, co zrobić z zarażonymi plikami, można w ten sposób odłożyć na później. Zaznacz wybrany plik w folderze Kwarantanny i zdecyduj, czy chcesz go zdezynfekować, przywrócić czy też usunąć.



- **Dezynfekcja:** Jeżeli wirus nie zniszczył zarażonego pliku, program może usunąć kod wirusa i odzyskać dane w oryginalnej postaci. Odzyskane pliki

przenoszone są automatycznie do folderu źródłowego.

- **Przywróć:** Czasem zachodzi konieczność przywrócenia pliku do pierwotnej lokalizacji, pomimo, że nie da się go zdezynfekować gdyż wirus uszkodził jego część. Jeżeli zajdzie potrzeba przywrócenia zarażonego pliku, zaleca się zachowanie wszelkich możliwych środków ostrożności (odłączenie komputera od sieci lokalnej/ Internetu, sporządzenie kopii zapasowych ważnych, niezarażonych danych).
- **Wyślij plik:** Istnieje możliwość przesłania zarażonego pliku z Kwarantanny do Ambulansu G Data. Możesz to zrobić, jeśli masz skonfigurowane konto e-mail w programie pocztowym. Patrz też rozdział: Inicjatywa G Data Malware Infomation.
- **Usuń:** Jeżeli plik nie jest potrzebny, można go po prostu usunąć z Kwarantanny.

13 Warunki licencji

Ogólne warunki licencji użytkowania oprogramowania G Data Security.

1. Przedmiot umowy

Przedmiotem umowy zawartej między firmą G Data Software Sp. z o.o., zwaną dalej Producentem, a Użytkownikiem jest oprogramowanie zabezpieczające

firmy G Data Software zwane dalej Oprogramowaniem. Producent dostarcza Użytkownikowi Oprogramowanie na nośniku danych lub w postaci pliku pobranego ze strony internetowej Producenta. Producent zwraca uwagę na fakt, że technicznie nie jest możliwe wyprodukowanie Oprogramowania współpracującego bezbłędnie z wszystkimi aplikacjami i z każdą kombinacją sprzętowo-programową.

2. Zakres stosowania

Użytkownik otrzymuje proste, niewyłączne i osobiste prawo, zwane dalej Licencją, do używania Oprogramowania na każdym kompatybilnym komputerze pod warunkiem, że Oprogramowanie będzie użytkowane na nie większej niż uzgodniona z Producentem ilości komputerów, maszyn wirtualnych lub sesji terminali. Jeżeli z komputera korzysta więcej niż jedna osoba, Licencja obejmuje wszystkie osoby korzystające z komputera. Użytkownik ma prawo przenieść Oprogramowania z jednego komputera na drugi, przy zachowaniu uzgodnionej z Producentem maksymalnej ilości komputerów.

3. Szczególne ograniczenia

Użytkownik nie może modyfikować Oprogramowania bez pisemnej zgody Producenta.

4. Prawo własności

Zakupując Oprogramowanie Użytkownik nabywa prawo

własności do nośnika z zapisanym Oprogramowaniem, a także czasowe prawo do otrzymywania aktualizacji i pomocy technicznej. Zakup Oprogramowania nie wiąże się z zakupem praw do Oprogramowania. Producent zastrzega sobie w szczególności wszystkie prawa do publikowania, powielania, modyfikacji i eksploatacji Oprogramowania.

5. Powielanie

Oprogramowanie i dokumentacja pisemna chronione są prawem autorskim. Dozwolone jest sporządzenie jednej kopii bezpieczeństwa Oprogramowania; kopia nie może zostać przekazana osobom trzecim.

6. Czas trwania umowy

Umowa zostaje zawarta na czas nieokreślony. Czas trwania umowy nie obejmuje prawa do otrzymywania aktualizacji i pomocy technicznej. Prawo do użytkowania Oprogramowania wygasa automatycznie bez okresu wypowiedzenia w momencie złamania przez Użytkownika któregokolwiek z postanowień tej umowy. Wraz z wygaśnięciem umowy Użytkownik jest zobowiązany do zniszczenia oryginalnego nośnika z Oprogramowaniem oraz dokumentacji pisemnej.

7. Złamanie warunków umowy

Użytkownik ponosi odpowiedzialność za wszystkie szkody poniesione przez Producenta w związku z naruszeniem praw autorskich, wynikłe ze złamania warunków tej

umowy.

8. Zmiany i aktualizacje

Obie strony obowiązującej najnowsza wersja tej umowy. Warunki umowy mogą ulec zmianie w każdej chwili, bez powiadamiania Użytkownika i podawania przyczyn.

9. Gwarancja i odpowiedzialność Producenta:

a) Producent gwarantuje, że w momencie przekazania Oprogramowania pierwotnemu Użytkownikowi, jest ono pozbawione błędów i zdatne do użytku w myśl dołączonej specyfikacji programu.

b) W przypadku stwierdzenia wady nośnika lub pobranego pliku, Użytkownik zobowiązany jest do zgłoszenia reklamacji wraz z dowodem zakupu w terminie do sześciu miesięcy od dnia zakupu.

c) Z przyczyn podanych w punkcie 1. Producent nie gwarantuje bezbłędności Oprogramowania, w szczególności w przypadku niespełnienia przez Oprogramowanie wymogów i oczekiwań użytkownika lub niekompatybilności z wybranymi aplikacjami oraz systemami operacyjnymi. Skutki decyzji zakupu i wyniku zamierzonego oraz niezamierzonego działania Oprogramowania ponosi Użytkownik. Zapis odnosi się również do dołączonej dokumentacji pisemnej. Jeśli Oprogramowanie nie jest zdatne do użytku w myśl punktu 1., Użytkownikowi przysługuje prawo odstąpienia od umowy. Takie samo prawo przysługuje Producentowi,

jeżeli wyprodukowanie Oprogramowania użytecznego w myśl punktu 1. nie jest możliwe.

d) Producent odpowiada tylko za szkody spowodowane umyślnie lub przez rażące zaniedbanie ze strony Producenta. Sprzedawca Oprogramowania nie odpowiada także za szkody spowodowane umyślnie lub przez rażące zaniedbanie sprzedawcy. Maksymalna kwota odszkodowania równa jest kwocie poniesionej przez Użytkownika na zakupienie Oprogramowania.

10. Właściwość sądu

Sądem właściwym dla wszystkich kwestii spornych wynikających bezpośrednio lub pośrednio z warunków umowy jest sąd odpowiedni dla siedziby Producenta.

11. Postanowienia końcowe

Unieważnienie tylko niektórych postanowień tej umowy, nie pociąga za sobą unieważnienia pozostałych postanowień. W miejsce unieważnionego postanowienia stosowane jest inne, aktualne postanowienie o najbardziej zbliżonym celu gospodarczym.

Instalując Oprogramowanie Użytkownik akceptuje powyższe warunki licencji. Akceptując warunki licencji Użytkownik zgadza się na przetwarzanie danych osobowych przez Producenta.

Copyright © 2010 G Data Software AG

Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2010 BitDefender SRL.

Engine B: © 2010 Alwil Software

OutbreakShield: © 2010 Commtouch Software Ltd.

