bitdefender
ANTIVIRUS v10

10th anniversary

Instrukcja obsługi

Antywirus

Antyspyware

bitdefender
secure your every bit

BitDefender Antywirus v10

Instrukcja obsługi

BitDefender

Data wydania 2007.06.14
Version 10.2

Uwagi Prawne


bitdefender
secure your every bit

Spis treści

Licencja i Gwarancja

JEŻELI NIE ZGADZASZ SIĘ NA NINIEJSZE WARUNKI NIE INSTALUJ OPROGRAMOWANIA. WYBIERAJĄC "AKCEPTUJĘ", "OK", "DALEJ", "TAK" LUB INSTALUJĄC ALBO UŻYTKUJĄC NINIEJSZE OPROGRAMOWANIE W DOWOLNY SPOSÓB, WSKAZUJESZ NA CAŁKOWITE ZROZUMIENIE I AKCEPTACJĘ WARUNKÓW NINIEJSZEJ UMOWY.

Niniejsze warunki obejmują rozwiązania i usługi BitDefender dla użytkowników domowych licencjonowane dla użytkownika, w tym związaną dokumentację oraz wszelkie aktualizacje i modyfikacje dostarczonych aplikacji w ramach zakupionej licencji lub wszelkie związane umowy serwisowe zgodnie z definicją w dokumentacji oraz wszelkich kopiach.

Ta umowa licencyjna jest prawnym porozumieniem pomiędzy tobą (osobą indywidualną lub prawną), a firmą SOFTWIN dotyczącym użytkowania określonego powyżej oprogramowania SOFTWIN, które obejmuje oprogramowanie komputerowe i usługi oraz może obejmować związane media, drukowane materiały oraz dokumentację „Online" lub elektroniczną („BitDefender"), które chronione są przez amerykańskie i międzynarodowe prawa autorskie oraz międzynarodowe traktaty. Przez zainstalowanie, kopiowanie lub inne użytkowanie programu BitDefender wyrażasz zgodę na związanie się warunkami tej umowy.

Jeżeli nie zgadzasz się na warunki tej umowy, nie instaluj, ani nie używaj programu BitDefender.

Licencja BitDefender. BitDefender jest chroniony przez prawa autorskie, międzynarodowe umowy dotyczące praw autorskich oraz inne przepisy i umowy dotyczące własności intelektualnej. BitDefender jest licencjonowanym produktem i nie podlega dalszej sprzedaży.

PRZYZNANIE LICENCJI. Firma SOFTWIN udziela tobie i tylko tobie innym osobom następującej niewyłącznej, ograniczonej, nie podlegającej przeniesieniu, zachowującej opłaty licencyjne, licencji do korzystania z BitDefende:

OPROGRAMOWANIE APLIKACYJNE. Możesz instalować i korzystać z BitDefender na tak wielu komputerach jak to konieczne, z uwzględnieniem ograniczeń wynikających z całkowitej liczby zakupionych licencji. Możesz wykonać jedną dodatkową kopię jako kopię zapasową.

LICENCJA UŻYTKOWNIKA NA KOMPUTERZE. Licencja niniejsza dotyczy oprogramowania BitDefender, które może być zainstalowane na pojedynczym komputerze, który nie zapewnia usług sieciowych. Każdy pierwszy użytkownik może

zainstalować to oprogramowanie na pojedynczym komputerze i może wykonać jedną dodatkowa kopię na innym urządzeniu jako kopię zapasową. Dopuszczalna ilość pierwotnych użytkowników jest liczbą użytkowników licencji.

WARUNKI LICENCJI. Przyznana licencja rozpoczyna się od daty zakupu programu BitDefender i wygasa na koniec okresu, na jaki została zakupiona.

UAKTUALNIENIA. Jeżeli BitDefender jest oznakowany jako uaktualnienie, musisz posiadać odpowiednią licencję na użytkowanie produktu określonego przez firmę SOFTWIN jako uprawnionego do uaktualnień produktu BitDefender. Uaktualnienie BitDefender zastępuje i/lub uzupełnia produkt stanowiący podstawę aktualizacji. Takiego produktu możesz używać tylko zgodnie z warunkami zawartymi w umowie licencyjnej. Jeżeli BitDefender jest uaktualnieniem części pakietu oprogramowania, na który masz przyznaną licencję jako na pojedynczy produkt, BitDefender może być użytkowany i przesyłany wyłącznie jako część takiego pojedynczego pakietu i nie może być przekazywany do użytkowania na więcej niż jednym stanowisku komputerowym. Warunki niniejszej licencji zastępują wszelkie poprzednie umowy, które mogą istnieć między tobą i SOFTWIN dotyczące oryginalnego produktu lub wynikowego produktu zaktualizowanego.

PRAWA AUTORSKIE. Wszystkie prawa, tytuły własności i korzyści z i do BitDefender oraz wszelkie prawa autorskie BitDefender (włączając, ale nie ograniczając wyłącznie do zdjęć, logo, animacji, wideo, audio, muzyki, tekstu i apletów zawartych w BitDefender), towarzyszące materiały wydrukowane i wszelkie kopie BitDefender są własnością SOFTWIN. BirDefender jest chroniony przez prawa autorskie i klauzule traktatów międzynarodowych. Dlatego też musisz taktować BitDefender jak każdy inny materiał objęty prawem autorskim. Nie możesz kopiować drukowanych materiałów BitDefender. Kopiując musisz uwzględniać wszystkie uwagi dotyczące praw autorskich w ich pierwotnej i oryginalnej postaci we wszystkich kopiach utworzonych, bez względu na formę w jakiej BitDefender występuje. Nie możesz udzielać sublicencji, wypożyczać, sprzedawać, oddawać w leasing lub współdzielić licencji BitDefender. Nie możesz: wykonywać inżynierii wstecznej, kompilować ponownie, dezasemblować, tworzyć produktów pochodnych, modyfikować, tłumaczyć lub próbować poznać kod źródłowy programu BitDefender.

OGRANICZENIA GWARANCJI. SOFTWIN gwarantuje, że nośnik, na którym BitDefender jest rozprowadzany będzie pozbawiony błędów przez okres trzydziestu dni od daty dostarczenia tobie BitDefender. SOFTWIN może według swojego uznania, w ramach gwarancji, jedynie wymienić uszkodzony nośnik na wolny od wad po otrzymaniu uszkodzonego, lub zwrócić pieniądze zapłacone za BitDefender. SOFIWIN nie gwarantuje, że BitDefender będzie pracował nieprzerwanie, będzie wolny od błędów lub, że błędy zostaną naprawione. SOFTWIN nie gwarantuje, że BitDefender spełni twoje oczekiwania.

ZA WYJĄTKIEM, KIEDY JEST TO WYRAŹNIE OKREŚLONE W NINIEJSZEJ UMOWIE, SOFTWIN NIE UWZGLĘDNIA INNYCH GWARANCJI WYRAŹNYCH LUB DOMNIEMANYCH DOTYCZĄCYCH PRODUKTU, UDOSKONALEŃ, KONSERWACJI LUB WSPARCIA LUB WSZELKICH INNYCH MATERIAŁÓW (MATERIALNYCH LUB NIEMATERIALNYCH) LUB USŁUG DOSTARCZANYCH Z PRODUKTEM. SOFTWIN NINIEJSZYM WYRAŹNIE WYŁĄCZA WSZELKIE DOMNIEMANE GWARANCJE I WARUNKI, W TYM BEZ OGRANICZEŃ DOMYŚLNE GWARANCJE PRZYDATNOŚCI DO SPRZEDAŻY, PRZYDATNOŚCI DO OKREŚLONEGO CELU, TYTUŁU, NIEZAKŁÓCANIA, DOKŁADNOŚCI DANYCH, DOKŁADNOŚCI ZAWARTOŚCI INFORMACYJNEJ, INTEGRACJI SYSTEMU ORAZ BRAKU NARUSZENIA PRAW STRON TRZECICH PRZEZ FILTROWANIE, DEASEMBLIZACJĘ LUB USUWANIE OPROGRAMOWANIA STRON TRZECICH, SPYWARE, ADWARE, CIASTECZEK, EMAILI, DOKUMENTÓW, OGŁOSZEŃ LUB PODOBNYCH, NIEZALEŻNIE OD TEGO CZY WYNIKA Z PRZEPISÓW, PRAWA, SPOSOBU PROWADZENIA DZIAŁALNOŚCI, ZWYCZAJU I PRAKTYKI LUB ZASTOSOWANIA HANDLOWEGO.

ZRZECZENIE SIĘ ODPOWIEDZIALNOŚCI ZA USZKODZENIA: Ktokolwiek użytkuje, testuje lub ocenia BitDefender, ponosi całkowite ryzyko wynikające z jakości i działania BitDefender. W żądnym przypadku SOFTWIN nie będzie ponosił odpowiedzialności za jakiekolwiek uszkodzenia, w tym bezpośrednie lub pośrednie uszkodzenia wynikające z użytkowania, działania lub dostarczania BitDefender, nawet jeśli SOFTWIN był poinformował o istnieniu lub możliwości pojawienia się takich uszkodzeń. NIEKTÓRE STANY NIE POZWALAJĄ OGRANICZAĆ LUB WYKLUCZAĆ ODPOWIEDZIALNOŚCI ZA PRZYPADKOWE LUB UMYŚLNE USZKODZENIA. TAK WIĘC POWYŻSZE OGRANICZENIA LUB WYKLUCZENIA MOGĄ NIE DOTYCZYĆ CIEBIE. W ŻADNYM PRZYPADKU ODPOWIEDZIALNOŚĆ SOFTWIN NIE MOŻE PRZEKROCZYĆ CENY ZAKUPU PRODUKTU BITDEFENDER. Ograniczenia poruszone wyżej będą miały zastosowanie bez względu na to czy akceptujesz, użytkujesz, oceniasz czy testujesz BitDefender.

WAŻNA INFORMACJA DLA UŻYTKOWNIKÓW. TO OPROGRAMOWANIE NIE JEST ODPORNE NA BŁĘDY I NIE JEST ZAPROJEKTOWANE DO PRACY W NIEBEZPIECZNYM ŚRODOWISKU WYMAGAJĄCY DZIAŁANIA LUB PRACY SAMOISTNIE BEZPIECZNEJ. OPROGRAMOWANIE NIE JEST PRZEZNACZONE DO UŻYTKU W OBSŁUDZE NAWIGACJI LOTNICZEJ, OBIEKTÓW NUKLEARNYCH LUB SYSTEMACH KOMUNIKACJI, SYSTEMACH UZBROJENIA, SYSTEMACH BEZPOŚREDNIEGO LUB POŚREDNIEGO ZABEZPIECZENIA ŻYCIA, KONTROLI RUCHU LOTNICZEGO LUB JAKIEJKOLWIEK APLIKACJI BĄDŹ INSTALACJI, KTÓRYCH BŁĄD MÓGŁBY SPOWODOWAĆ ŚMIERĆ, E OBRAŻENIA FIZYCZNE LUB USZKODZENIE WŁASNOŚCI.

UWAGI OGÓLNE. Niniejsza umowa będzie regulowana przez prawo rumuńskie oraz przez międzynarodowe umowy i traktaty dotyczące praw autorskich. Wyłącznym

miejscem jurysdykcji i realizacji czynności prawnych mających na celu rozstrzygnięcie wszystkich sporów powstałych w wyniku warunków niniejszej licencji będą sądy rumuńskie.

Ceny, koszty i opłaty za korzystanie z programu BitDefender podlegają zmianom bez uprzedniej informacji.

W przypadku nieważności któregokolwiek postanowienia niniejszej Umowy, nieważność ta nie ma wpływu na ważność pozostałych części Umowy.

BitDefender i logo BitDefender są zastrzeżonymi znakami towarowymi SOFTWIN. Wszystkie pozostałe zastrzeżone znaki towarowe używane w produkcie lub materiale towarzyszącym należą do odpowiednich właścicieli.

Ważność licencji wygasa natychmiast i bez uprzedzenia w przypadku naruszenia któregokolwiek warunku. Użytkownik nie będzie uprawniony do zwrotu kosztów od SOFTWIN lub jakiegokolwiek sprzedawcy BitDefender w przypadku wygaśnięcia ważności. Po wygaśnięciu ważności nadal obowiązują warunki dotyczące poufności oraz ograniczeń użytkowania.

SOFTWIN może w dowolnym momencie dokonać zmiany niniejszych warunków, a nowe warunki będą automatycznie obowiązywać dla odpowiednich wersji oprogramowania dystrybuowanego ze zmienionymi warunkami. W przypadku stwierdzenia nieważności lub nieobowiązywania którejkolwiek z części niniejszych warunków, nie ma to wpływu na obowiązywanie pozostałych warunków, które pozostaną ważne i obowiązujące.

W przypadku niejasności lub niespójności między tłumaczeniami niniejszych warunków na inne języki, pierwszeństwo ma wersja angielska wydana przez SOFTWIN.

Skontaktować się z SOFTWIN, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Rumunia lub nr tel. 40-21-2330780 albo faks:40-21-2330763, adres e-mail: <office@bitdefender.com>.

Wstęp

Ta instrukcja obsługi przeznaczona jest dla wszystkich użytkowników, którzy wybrali **BitDefender v10 Standard** jako narzędzie bezpieczeństwa dla swojego komputera. Informacje przedstawione w tej instrukcji są przeznaczone zarówno użytkownikom zaawansowanym jak i początkującym.

Instrukcja obsługi pozwoli przejść krok po kroku przez cały proces instalacji **BitDefender v10 Standard**, nauczy jak należy go skonfigurować oraz metod użytkowania, sposobu aktualizacji i testowania. Będą mogli Państwo skorzystać z tego, co najlepsze w BitDefender.

Życzymy Państwu miłej i owocnej lektury.

1. Znaki umowne stosowane w instrukcji

1.1. Konwencje typograficzne

Dla poprawy czytelności instrukcji użyto kilka rodzajów czcionki. Ich wygląd i znaczenie zostały przedstawione w poniższej tabeli.

Wygląd	Opis
`sample syntax`	Przykłady i niektóre dane liczbowe są wydrukowane czcionką `szeryfową`.
http://www.bitdefender.com	Linki URL odnoszą do innych miejsc takich jak serwery http czy ftp.
`<support@bitdefender.com>`	Adresy Email zostały umieszczone w tekście dla informacji kontaktowych.
„Wstęp” (p. xiii)	Jest to odnośnik do linka wewnętrznego umiejscowionego w dokumencie.
`filename`	Pliki i foldery są wydrukowane czcionką `szeryfową`.
option	Wszystkie opcje są wydrukowane **pogrubioną czcionką**.
`sample code listing`	Kody są wydrukowane czcionką `szeryfową`.

1.2. Uwagi

Uwagi, są to notatki graficznie wyróżnione, zwracające Państwa uwagę na dodatkowe informacje odnoszące się do aktualnego paragrafu.

Notatka

Wskazówka jest krótką poradą. Zawierają one użyteczne informacje, takie jak specyficzne funkcje lub odnośnik do podobnego tematu.

WAŻNE

Ten znak wymaga Państwa uwagi i jego pomijanie nie jest zalecane. Zazwyczaj nie są to wiadomości krytyczne, ale znaczące.

Ostrzeżenie

Zaznacza wiadomości krytyczne, które należy uważnie przeczytać. Nic złego nie może się stać jeśli podążasz za tymi wskazówkami. Trzeba je przeczytać i zrozumieć, ponieważ znak ten opisuje ryzykowną operacje.

2. Struktura instrukcji

Instrukcja składa się z siedmiu części, zawierających główne tematy: O produkcie, Instalacja, Opis i funkcje, Konsola zarządzająca, Dobre rady, Dysk ratunkowy i Otrzymywanie pomocy. Ponadto dostarczony jest bogaty słownik, który rozjaśni niektóre techniczne zwroty.

O produkcie. Krótkie wprowadzenie do BitDefender.

Instalacja produktu. Instalacja BitDefendera na komputerze krok po kroku. Jest to prosty samouczek instalacji i konfiguracji **BitDefender Antywirus v10**. Instrukcje rozpoczynają się wymaganiami dla poprawnej instalacji, a następnie zostaniecie poprowadzeni przez cały proces instalacji. Ostatecznie zostały opisane procedury odinstalowania na wypadek konieczności usunięcia BitDefender.

Opis i funkcje. BitDefender Antywirus v10, jego funkcje i moduły.

Konsola zarządzająca. Opis podstawowego zarządzania i obsługi BitDefender. Rozdziały te wyjaśniają szczegółowo wszystkie opcje **BitDefender Antywirus v10**, jak skanować komputer, jak zarejestrować program i jak wykonywać aktualizacje wszystkich modułów.

Zasady dobrego postępowania. Podążaj za instrukcją aby jak najlepiej skonfigurować BitDefender'a.

Dysk Ratunkowy BitDefender. Opis dysku ratunkowego programu BitDefender. Ułatwia zrozumienie i korzystanie z funkcji umożliwiającej uruchamianie systemu operacyjnego płyty CD.

Otrzymywanie pomocy. Gdzie zajrzeć i kogo zapytać o rade kiedy coś idzie nie tak, jak powinno.

Słownik. Słownik zawiera terminy techniczne, które pojawiają się w tej instrukcji.

3. Komentarze

Prosimy o pomoc w udoskonalaniu instrukcji. Testowaliśmy i sprawdzaliśmy wszystkie informacje. Proszę do nas pisać o wszystkich błędach jakie znajdziecie w tej instrukcji lub waszych pomysłach jak ją ulepszyć. Z pewnością pomoże nam to stworzyć jak najlepszą dokumentację.

Prosimy wysyłać maile na adres<documentation@bitdefender.com>.

WAŻNE

Wszystkie maile związane z dokumentacją prosimy pisać w języku angielskim.

O produkcie

1. Czym jest BitDefender?

BitDefender jest przodującym rozwiązaniem bezpieczeństwa, które zaspokaja potrzeby dzisiejszych środowisk komputerowych. Firma dostarcza jedno z najszybszych i najbardziej wydajnych rozwiązań programowych, ustalając nowe standardy zapobiegania zagrożeniom. BitDefender dostarcza oprogramowanie do ponad 41 milionów odbiorców domowych i korporacyjnych w ponad 180 krajach. BitDefender posiada biura w **Stanach Zjednoczonych**, **Wielkiej Brytanii**, **Niemczech**, **Hiszpanii** i **Rumunii**.

- Funkcje antywirusa, firewalla, antyspyware'a, antyspama oraz ochrony rodzicielskiej dla użytkowników korporacyjnych i domowych.
- Gama produktów BitDefender implementuje się we wszystkich strukturach informatycznych(stacje robocze, serwery plików, serwery pocztowe i bramki internetowe) w środowiskach Windows, Linux oraz FreeBSD.
- Światowa dystrybucja, produkty dostępne w 18 językach;
- Łatwy w użyciu, posiada konfiguratora instalacji który prowadzi użytkownika przez proces instalacji zadając tylko kilka pytań;
- Międzynarodowe certyfikaty: Virus Bulletin, ICSA Labs, Checkmark, IST Prize, itd;
- 24 godzinna opieka nad klientami - dostępność 24 godziny, 7 dni w tygodniu;
- Szybka reakcja na nowe zagrożenia;
- Najlepszy współczynnik wykrywalności;
- Cogodzinne aktualizacje sygnatur - automatyczne lub zaplanowane - zapewniające ochronę przed najnowszymi wirusami.

1.1. Dlaczego BitDefender?

Udowodnione. Najszybciej reagujący antywirus. Szybka reakcja BitDefender'a została potwierdzona podczas głośnych ostatnio epidemii wirusów CodeRed, Nimda, Sircam i Badtrans.B. BitDefender jako pierwszy udostępnił szczepionki w internecie całkowicie za darmo dla wszystkich zainteresowanych. Obecnie, wraz z szybkim rozprzestrzenianiem się Wirusa Klez, w wielu jego wersjach, ochrona antywirusowa BitDefender została uznana za niezwykle skuteczną dla każdego systemu komputerowego.

Innowacje. Nagroda za innowacje przyznana przez Organizacje Europejskie i EuroCase. BitDefender został ogłoszony zwycięzcą europejskiej nagrody IST, przyznanej przez Organizacje Europejskie i reprezentantów 18 akademii w Europie. Po raz ósmy europejska nagroda IST, jest uhonorowaniem nowego produktu, który najlepiej przedstawia innowacje w dziedzinie technologii informatycznej.

Wszechstronność. Zabezpiecza każdy punkt Twojej sieci, zapewniając całkowite bezpieczeństwo. Rozwiązania bezpieczeństwa BitDefender dla korporacyji spełniają wymogi ochrony dzisiejszego środowiska biznesu, umożliwiając kompleksowe zarządzanie wszystkimi zagrożeniami, które zagrażają wszystkim rodzajom sieci.

Niezawodna Ochrona. Ostateczna zapora dla wszystkich możliwych zagrożeń systemów komputerowych. Wykrywalność podstawowych wirusów za pomocą analizy kodów nie zawsze dowodzi swoją skuteczność, BitDefender ma zaimplementowaną podstawową ochronę, opartą na zachowaniach podejrzanych kodów, dostarczając zabezpieczenie przeciw nowopowstałym złośliwym programom.

Oto **koszty**, których organizacje chcą uniknąć i powody, dla których produkty bezpieczeństwa są projektowane:

- Ataki Robaków
- Utrata komunikacji z powodu zainfekowanych emaili
- Przerwy w działaniu poczty elektronicznej
- Czyszczenie i odzyskiwanie systemów
- Utrata produktywności przez nieużywanie systemu z powodu jego niedostępności
- Hakerzy i nieautoryzowany dostęp, który może spowodować szkody

Niektóre użyteczne funkcje dostępne w pakiecie BitDefender:

- Zwiększenie dostępności sieci poprzez zatrzymanie rozprzestrzeniania się ataków złośliwych programów (takich jak Nimda, Konie Trojańskie, DDoS).
- Zdalna Ochrona użytkowników.
- Obniżenie kosztów administrowania z możliwością szybkiego zarządzania przy pomocy BitDefender Enterprise.
- Zatrzymanie rozprzestrzeniania się oprogramowania złośliwego za pośrednictwem poczty elektronicznej przy pomocy rozwiązań BitDefender dla bram internetowych. Czasowe lub stałe blokowanie nieautoryzowanych połączeń za pomocą kosztownych aplikacji.

Więcej informacji na temat BitDefendera znajdziecie Państwo na stronie: http://www.bitdefender.com.

Instalacja produktu

2. Instalacja BitDefender Antywirus v10

Dział **Instalacja BitDefender Antywirus v10** tej instrukcji zawiera następujące tematy:

- Wymagania systemowe
- Etapy instalacji
- Kreator Instalacji
- Aktualizacja
- Usuwanie, naprawa lub modyfikowanie modułów BitDefender

2.1. Wymagania systemowe

Aby zapewnić prawidłowe działanie produktu, należy sprawdzić przed instalacją czy spełnione są następujące wymagania:

Microsoft Windows 98 SE / NT-SP6 / Me / 2000 / XP 32-bit

- Procesor Pentium II 350 MHz lub lepszy
- Minimum 128 MB pamięci RAM Memory (zalecane 256 MB)
- Minimum 60 MB wolnego miejsca na twardym dysku
- Internet Explorer 5.5 lub nowsza wersja

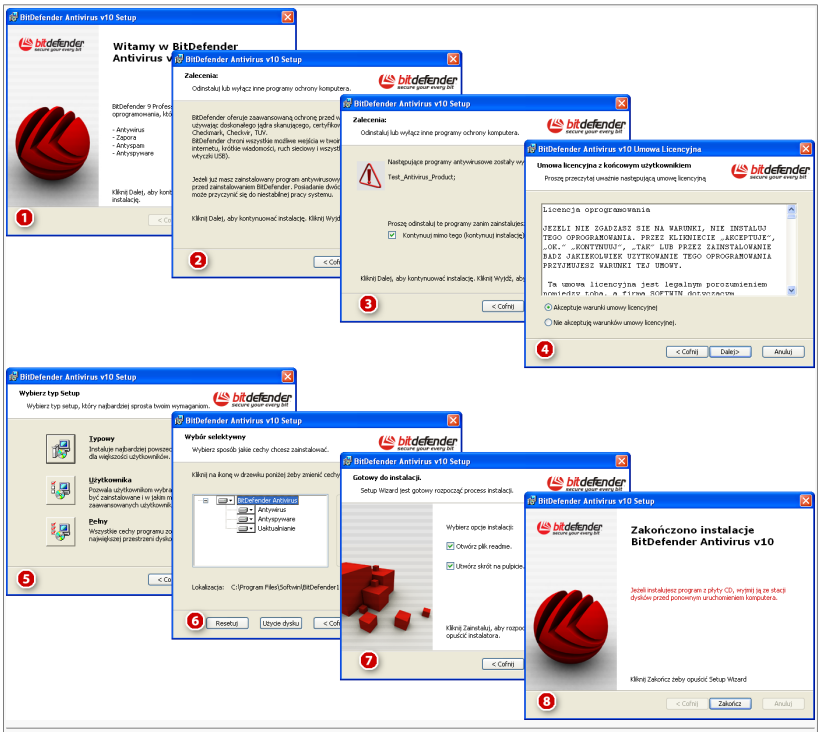
Microsoft Windows Vista 32-bit

- Procesor Pentium 800 Mhz lub wyższy
- Minimum 512 MB pamięci RAM (zalecane 1 GB)
- Minimum 60 MB wolnego miejsca na twardym dysku

BitDefender Antywirus v10 można pobrać ze strony SOFTWIN http://www.bitdefender.com

2.2. Etapy instalacji

Odnajdź plik setup i kliknij na niego dwa razy. Uruchomi się kreator instalacji produktu, który poprowadzi cię przez proces instalacji:



Etapy instalacji

1. Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** jeżeli chcesz opuścić kreatora.
2. Kliknij **Dalej** aby kontynuować lub kliknij **Cofnij** aby powrócić do pierwszego kroku.
3. BitDefender Antywirus v10 zaalarmuje jeżeli masz zainstalowane inne produkty antywirusowe.

Ostrzeżenie

Zalecamy odinstalowanie innych produktów antywirusowych przed instalacją BitDefender'a. Uruchomienie dwóch lub więcej produktów antywirusowych na jednej stacji blokuje system operacyjny.

Kliknij **Cofnij** aby powrócić do poprzedniego kroku lub kliknij **Anuluj** aby opuścić instalację. Jeżeli chcesz kontynuować, kliknij**Dalej**.

Notatka

Jeżeli BitDefender Antywirus v10 nie wykryje innych produktów antywirusowych pominiesz ten krok.

4. Proszę przeczytać Umowę Licencyjną, wybierz **Akceptuję Warunki Zawarte w Umowie Licencyjnej** i kliknij **Dalej**. Jeżeli nie zgadzasz się z warunkami umowy kliknij **Anuluj**. Proces instalacji zostanie zakończony i wyjdziesz z kreatora instalacji programu.
5. Możesz wybrać rodzaj instalacji jaki chcesz wykonać: typową, użytkownika lub pełną.

   Typowa
   Program zostanie zainstalowany z najbardziej typowymi opcjami. Jest ona zalecana dla większości użytkowników.

   Użytkownika
   Możesz dokonać wyboru elementów jakie mają być zainstalowane. Jest ona zalecana wyłącznie dla zaawansowanych użytkowników.

   Pełna
   Program zostanie zainstalowany ze wszystkimi dostępnymi elementami.

   Jeżeli wybierzesz instalację **Typowa** lub **Pełna** pomiń 6 krok.
6. Jeżeli wybrałeś instalację **Użytkownika**, zostanie wyświetlone okno zawierające wszystkie komponenty BitDefender. Możesz wybrać te, które chcesz zainstalować.

   Jeżeli klikniesz nazwę elementu, po prawej stronie pojawi się jego krótki opis (zawierający informacje o wymaganej minimalnej przestrzeni dyskowej na twardym dysku). Jeżeli klikniesz na ikonę elementu pojawi się okno, w którym będziesz mógł wybrać instalację danych modułów.

   Możesz wybrać folder, w którym chcesz zainstalować produkt. Domyślny folder jest zlokalizowany następująco `C:\Program Files\Softwin\BitDefender 10`.

   Jeżeli chcesz wybrać inny folder, kliknij **Przeglądaj** i wybierz dany folder. Kliknij **Dalej**.
7. Domyślnie masz wybrane dwie opcje:
   - **Otwórz plik readme** - aby otworzyć plik readme na końcu instalacji.
   - **Utwórz skrót na pulpicie** - aby umieścić skrót do BitDefender Antivirus v10 na pulpicie na końcu instalacji.
   - **Wyłącz Windows Defender** wyłącza Windows Defender; opcja ta pojawia się tylko w Windows Vista.

   Kliknij **Instaluj** aby rozpocząć instalację programu.

WAŻNE

Podczas instalacji pojawi się kreator. Pomoże on zarejestrować Twój **BitDefender Antywirus v10**, stworzyć konto oraz skonfigurować najważniejsze zadania ochrony. Po zakończeniu pracy z kreatorem przejdziesz do następnego kroku.

8. Kliknij **Zakończ** aby zakończyć instalację programu. Jeżeli zaakceptowałeś ustawienia domyślne dla ścieżki instalacyjnej, nowy folder pod nazwą `Softwin` zostanie utworzony w `Program Files` i będzie on zawierał podfolder `BitDefender 10`.

Notatka

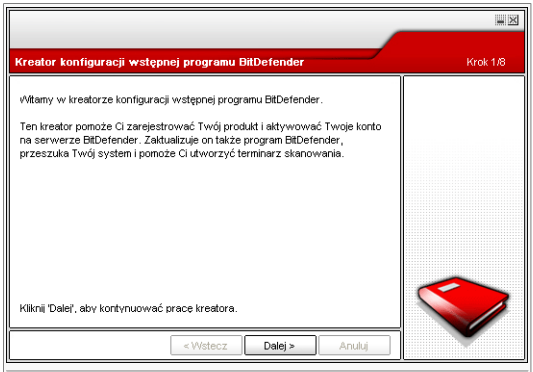
Możesz zostać poproszony o zrestartowanie systemu, aby zakończyć proces instalacji.

2.3. Kreator Konfiguracji

Podczas instalacji pojawi się kreator. Pomoże on zarejestrować Twój **BitDefender Antywirus v10**, stworzyć konto BitDefender oraz skonfigurować najważniejsze zadania ochrony programu.

Przejście przez kreatora nie jest wymagane, jednak zalecamy to zrobić aby w przyszłości zaoszczędzić czas i upewnić się, że system jest bezpieczny nawet przed instalacją BitDefender Antywirus v10.

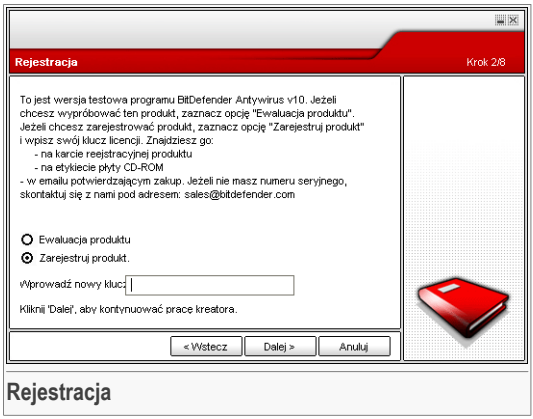
2.3.1. Krok 1/8 - Kreator konfiguracji BitDefender



Okno powitania

Kliknij **Dalej**.

2.3.2. Krok 2/8 - Zarejestruj BitDefender Antywirus v10



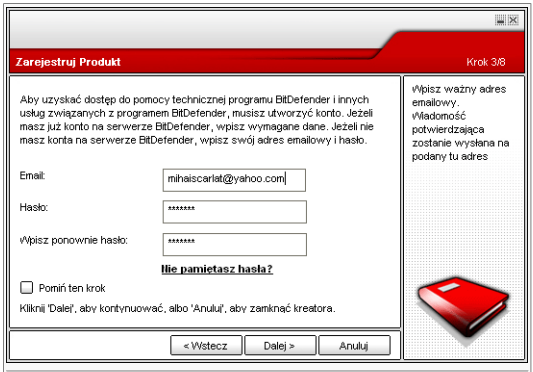
Rejestracja

Wybierz **Zarejestruj produkt** aby zarejestrować **BitDefender Antywirus v10**. Wprowadź klucz licencyjny w polu **Wprowadź nowy klucz**.

Aby korzystać z wersji testowej wybierz **Kontynuuj wersję testową**.

Kliknij **Dalej**.

2.3.3. Krok 3/8 - Utwórz konto BitDefender



Tworzenie konta

Nie mam konta BitDefender

Aby korzystać z darmowej pomocy technicznej BitDefender i innych darmowych serwisów musisz utworzyć konto.

Wpisz adres mailowy w polu **E-mail**. Wymyśl hasło i wpisz je w polu **Hasło**. Potwierdź hasło w polu **Potwierdź hasło**. Użyj adresu e-mail oraz hasła aby zalogować się na swoje konto pod adresem: http://myaccount.bitdefender.com.

Notatka

Hasło musi zawierać minimum 4 znaki.

Aby poprawnie utworzyć konto musisz najpierw uaktywnić swój adres mailowy. Sprawdź swoją skrzynkę mailową i podążaj za instrukcją przesłaną do Ciebie przez serwis rejestracyjny BitDefender.

WAŻNE

Proszę uaktywnić konto zanim przejdziesz do następnego kroku.

Jeżeli nie chcesz zakładać konta BitDefender po prostu wybierz: **Pomiń ten krok**.

Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** aby wyjść z kreatora.

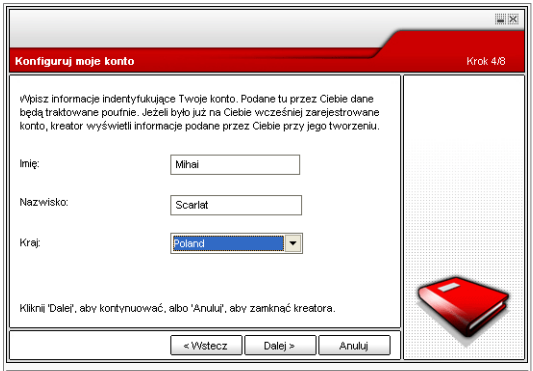
Posiadam konto BitDefender

Jeżeli juz posiadasz aktywne konto użyj swojego adresu e-mail i hasła. Jeżeli wpiszesz nieprawidłowe hasło zostaniesz poproszony o jego ponowne wpisanie.

Jeżeli zapomniałeś hasła kliknij **Zapomniałeś hasła?** i podążaj za instrukcją.

Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** aby wyjść z kreatora.

2.3.4. Krok 4/8 - Wpisz szczegóły konta



Szczegóły konta

Notatka

Jeżeli nie chcesz przechodzić przez ten krok zaznacz **Skip this step** w trzeci krok.

Wpisz imię i nazwisko oraz zaznacz kraj Twojego pochodzenia.

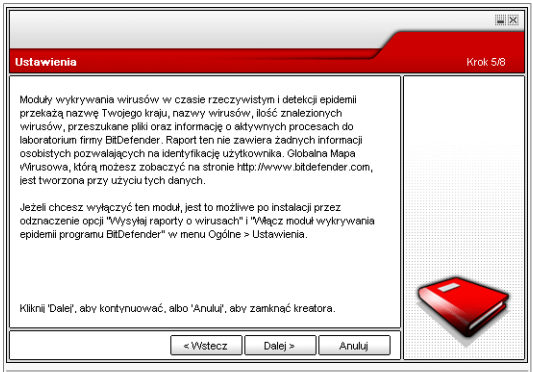
Jeżeli posiadasz już konto, kreator wyświetli informacje, które wprowadziłeś wcześniej. Jeżeli chcesz możesz je teraz zmodyfikować.

WAŻNE

Dane które teraz wprowadzisz pozostaną tajne.

Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** aby wyjść z kreatora.

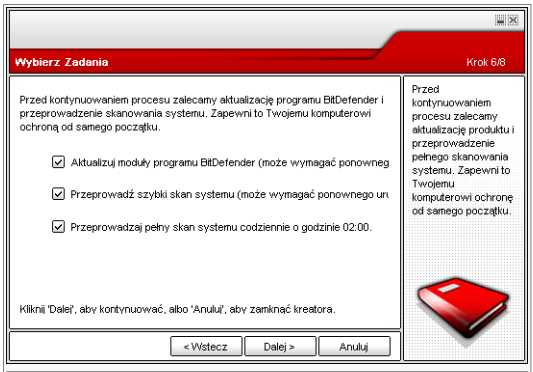
2.3.5. Krok 5/8 - Poznaj RTVR



Informacje RTVR

Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** aby wyjść z kreatora.

2.3.6. Krok 6/8 – Wybierz zadanie do wykonania



Wybór Zadania

Skonfiguruj BitDefender Antywirus v10 aby mógł wykonywać ważne zadania w celu zabezpieczenia Twojego systemu.

Dostępne są następujące opcje:

- **Zaktualizuj silniki BitDefender Antywirus v10 (może wymagać restartu)** - podczas następnego kroku silniki BitDefender Antywirus v10 zostaną zaktualizowane.
- **Uruchom szybkie skanowanie systemu (może wymagać restartu)** - podczas następnego kroku uruchomi się szybkie skanowanie systemu. BitDefender Antywirus v10 upewni się, że pliki z `Windows` oraz `Program Files` nie są zainfekowane.
- **Uruchom pełne skanowanie systemu każdego dnia o godz. 2.00**

WAŻNE

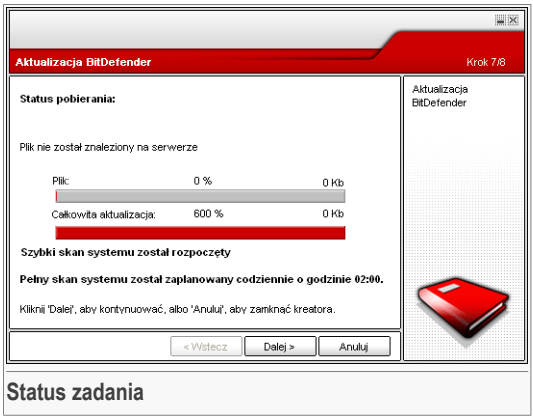
Zalecamy uruchomienie tych opcji przed przejściem do następnego kroku dla zapewnienia bezpieczeństwa systemu.

Jeżeli zaznaczysz tylko ostatnią opcję lub nie zaznaczysz żadnej, zostaniesz przeniesiony do następnego kroku.

Możesz dokonywać zmian w każdej chwili wracając do poprzednich kroków (klikij **Wstecz**).

Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** aby wyjść z kreatora.

2.3.7. Krok 7/8 - Zaczekaj na zakończenie zadania.

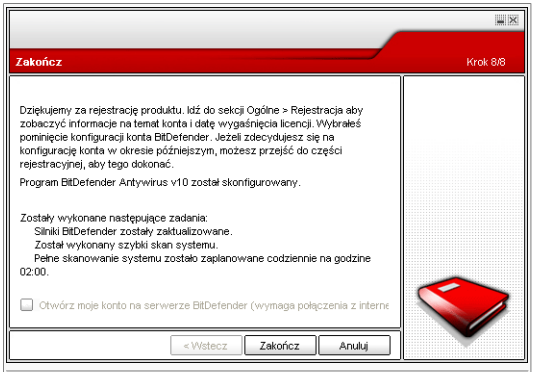


Status zadania

Zaczekaj na zakończenie zadania. Będziesz widział status zadania zaznaczonego w poprzednim kroku.

Kliknij **Dalej** aby kontynuować lub kliknij **Anuluj** aby wyjść z kreatora.

2.3.8. Krok 8/8 - Podsumowanie



Zakończ

To jest ostatni krok kreatora konfiguracji.

Wybierz **Otwórz moje konto BitDefender** aby wejść na swoje konto. Wymagane jest połączenie z internetem.

Kliknij **Zakończ** aby kontynuować instalację programu.

2.4. Aktualizacja

Aktualizacja może być wykonana w następujące sposoby:

- **Instalacja bez usuwania poprzedniej wersji – dla v8 lub wyższej, bez Internet Security**

  Kliknij dwukrotnie plik setup i podążaj za kreatorem opisanym w rozdziale „*Etapy instalacji*” (p. 7).

  WAŻNE

  Podczas instalacji może pojawić się błąd spowodowany przez `Filespy service`. Kliknij **OK** aby kontynuować instalację.

- **Odinstalować poprzednią wersję i zainstalować nową – dla wszystkich wersji BitDefender**

W pierwszej kolejności należy usunąć poprzednią wersję, następnie uruchomić ponownie komputer i zainstalować nową wersję jak opisano w rozdziale *„Etapy instalacji”* (p. 7).

WAŻNE

Jeżeli aktualizowałeś z wersji 8 lub wyższej zalecamy zachować BitDefender settings. Po procesie aktualizacji możesz go ponownie załadować.

2.5. Usuwanie, naprawa lub modyfikowanie modułów BitDefender

Jeżeli chcesz zmodyfikować, naprawić lub usunąć **BitDefender Antywirus v10**, wybierz z menu Start: **Start** -> **Programs** -> **BitDefender 10** -> **Modyfikuj, Napraw lub Odinstaluj**.

Będziesz proszony o potwierdzenie twojego wyboru przez kliknięcie **Następny**. Pojawi się nowe okno, w którym będziesz mógł dokonać następującego wyboru:

- **Modyfikuj** - aby wybrać i dodać nowe elementy programu lub wybrać i usunąć poprzednio zainstalowane elementy.

  Notatka

  Aby dowiedzieć się jak zakończyć proces instalacji sprawdź łącze szósty krok w rozdziale *„Etapy instalacji”* (p. 7).

- **Napraw** - aby ponownie zainstalować wszystkie składniki programu z poprzedniej instalacji.

  WAŻNE

  Przed naprawianiem programu zalecamy zapisać Ustawienia BitDefender'a. Gdy proces naprawiania zostanie zakończony możesz je ponownie zainstalować.

- **Usuń** - aby usunąć zainstalowane elementy.

  Jeżeli zdecydowałeś się usunąć program BitDefender, nie będziesz dalej chroniony przed wirusami, programami szpiegowskimi i hakerami. Jeżeli po odinstalowaniu programu BitDefender chcesz włączyć Zaporę Windows i Windows Defender, zaznacz odpowiednie pola wyboru w kolejnym kroku kreatora.

  Będziemy wdzięczni, jeżeli poświęcisz czas aby opowiedzieć nam o przyczynach dla których zdecydowałeś się odinstalować program BitDefender. Zaznacz pole wyboru odpowiadające poleceniu **Wyślij komentarz** i wypełnij formularz sieciowy, aby przesłać nam swoje uwagi.

Aby kontynuować instalację wybierz jedną z trzech opcji wymienionych powyżej. Zalecamy wybrać **Usuń** dla czystej reinstalacji. Gdy proces odinstalowania dobiegnie końca zalecamy usunąć folder `Softwin` z folderu `Program Files`.

Opis i funkcje

3. BitDefender Antywirus v10

Rozwiązanie antywirusowe i antyspamowe dla Twojego komputera!

BitDefender Antywirus v10 jest wydajnym narzędziem antywirusowym i antyspamowym z funkcjami najlepiej odpowiadającymi twoim potrzebom bezpieczeństwa. Łatwość obsługi i automatyczne aktualizacje czynią **BitDefender Antywirus** produktem typu "zainstaluj i zapomnij".

3.1. Antywirus

Zadaniem modułu antywirusowego jest wykrywanie i likwidowanie wszystkich wirusów. BitDefender Antywirus używa solidnych silników, które otrzymały certyfikaty od ICSA Labs, Virus Bulletin, Checkmark, CheckVir i TÜV.

Aktywne Wykrywanie. B-HAVE (Behavioral Heuristic Analyzer in Virtual Environments) emuluje wirtualną maszynę wewnątrz Twojego komputera gdzie odpowiednie elementy oprogramowania zostają uruchomione w celu wykrycia potencjalnych zagrożeń. Technologia ta należąca do BitDefender'a reprezentuje nowy poziom ochrony, dzięki któremu system operacyjny jest chroniony przed jeszcze nieznanymi wirusami.

Ciągła ochrona Antywirusowa. Nowe i ulepszone silniki skanowania BitDefender pozwalają skanować i leczyć pliki podczas ich otwierania, redukując utratę danych. Możesz teraz odzyskiwać zainfekowane dokumenty, zamiast je usuwać.

Wykrywanie i Usuwanie Rootkit'ów. Nowy moduł BitDefender'a wyszukuje i usuwa Rootkit'y (złośliwe oprogramowanie stworzone do przejmowania kontroli nad komputerem, pozostajac niezauważonym).

Skanowanie Ruchu Sieciowego. Ruch sieciowy jest teraz filtrowany w czasie rzeczywistym zanim dotrze do Twojej przeglądarki internetowej, zapewniając bezpieczne i przyjemne surfowanie po internecie.

Ochrona Aplikacji Peer-2-Peer oraz IM. Filtruje pod kątem wirusów rozprzestrzeniających się przez komunikatory typu Instant Messaging oraz przez aplikacje współdzielenia plików.

Pełna ochrona E-mail. BitDefender działa na poziomie protokołów POP3/SMTP, filtrując wchodzące i wychodzące wiadomości, niezależnie od rodzaju klienta pocztowego (Outlook™, Outlook Express™ / Windows Mail™, The Bat!™, Netscape®, itp.) bez konieczności dodatkowej konfiguracji.

3.2. Antyspyware

BitDefender monitoruje i zapobiega potencjalnym atakom typu spyware w czasie rzeczywistym, zanim uszkodzą twój system. Przy użyciu obszernej bazy danych sygnatur uwalnia twój komputer od spyware'ów.

Antyspyware. BitDefender monitoruje wiele potencjalnych punktów ataku, którymi mogą dostać się do systemu spyware'y, sprawdzając wszelkie zmiany wprowadzone do systemu i oprogramowania. Znane zagrożenia spyware są także blokowane w czasie rzeczywistym.

Skanowanie i Usuwanie Spyware'ów. BitDefender może skanować cały system, lub jego część, pod kątem znanych zagrożeń spyware. Do skanowania używa stale aktualizowanych baz sygnatur.

Ochrona Prywatności. Strażnik Prywatności monitoruje ruch HTTP i SMTP, sprawdzając czy osobiste informacje (numery kart kredytowych, PINy, itp.) nie opuszczają Twojego komputera.

Anty-Dialer. Konfigurowalny antydialer chroni przed aplikacjami łączącymi się z drogimi numerami telefonu.

Kontrola Cookie. Antyspyware filtruje wchodzące i wychodzące pliki typu cookie, chroniąc twoje dane osobiste podczas przeglądania stron internetowych.

Kontrola Aktywnej Zawartości. Blokuje wszystkie potencjalne szkodliwe aplikacje takie jak: ActiveX, Aplety Java albo Skrypty Java.

3.3. Inne Funkcje

Obsługa i sposób używania. Kreator konfiguracji uruchamia się autmatycznie po instalacji, pomagając użytkownikom wybrać najbardziej prawidłowe ustawienia aktualizacji, zaimplementować skanowanie zaplanowane oraz zapewnić szybką rejestrację i aktywację produktu.

Interfejs Użytkownika. BitDefender zaprojektował nowy interfejs użytkownika, stawiając nacisk na łatwość użycia oraz ergonomię. W rezultacie wiele modułów BitDefender v10 wymagają mniej wkładu użytkownika, poprzez użycie uczących się mechanizmów.

Cogodzinne Aktualizacje. BitDefender będzie aktualizowany przez internet 24 razy dziennie, bezpośrednio lub przez serwer Proxy. Produkt może się sam naprawić jeżeli zajdzie taka potrzeba, pobierając uszkodzone albo brakujące pliki z serwerów BitDefendera.

Wsparcie 24/7. Wsparcie online oferowane przez wykwalifikowany personel oraz baza danych online z odpowiedziami na często zadawane pytania.

Dysk Ratunkowy. **BitDefender Antywirus v10** jest sprzedawany na samobootowalnych płytach CD (bazujących na LinuxDefender), które mogą być używane w celu odinfekowania systemu bez jego uruchamiania.

4. Moduły BitDefender

BitDefender Antywirus v10 zawiera następujące moduły: **Ogólne**, **Antywirus**,**Antyspyware** i **Aktualizacja**.

4.1. Moduł Ogólne

BitDefender jest domyślnie skonfigurowany pod kątem maksymalnego bezpieczeństwa.

W module Ogólne możesz skonfigurować poziom bezpieczeństwa i uruchomić najważniejsze zadania bezpieczeństwa. Ponadto możesz zarejestrować swój produkt oraz ustawić ogólne zachowanie BitDefender'a.

4.2. Moduł Antywirus

BitDefender chroni przed wirusami, spyware'ami i innymi zagrożeniami dostającymi się do twojego systemu, skanując pliki, wiadomości e-mail, ruch internetowy i wszystkie inne treści jakie dostają się do twojego systemu.

Ochrona antywirusowa jest podzielona na dwie kategorie:

- Skanowanie on-access - Zapobiega dostaniu się nowych wirusów do twojego systemu. Nazywane jest to również ochroną czasu rzeczywistago – pliki są skanowane kiedy użytkownik chce je otworzyć. BitDefender będzie np. skanował document word w poszukiwaniu wirusów kiedy będziesz go otwierał, a wiadomości e-mail kiedy będziesz je otrzymywał.
- Skanowanie na żądanie - Wykrywa wirusy, które są już obecne w twoim systemie. Jest to klasyczne skanowanie wirusów zainicjowane przez użytkownika – wybierasz jaki dysk, folder lub plik ma być skanowany, a BitDefender skanuje go na żądanie.

4.3. Moduł Antyspyware

BitDefender monitoruje wiele potencjalnych punktów ataku, którymi mogą dostać się do systemu spyware'y, sprawdzając wszelkie zmiany wprowadzone do systemu i oprogramowania. Jest efektywny w blokowaniu koni trojańskich i innych narzędzi instalowanych przez hakerów próbujących przejąc prywatne informacje z twojego komputera.

4.4. Moduł Aktualizacji

Nowe oprogramowanie złośliwe jest znajdywane i identyfikowane każdego dnia. Dlatego bardzo ważnym jest aby na bierząco aktualizować BitDefender'a. Domyślnie Bitdefender automatycznie sprawdza aktualizacje co godzinę.

Aktualizacje są dostarczane w następujący sposób:

- **Aktualizacje silników antywirusowych** - kiedy pojawiają się nowe zagrożenia, pliki zawierające sygnatury wirusów muszą być nieustannie aktualizowane. Ten typ aktualizacji jest także znany pod nazwą **Aktualizacja Definicji Wirusów**.
- **Aktualizacja silników antyspyware** - nowe sygnatury są dodawane do bazy danych. Ten typ aktualizacji jest także znany pod nazwą **Aktualizacja Antyspyware**.
- **Aktualizacja produktu** - kiedy wychodzi nowa wersja programu, nowe elementy i techniki skanowania są dodawane aby zwiększyć wydajność produktu. Ten typ aktualizacji jest także znany pod nazwą **Product Update**.

Ponadto, z punktu widzenia użytkownika można wybrać:

- Aktualizacje automatyczne - BitDefender automatycznie kontaktuje się z serwerem aktualizacyjnym. Jeśli nowe aktualizacje są dostępne, to BitDefender jest aktualizowany automatycznie. Automatyczną aktualizacje można wykonać w każdym momencie klikając **Aktualizuj** w module Aktualizacja.
- Aktualizacje ręczne - należy pobrać i zainstalować najnowsze definicje wirusów ręcznie.

Konsola zarządzająca

5. Przegląd

BitDefender Antivirus v10 został zaprojektowany ze zintegrowaną konsolą zarządzania, która pozwala na konfiguracje ochrony dla wszystkich modułów BitDefender'a. Innymi słowy wystarczy otworzyć konsolę zarządzania i mieć dostęp do wszystkich modułów: **Antywirus**, **Antyspyware**, **Zapora** i **Aktualizacja**.

Aby uzyskać dostęp do konsoli zarządzającej użyj menu Windows Start: **Start** -> **Programs** -> **BitDefender 10** -> **BitDefender Antywirus v10** lub kliknij na **ikonę BitDefender** w pasku systemowym.

Konsola zarządzająca

Po lewej stronie konsoli zarządzania możesz zobaczyć sektor modułowy:

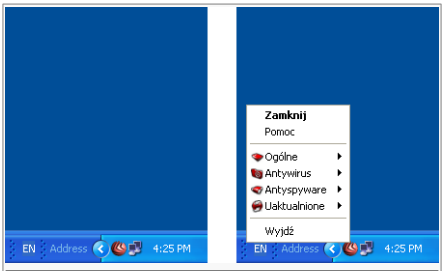
- Ogólne - w tej sekcji, możesz ustawić ogólny poziom zabezpieczenia i wykonać podstawowe zadania. Możesz tu także zarejestrować produkt i zobaczyć wszystkie ustawień BitDefender'a, szczegóły produktu oraz informacje kontaktowe.
- Antywirus - w tej sekcji mozesz skonfigurować moduł **Antywirus**.
- Antyspyware - w tej sekcji mozesz skonfigurować moduł **Antyspyware**.
- Aktualizacja - w tej sekcji mozesz skonfigurować moduł **Aktualizacja**.

Z prawej strony konsoli zarządzającej możesz zobaczyć informacje dotyczące sekcji, w której obecnie się znajdujesz. Opcja **Więcej Pomocy** znajdująca się w prawym dolnym rogu, otwiera plik **Pomoc**.

5.1. Pasek systemowy

Kiedy konsola jest zminimalizowana, w pasku systemowym pojawi się ikona.

Jeżeli klikniesz dwukrotnie w tą ikonę otworzy się konsola zarządzająca.



Ikona Bitdefender'a w Pasku Systemowym

- **Pokaż/Zamknij** - otwiera konsolę zarządzającą lub minimalizuje ją do paska systemowego.
- **Pomoc** - otwiera plik pomocy.
- **Ogolne** - pozwala zarządzać modułem Ogólne.
  - **Wprowadź Nowy Klucz** - rozpoczyna kreatora rejestracji, który poprowadzi Cię przez proces rejestracji.
  - **Edytuj Konto** - rozpoczyna kreatora, który pomoże Ci utworzyć konto BitDefender.
- **Antywirus** - administracja modułem Antywirus.
  - **Ochrona czasu rzeczywistego jest włączona/wyłączona** - pokazuje status ochrona czasu rzeczywistego (włączona/wyłączona). Kliknij tą opcję aby włączyć lub wyłączyć ochronę czasu rzeczywistego.
  - **Skanuj** - otwiera okno, w którym możesz uruchomić jedno ze skanowań dostępnych w sekcji Skanuj
- **Antyspyware** - administracja modułem Antyspyware
  - **Antispyware Behawioralny jest włączony/wyłączony** - pokazuje status behawioralna ochrona antyspyware'owa (włączona/wyłączona). Kliknij tą opcję aby włączyć lub wyłączyć behawioralną ochronę antyspyware'ową.
  - **Ustawienia Zaawansowane** - pozwala konfigurować sterowniki antyspyware'a.
- **Aktualizacja** - administracja modułem Aktualizacja.
  - **Zaktualizuj Teraz** - uruchamia aktualizację.
  - **Automatyczna aktualizacja włączona/wyłączona** pokazuje status automatyczna aktualizacja (włączona/wyłączona). Kliknij tą opcję aby włączyć lub wyłączyć automatyczną aktualizację.
- **Wyjdź** - zamyka aplikację. Po wybraniu tej opcji ikona z zniknie z paska systemowego. Aby ponownie uzyskać dostęp do konsoli zarządzającej musisz ponownie ją uruchomić z Menu Start.

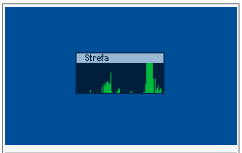
Notatka

Jeżeli zostanie wyłączony jeden lub więcej modułów BitDefendera, ikona zmieni kolor na czarny. Dzięki temu będziesz wiedział, że nie wszystkie moduły są aktywne bez potrzeby włączania konsoli zarządzającej.
Jeśli będą dostępne aktualizacje ikona będzie mrugać.

5.2. Okno Skanowania

Okno skanowania jest graficznym odzwierciedleniem wykonywanych czynności skanowania na twoim systemie.

Zielone okienka (the **Pliku**) pokażą ilość przeskanowanych plików/sek w skali od 1 do 50.



Okno Aktywności

Notatka

Okno skanowania poinformuje Cię jeśli Ochrona Antywirusowa będzie wyłączona - pojawi się czerwony krzyżyk w odpowiednim miejscu (**Plik**). Dzięki temu będziesz wiedział czy jesteś chroniony, bez konieczności otwierania konsoli zarządzającej.

Jeżeli chcesz wyjść z interfejsu graficznego, po prostu kliknij prawy przyciski myszy i wybierz **Ukryj**.

Notatka

Aby całkowicie ukryć to okno odznacz **Włącz okno skanowania** (z modułu **Ogólnie**, sekcji Ustawienia).

6. Moduł Ogólne

Rozdział **Ogólne** tej instrukcji obsługi zawiera następujące tematy:

- Centralna Administracja
- Ustawienia Konsoli Zarządzającej
- Dziennik Zdarzeń
- Rejestracja Produktu
- O Programie

Notatka

Aby uzyskać więcej szczegółów dotyczących modułu **Ogólne** przeczytaj opis „*Moduł Ogólne*” (p. 25).

6.1. Centralna Administracja

Centralna Administracja

W tej sekcji możesz skonfigurować ogólny poziom bezpieczeństwa i uruchomić ważne zadania. Ponadto możesz zarejestrować produkt i kontrolować datę wygaśnięcia licencji.

6.1.1. Szybkie Zadania

BitDefender pozwala na szybki dostęp do najważniejszych zadań bezpieczeństwa. Korzystając z tych zadań możesz być pewny, że BitDefender jest zaktualizowany, skanuje Twój system czy blokuje ruch.

Aby przeskanować cały system po prostu kliknij **Skanuj Teraz**. Pojawi się okno skanowania i cały system zostanie przeskanowany.

WAŻNE

Bardzo zalecamy uruchamianie pełnego skanowania systemu przynajmniej raz w tygodniu. Dodatkowe informacje na temat zadań i procesu skanowania znajdują się w rozdziale Skanowanie na Żądanie niniejszej instrukcji.

Przed skanowaniem systemu zalecamy zaktualizowanie BitDefendera aby mógł wykryć najnowsze wirusy. Aby rozpocząć aktualizację po prostu kliknij **Aktualizuj Teraz**. Zaczekaj parę sekund do momentu zakończenia procesu aktualizacji i sprawdź sekcję Aktualizacja aby zobaczyć status.

Notatka

Aby poznać więcej szczegółów na temat procesu aktualizacji idź do działu Automatyczne Aktualizacje tej instrukcji.

6.1.2. Poziom Bezpieczeństwa.

Możesz wybrać poziom bezpieczeństwa, który najbardziej odpowiada Twoim potrzebom.

Dostępne są 3 poziomy bezpieczeństwa:

Poziom bezpieczeństwa	Opis
Podstawowy	Nie oferuje żadnej ochrony. Włączona jest tylko **Automatyczna Aktualizacja**. Zapewnia tylko aktualizację BitDefender'a. Ponadto nie oferuje żadnej ochrony i może być użyteczny dla administratorów.
System Lokalny	Oferuje ochronę antywirusową. Szczególnie zalecany dla komputerów nie posiadających połączenia z Internetem. Zużycie zasobów komputera jest wtedy bardzo niskie. Wszystkie pliki są skanowane pod kątem wirusów.
System Lokalny Plus	Oferuje ochronę antywirusową i antyspyware'ową. Szczególnie zalecany dla komputerów nie posiadających połączenia z Internetem. Zużycie zasobów komputera jest wtedy niskie. Wszystkie pliki są skanowane pod kątem wirusów i spyware'ów.

BitDefender Antywirus v10 jest zalecany dla komputerów nie posiadających połączenia z Internetem.

Możesz dostosować poziom bezpieczeństwa klikając **Poziom Użytkownika**. Pojawi się okno, w którym możesz wybrać elementy BitDefender'a niezbędne do Twojej ochrony i kliknij **OK**.

Kliknij **Poziom Domyślny** aby uruchomić domyślne ustawienia.

6.1.3. Status Rejestracji

Dostępne są informacjena temat statusu licencji BitDefender'a. Możesz tutaj także zarejestrować produkt i kontrolować datę wygaśnięcia licencji.

Aby wprowadzić nowy klucz kliknij **Wprowadź Nowy Klucz**. Przejdź przez konfigurator rejestracji by pomyślnie zarejestrować BitDefender'a.

Notatka

Więcej szczegółów na temat procesu rejestracji dostępnych jest w sekcji Rejestracja Produktu tej instrukcji.

6.2. Ustawienia Konsoli Zarządzającej

Ustawienia Konsoli Zarządzającej

Możesz tutaj ustawić ogólne zachowania BitDefender'a. Domyślnie BitDefender jest załadowany w systemie startowym Windowsa i uruchamia się zminimalizowany w pasku zadań.

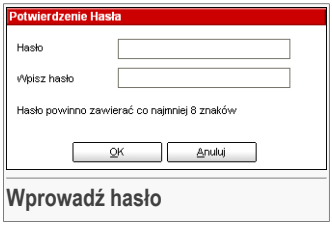
6.2.1. Ustawienia raportów

- **Włącz hasło dla ustawień produktu** - umożliwia ustawianie hasła do ochrony konfiguracji panelu sterowania BitDefender'a.

Notatka

Jeżeli nie jesteś jedynym użytkownikiem danego komputera zaleca się żebyś chronił swoje ustawienia hasłem.

Jeśli wybierzesz tą opcje, pojawi się następne okno:



Wprowadź hasło

Wpisz hasło w pole **Hasło**, następnie wpisz je ponownie w polu **Potwierdź hasło** i kliknij **OK**.

Od tego momentu, przy każdej zmianie konfiguracji BitDefender'a, będziesz poproszony o wprowadzenie hasła.

WAŻNE

Jeżeli zapomnisz hasła będziesz musiał naprawić program, aby modyfikować konfigurację BitDefender'a.

- **Pokaż Wiadomości BitDefender'a (związane z bezpieczeństwem)** - pokazuje informacje związane z bezpieczeństwem, wysyłane przez serwer BitDefender.
- **Pokaż okienka pop-up** - pokazuje okienka pop-up odnoszące się do statusu produktu.
- **Uruchom BitDefender podczas startu Windows** - automatycznie uruchamia BitDefender przy starcie systemu.

Notatka

Zalecamy wybranie tej opcji.

- **Włącz Pasek Skanowania** - włącza / wyłącza Pasek Skanowania.
- **Minimalizuj konsolę przy uruchamianiu** - minimalizuje konsolę BitDefender po starcie systemu. Tylko Ikona BitDefender pojawi się w pasku systemowym.

6.2.2. Ustawienia Raportów

- **Wyślij raport o wirusach** - wysyła raporty dotyczące zidentyfikowanych wirusów do laboratorium BitDefender. Pomoże nam to kontolować rozprzestrzenianie wirusów.

  Raporty nie będą zawierały żadnych tajnych danych takich jak: nazwa, adres IP itp. oraz nie będą wykorzystywane do celów komercyjnych. Dostarczona informacja będzie zawierała wyłącznie nazwę wirusa i wykorzystywana będzie jedynie w celu tworzenia statystyk raportów.

- **Wyślij raport o wirusach** - wysyła raporty dotyczące zidentyfikowanych wirusów do laboratorium BitDefender.

  Raporty nie będą zawierały żadnych tajnych danych takich jak: nazwa, adres IP itp. oraz nie będą wykorzystywane do celów komercyjnych. Dostarczona informacja będzie zawierała wyłącznie nazwę wirusa i wykorzystywana będzie jedynie w celu wykrywania nowych wirusów.

6.2.3. Ustawienia Wyglądu

Pozwala na wybranie koloru konsoli zarządzającej. W celu wybrania innego wyglądu kliknij na odpowiedni kolor.

6.2.4. Ustawienia Administracji

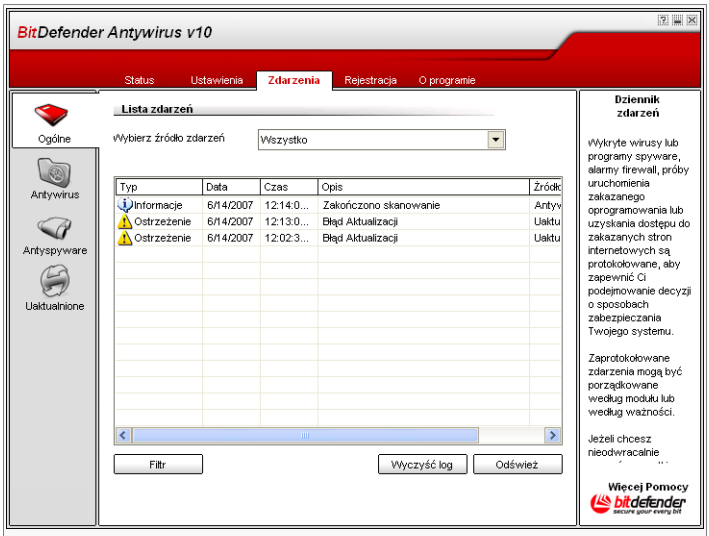
Użyj przycisków **Zapisz Wszystkie Ustawienia** / **Wczytaj Wszystkie Ustawienia** aby zachować / wczytać wszystkie ustawienia BitDefender'a. Dzięki temu możesz korzystać z tych samych ustawień po przeinstalowaniu czy naprawie BitDefender'a.

WAŻNE

Tylko użytkownicy z prawami administracyjnymi mogą zapisywać i wczytywać ustawienia.

Aby wczytać ustawienia domyślne, kliknij klawisz **Przywróć ustawienia domyślne**.

6.3. Dziennik zdarzeń



Dziennik zdarzeń

W tej sekcji są wyświetlane wszystkie zdarzenia wygenerowane przez BitDefender'a.

Istnieją 3 typy zdarzeń: **Informacja**, **Ostrzeżenie** i **Krytyczny**.

Przykłady zdarzeń:

- **Informacja** - gdy e-mail został przeskanowany;
- **Ostrzeżenie** - gdy został wykryty podejrzany plik;
- **Krytyczny** - gdy został wykryty zainfekowany plik.

Do każdego zdarzenia dodawane są następujące informacje: data i czas wystąpienia zdarzenia oraz krótki opis źródła (**Antywirus** albo **Aktualizacja**). Dwukrotne kliknięcie zdarzenia powoduje wyświetlenie jego właściwości.

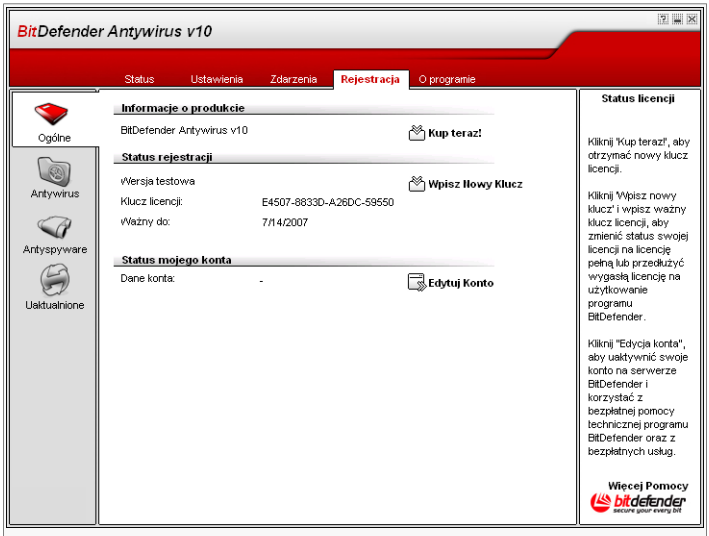
Możesz filtrować zdarzenia na 2 sposoby (ze względu na typ lub źródło):

- Kliknij **Filtr** aby wybrać jakie typy zdarzeń mają być wyświetlane.
- Wybierz źródło zdarzeń z rozwijanego menu;

Jeżeli konsola zarządzająca jest otwarta na sekcji **Zdarzenia** w tym samym czasie, w którym zdarzenie wystąpi, musisz kliknąć **Odśwież** aby zobaczyć to zdarzenie.

Aby usunąć wszystkie zdarzenia z listy kliknij **Wyczyść log** a następnie **Tak**, aby potwierdzić wybór.

6.4. Rejestracja Produktu



Rejestracja Produktu

Ta sekcja zawiera informacje o produkcie BitDefender (status rejestracji, ID produktu, data wygaśnięcia). W tej sekcji możesz także zarejestrować swój produkt i skonfigurować konto BitDefender.

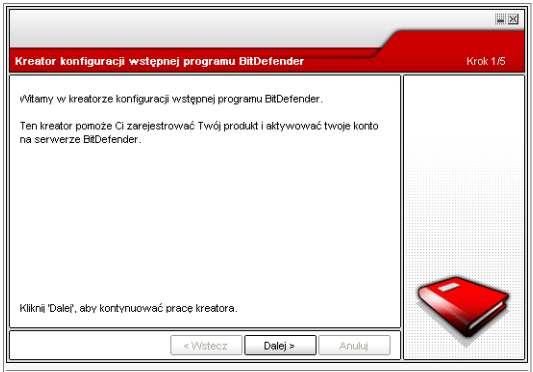
Kliknij **Kup Teraz** aby uzyskać nowy klucz licencyjny.

Klikając **Wprowadź Nowy Klucz** możesz zarejestrować produkt, modyfikować klucz lub szczegóły konta. Aby skonfigurować konto BitDefender kliknij **Edytuj Konto**. W obu przypadkach pojawi się kreator rejestracji.

6.4.1. Kreator Rejestracji

Kreator rejestracji składa się z 5 kroków.

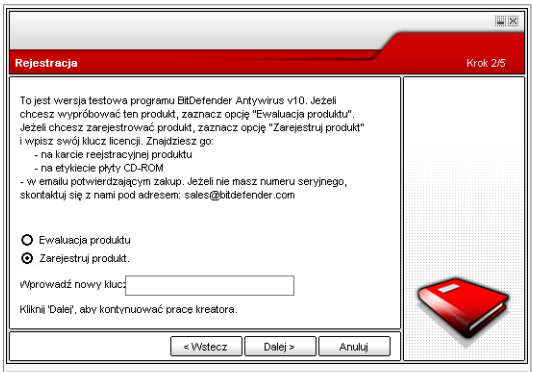
Krok 1/5 - Witamy w Kreatorze Rejestracji BitDefender



Okno powitania

Kliknij **Dalej**.

Krok 2/5 - Rejestracja BitDefender



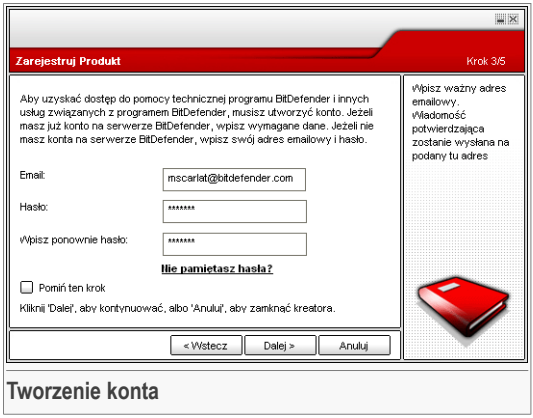
Rejestracja

Wybierz **Zarejestruj produkt** aby zarejestrować **BitDefender Antywirus v10**. Wprowadź klucz licencyjny w polu **Wprowadź nowy klucz**.

Aby kontynuować wersję testową wybierz **Kontynuuj wersję testową**.

Kliknij **Dalej**.

Krok 3/5 - Utwórz Konto BitDefender



Tworzenie konta

Nie mam konta BitDefender

Aby korzystać z darmowej pomocy technicznej BitDefender i innych darmowych serwisów musisz utworzyć konto.

Wpisz adres mailowy w polu **E-mail**. Wymyśl hasło i wpisz je w polu **Hasło**. Potwierdź hasło w polu **Potwierdź hasło**. Użyj adresu e-mail oraz hasła aby zalogować się na swoje konto pod adresem: http://myaccount.bitdefender.com.

Notatka

Hasło musi zawierać minimum 4 znaki.

Aby poprawnie utworzyć konto musisz najpierw uaktywnić swój adres mailowy. Sprawdź swoją skrzynkę mailową i podążaj za instrukcją przesłaną do Ciebie przez serwis rejestracyjny BitDefender.

WAŻNE

Proszę uaktywnić konto zanim przejdziesz do następnego kroku.

Jeżeli nie chcesz zakładać konta BitDefender po prostu wybierz: **Pomiń ten krok**.

Aby kontynuować kliknij **Dalej**.

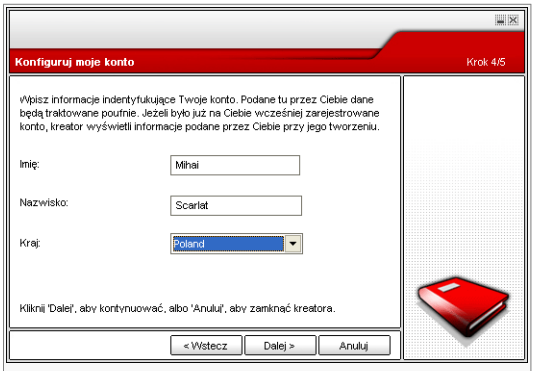
Posiadam konto BitDefender

Jeżeli juz posiadasz aktywne konto użyj swojego adresu e-mail i hasła. Jeżeli wpiszesz nieprawidłowe hasło zostaniesz poproszony o jego ponowne wpisanie.

Jeżeli zapomniałeś hasła kliknij **Zapomniałeś hasła?** i podążaj za instrukcją.

Aby kontynuować kliknij **Dalej**.

Krok 4/5 - Wprowadź Szczegóły Konta



Szczegóły konta

Notatka

Nie będziesz przechodził przez ten krok jeżeli masz zaznaczone **Pomiń ten krok** w trzecim kroku.

Wpisz swoje imię i nazwisko oraz wybierz kraj pochodzenia.

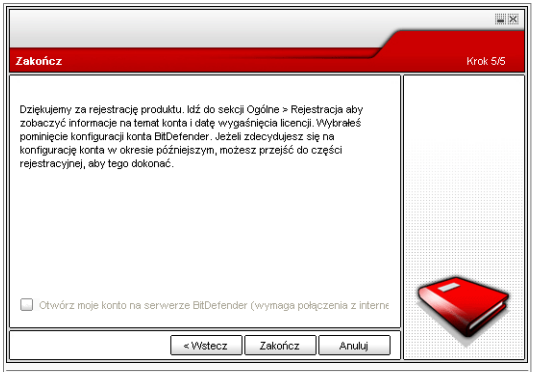
Jeżeli juz posiadasz konto, kreator wyświetli informacje, które wprowadziłeś wcześniej. Jeżeli chcesz możesz tutaj te informacje zmodyfikować.

WAŻNE

Dane które teraz wprowadzisz pozostaną tajne.

Kliknij **Dalej**.

Krok 5/5 - Podsumowanie



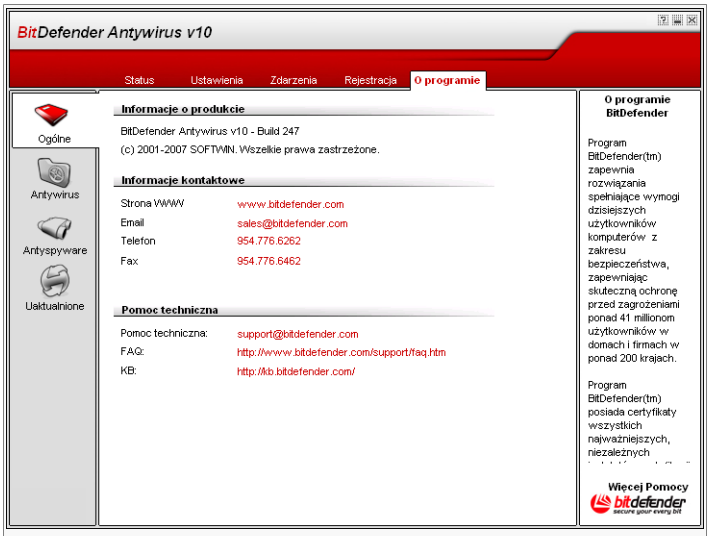
Zakończ

To jest ostatni krok kreatora konfiguracji. Jeśli chcesz coś zmienić musisz wrócić do poprzedniego kroku (kliknij **Wstecz**).

Jeśli nie chcesz robić żadnych zmian kliknij **Zakończ**.

Wybierz **Otwórz moje konto BitDefender** aby wejść na swoje konto. Wymagane jest połączenie z internetem.

6.5. O programie



Informacje Ogólne

W tym dziale znajdziesz informacje dotyczące kontaktu i szczegółów produktu.

BitDefender™ jest przodującym dostawcą rozwiązań bezpieczeństwa, które odpowiadają wymaganiom dzisiejszych środowisk komputerowych. Firma oferuje jedno z najszybszych i najbardziej wydajnych rozwiązań, ustalając nowe standardy w walce z zagrożeniami. BitDefender dostarcza swoje produkty i usługi do ponad 41 milionów użytkowników domowych i korporacyjnych w ponad 180 krajach.

BitDefender™ jest certyfikowany przez **ICSA Labs**, **CheckMark** and **Virus Bulletin** i jest jedynym produktem, który otrzymał nagrodę **IST Prize**.

Więcej informacji na temat BitDefendera znajdziecie Państwo na stronie: http://www.bitdefender.com.

7. Moduł Antywirus

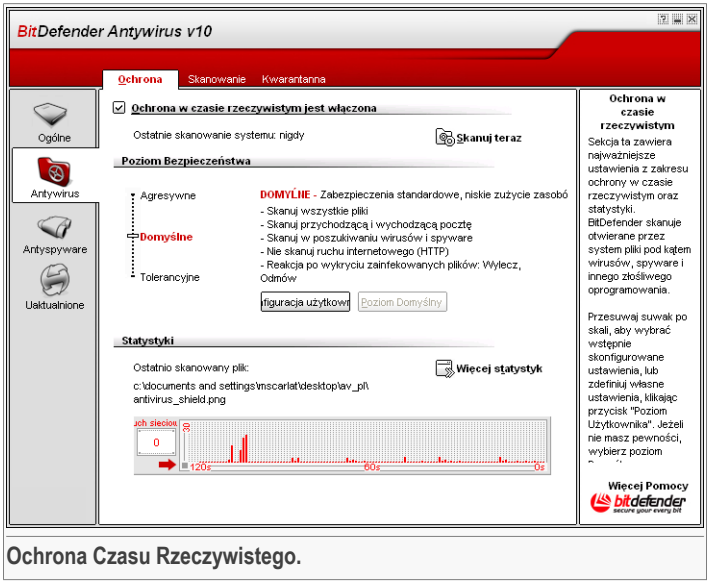
Rozdział **Antywirus** tej instrukcji obsługi zawiera następujące tematy:

- Skanowanie On-access
- Skanowanie na żądanie
- Kwarantanna

Notatka

Aby uzyskać więcej szczegółów dotyczących modułu **Antywirus** przeczytaj opis *„Moduł Antywirus”* (p. 25).

7.1. Skanowanie On access



Ochrona Czasu Rzeczywistego.

W tej sekcji możesz skonfigurować **Ochrona Czasu Rzeczywistego** i zobaczyć informacje dotyczące jej aktywności. **Ochrona Czasu Rzeczywistego** zabezpiecza twój komputer przez skanowanie wiadomości email, ściąganych plików i plików znajdujących się na dysku.

WAŻNE

Aby zapobiec zainfekowaniu komputera wirusami, miej włączoną opcję **Ochrona Czasu Rzeczywistego**.

W dolnej części sekcji możesz zobaczyć statystyki **Ochrona Czasu Rzeczywistego** dotyczące plików i wiadomosci email. Kliknij **Więcej statystyk** jeżeli chcesz zobaczyć więcej szczegółów dotyczących tego modułu.

7.1.1. Poziom Bezpieczeństwa

Możesz wybrać poziom bezpieczeństwa, który najbardziej odpowiada Twoim potrzebom.

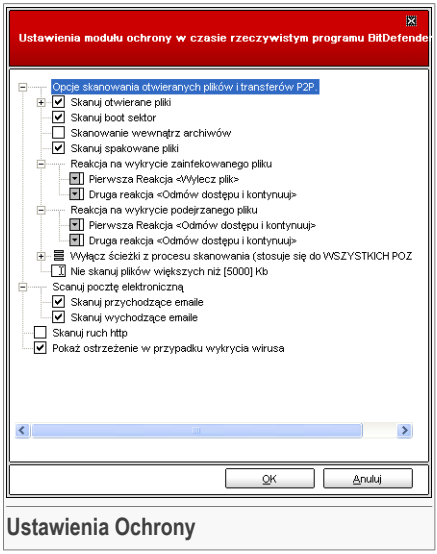
Dostępne są 3 poziomy bezpieczeństwa:

Poziom bezpieczeństwa	Opis
Tolerancyjny	Zapewnia podstawowe funkcje bezpieczeństwa. Zużycie zasobów komputera jest w tym przypadku bardzo niskie. Programy i przychodzące maile są skanowane tylko pod kątem wirusów. Ponadto używane jest klasyczne skanowanie oparte na sygnaturach . Na zainfekowanych plikach można wykonać następujące akcje: wylecz plik/zablokuj dostęp.
Domyślny	Oferuje standardowe zabezpieczenia. Zużycie zasobów komputera jest w tym przypadku niskie. Wszystkie pliki oraz przychodzące i wychodzące maile są skanowane pod kątem wirusów i spyware'ów. Ponadto używane jest klasyczne skanowanie oparte na sygnaturach . Na zainfekowanych plikach można wykonać następujące akcje: wylecz plik/zablokuj dostęp
Agresywny	Oferuje maksymalne zabezpieczenie. Zużycie zasobów komputera jest w tym przypadku umiarkowane. Wszystkie pliki oraz przychodzące i wychodzące maile są skanowane pod kątem wirusów i spyware'ów. Ponadto używane jest klasyczne skanowanie oparte na sygnaturach . Na zainfekowanych plikach można wykonać następujące akcje: wylecz plik/zablokuj dostęp.

Aby zastosować domyślne ustawienia ochrony czasu rzeczywistego kliknij **Poziom Domyślny**.

Zaawansowani użytkownicy mogą dokonywać zmian w ustawieniach skanowania. Skaner może być ustawiony, aby pomijać rozszerzenia plików, katalogi lub archiwa, które uważasz za nieszkodliwe. Może to znacząco zredukować czas skanowania i poprawić komfort pracy podczas skanowania.

Możesz dostosować **Ochrona Czasu Rzeczywistego** klikając **Poziom Użytkownika**. Pojawi się nastepujące okno:



Ustawienia Ochrony

Opcje skanowania są zorganizowane jako rozwijalne menu.

Kliknij okienko "+" aby otworzyć opcję lub "-" aby zamknąć opcję.

Możesz zaobserwować, że niektóre opcje skanowania, mimo że są odznaczone "+" nie mogą być otwarte. Dzieje się tak dlatego, że te opcje nie zostały jeszcze wybrane. Zaobserwujesz, że mogą być one otwarte, gdy je wybierzesz.

- **Skanuj pliki podczs otwierania i transferu P2P** - skanuje pliki podczas otwierania i transfer pomiędzy komunikatorami (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Następnie zaznacz typy plików, które chcesz skanować.

Opcja		Opis
Skanuj pliki podczas otwierania	**Skanuj wszystkie pliki**	Wszystkie pliki zostaną przeskanowane podczas otwierania, bez względu na ich typ.
	Skanuj tylko pliki programowe	Przeskanowane zostaną wyłącznie pliki programowe tzn. pliki z następującymi rozszerzeniami: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa;

Opcja		Opis
		.xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml i .nws.
	Skanuj tylko zdefiniowane rozszerzenia	Przeskanowane zostaną wyłącznie pliki z rozszerzeniami określonymi przez użytkownika. Rozszerzenia muszą być oddzielone przez ";".
	Wyłącz rozszerzenia ze skanowania:	Pliki z rozszerzeniami określonymi przez użytkownika NIE będą skanowane. Rozszerzenia muszą być oddzielone przez ";".
	Szukaj oprogramowania szpiegującego	Szuka aplikacji szpiegujących. Pliki tego typu będą traktowane jako zainfekowane. Oprogramowanie, które zawiera komponenty adware może przestać działać jeśli ta opcja jest włączona. Wybierz **Pomiń dialery i aplikacje podczas skanowania** jeżeli chcesz wyłączyć tego typu pliki ze skanowania.
Skanuj stację dyskietek		Skanuje stację dyskietek podczas dostępu.
Skanuj wewnątrz archiwów		Archiwa zostaną przeskanowane podczas otwierania. Ta opcja spowalnia pracę komputera.
Skanuj spakowane pliki		Wszystkie spakowane pliki zostaną przeskanowane.
Pierwsza reakcja		Możesz wybrać jedno z następujących działań:
	Zablokuj dostep i kontynuuj	W przypadku wykrycia zainfekowanego pliku dostęp do niego zostanie zablokowany.
	Wylecz plik	Leczy zainfekowany plik.
	Usuń plik	NatychmiastuUsuwa zainfekowane pliki, bez żadnego ostrzeżenia.
	Przenieś plik do kwarantanny	Zainfekowane pliki są przenoszone do kwarantanny.

Opcja		Opis
Druga reakcja		Wybierz drugą reakcję z rozwijanego menu, w przypadku gdy pierwsza reakcja zawiedzie.
	Zablokuj dostep i kontynuuj	W przypadku wykrycia zainfekowanego pliku dostęp do niego zostanie zablokowany.
	Usuń plik	NatychmiastuUsuwa zainfekowane pliki, bez żadnego ostrzeżenia.
	Przenieś plik do kwarantanny	Zainfekowane pliki są przenoszone do kwarantanny.
Nie skanuj plików większych niż [x] Kb		Wpisz maksymalny rozmiar plików jakie mają być skanowane. Jeżeli wpiszesz 0 Kb, wszystkie pliki zostaną przeskanowane, niezależnie od ich rozmiaru.
Wyłącz ścieżkę ze skanowania (dotyczy WSZYSTKICH POZIOMÓW)		Kliknij "+" odpowiadający tej opcji w celu określenia folderu, który będzie wyłączony ze skanowania. Elementy zaznaczone będą wyłączone ze skanowania, niezależnie od wybranego poziomu bezpieczeństwa(nie tylko dla **Poziom Użytkownika**).

- **Skanuj pocztę** - skanuje cały ruch pocztowy.

  Dostępne są następujące opcje:

Opcja	Opis
Skanuj przychodzące maile	Skanuje wszystkie przychodzące wiadomości e-mail
Skanuj wychodzące maile	Skanuje wszystkie wychodzące wiadomości e-mail

- **Skanuj ruch http** - skanuje ruch http.
- **Pokaż ostrzeżenie gdy wirus zostanie wykryty** -okno alarmu wyświetli się, gdy wirus zostanie znaleziony w pliku lub w wiadomości e-mail.

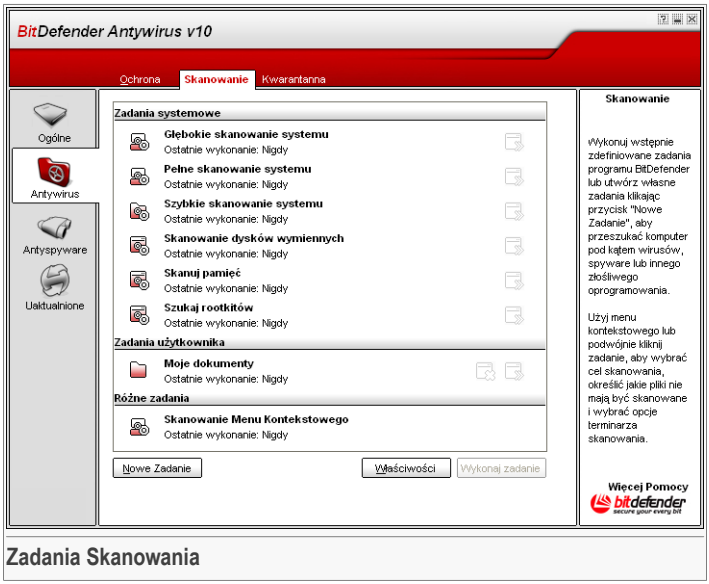
  W przypadku zainfekowanych plików, okno będzie zawierało nazwę wirusa, ścieżkę do niego i akcję jaką wykonał BitDefender. Zawierał będzie także link do strony

BitDefender'a, gdzie możesz znaleźć więcej informacji o danym wirusie. Natomiast, w przypadku zainfekowanych e-maili, okno alarmu będzie zawierało dodatkowo informacje o nadawcy i odbiorcy poczty.

W wypadku wykrycia podejrzanego pliku, możesz uruchomić kreatora z okna alarmu, który pomoże Ci wysłać plik do Laboratorium BitDefender'a w celu analizy. Możesz także wpisać swój e-mail aby otrzymać informacje dotyczące tego raportu.

Kliknij **OK** aby zapisać zmiany i zamknąć okno.

7.2. Skanowanie na żądanie



Zadania Skanowania

W tej sekcji możesz skonfigurować moduł skanowania BitDefender'a.

Głównym zadaniem BitDefender jest zabezpieczenie twojego komputera przed wirusami. Wykonywane jest to przede wszystkim poprzez uniemożliwianie dostępu do komputera nowym wirusom oraz przez skanowanie twoich wiadomości e-mail oraz każdych nowych plików zapisywanych lub kopiowanych do twojego systemu.

Istnieje ryzyko, że wirus już umiejscowił się w systemie, zanim zainstalowałeś BitDefender'a. Dlatego też ważne jest przeskanowanie twojego komputera w

poszukiwaniu obecnych wirusów, zaraz po zainstalowaniu BitDefender'a. Ważne również jest regularne skanowanie komputera.

7.2.1. Zadania Skanowania

Skanowanie na żądanie jest oparte na zadaniach skanowania. Użytkownik może przeskanować komputer używając domyślnych zadań lub zadań przez siebie zdefinowanych.

Dostępne są trzy kategorie zadań skanowania:

- **Zadania systemowe** - zawiera listę domyślnych zadań systemowych. Dostępne są następujące zadania:

Zadania Domyślne	Opis
Głębokie Skanowanie Systemu	Skanuje cały system, łącznie z archiwami.
Pełne Skanowanie Systemu	Skanuje cały system wyłączając archiwa
Szybkie Skanowanie Systemu	Skanuje wszystkie programy pod kątem wirusów i spyware'ów.
Skanuj dyski usuwalne	Skanuje wszystkie dyski usuwalne pod kątem wirusów i spyware'ów.
Skanuj Pamięć	Skanuje pamięć pod kątem znanych spyware'ów.
Szukaj Rootkit'ów	Skanuje pamięć pod kątem oprogramowania złośliwego.

- **Zadania użytkownika** - zawiera zadania zdefiniowane przez użytkownika.

  Dostępne jest zadanie `Moje Dokumenty`. Użyj tego zadania do skanowania swoich dokumentów z folderu `Moje Dokumenty`.

- **Różne zadania** - zawiera listę różnych zadań skanowania. Zadania te odpowiadają alternatywnym typom skanowania, które nie mogą być uruchomione z pozomu tego okienka. Możesz tylko modyfikować ich ustawienia lub zobaczyć raporty skanowania.

Na prawo od każdego zadania dostępne są 3 przyciski:

- **Zadania Zaplanowane** - oznacza, że dane zadanie jest zaplanowane na później. Kliknij ten przycisk aby przejść do sekcji Terminarz do okna **Właściwości**, gdzie możesz modyfikować te ustawienia.

- **Usuń** - usuwa zaznaczone zadania.

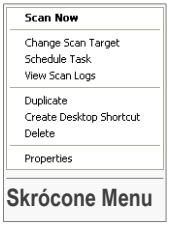
Notatka

Niedostępne dla zadań systemowych. Nie możesz usunąć zadań systemowych.

- **Skanuj Teraz** - uruchamia zaznaczone zadanie, rozpoczynając natychmiastowe skanowanie.

7.2.2. Skrócone Menu

Skrócone menu jest dostępne dla każdego zadania. Aby je otworzyć kliknij prawym przyciskiem na wybranym zadaniu.



Skrócone Menu

Dostępne są następujące opcje w skróconym menu:

- **Skanuj Teraz** - uruchamia zaznaczone zadanie.
- Polecenie **Zmień Miejsca Skanowania** - otwiera zakładkę **Ścieżka Skanowania** w oknie **Właściwości**, gdzie możesz zmienić miejsca skanowania dla zaznaczonych zadań.
- **Zaplanuj Zadanie** - otwiera okno **Właściwości**, zakładkę **Terminarz**, gdzie możesz zaplanować zaznaczone zadanie.
- **Pokaż Logi Skanowania** - otwiera okno **Właściwości**, zakładkę **Logi Skanowania**, gdzie możesz zobaczyć raporty wygenerowane po wykonaniu danego zadania.
- **Duplikuj** - duplikuje zaznaczone zadanie.

Notatka

Jest to szczególnie przydatne podczas tworzenia nowego zadania, ponieważ możesz modyfikować ustawienia zduplikowanego zadanie.

- **Utwórz Skrót na Pulpicie** - tworzy skrót do danego zadania.
- **Usuń** - usuwa wybrane zadanie.

Notatka

Niedostępne dla zadań systemowych. Nie możesz usunąć zadań systemowych.

- **Właściwości** - otwiera okno **Wlasciwości**, zakładkę **Przegląd**, gdzie możesz zmienić ustawienia zaznaczonego zadania.

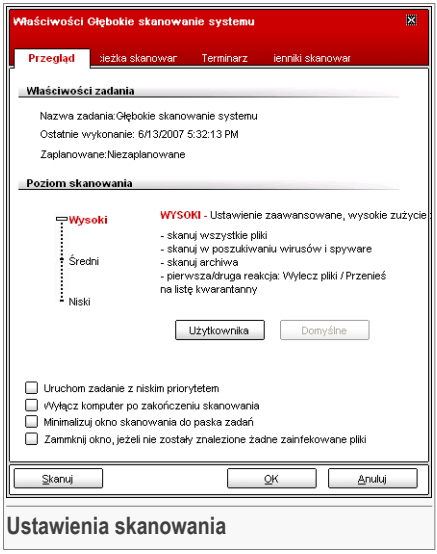
WAŻNE

Tylko opcje **Właściwości** i **Pokaż Logi Skanowania** są dostępne dla zadań w kategorii **Różne Zadania**

7.2.3. Właściwości Zadań Skanowania

Każde zadanie skanowania ma swoje własne okno **Właściwości**, gdzie możesz konfigurować opcje skanowania, ustawić elementy skanowania, zaplanować zadania lub zobaczyć raporty. Aby wejść do tego okna wybierz zadanie i kliknij **Właściwości** (lub kliknij prawym klawiszem na zadanie. a następnie kliknij **Właściwości**).

Ustawienia skanowania



Ustawienia skanowania

Możesz tutaj zobaczyć informacje o zadaniach (nazwa, ostatnie uruchomienie i status terminarza) oraz skonfigurować ustawienia skanowania.

Poziom Skanowania

Po pierwsze, musisz wybrać poziom skanowania. Przeciągnij wskaźnik po pasku aby ustawić odpowiedni poziom skanowania.

Dostępne są 3 poziomy skanowania:

Poziom bezpieczeństwa	Opis
Niski	Oferuje rozsądną skuteczność wykrywania. Poziom zużycia zasobów komputera jest niski. Programy są skanowane tylko pod kątem wirusów. Ponadto uruchomione jest klasyczne skanowanie oparte na sygnaturach. Na zainfekowanych plikach można wykonać następujące zadania: wylecz plik/przenieś do kwarantanny.
Średni	Oferuje dobrą skuteczność wykrywania. Poziom zużycia zasobów komputera jest umiarkowany. Wszystkie pliki są skanowane pod kątem wirusów i spyware'ów. Ponadto uruchomione jest klasyczne skanowanie oparte na sygnaturach. Na zainfekowanych plikach można wykonać następujące zadania: wylecz plik/przenieś do kwarantanny.
Wysoki	Oferuje maksymalną skuteczność wykrywania. Poziom zużycia zasobów komputera jest wysoki. Wszystkie pliki i archiwa są skanowane pod kątem wirusów i spyware'ów. Ponadto uruchomione jest klasyczne skanowanie oparte na sygnaturach. Na zainfekowanych plikach można wykonać następujące zadania: wylecz plik/przenieś do kwarantanny

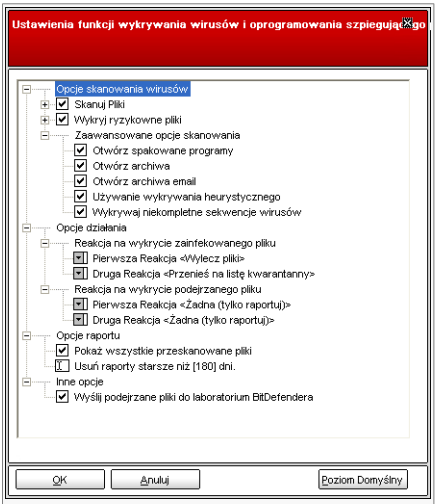
WAŻNE

Zadanie **Szukaj Rootkit'ów** ma te same poziomy skanowania. Jednakże opcje są inne:

- **Niski** - skanowane są jedynie procesy. Żadna akcja nie jest podejmowana na wykrytych obiektach.
- **Średni** - pliki i procesy są skanowane w poszukiwaniu ukrytych obiektów. Żadna akcja nie jest podejmowana na wykrytych obiektach.
- **Wysoki** - pliki i procesy są skanowane w poszukiwaniu ukrytych obiektów. Nazwa wykrytych obiektów zostanie zmieniona.

Zaawansowani użytkownicy mogą dokonywać zmian w ustawieniach skanowania. Skaner może być ustawiony, aby pomijać rozszerzenia plików, katalogi lub archiwa, które uważasz za nieszkodliwe. Może to znacząco zredukować czas skanowania i poprawić komfort pracy podczas skanowania.

Kliknij **Użytkownika** aby ustawić własne opcje. Pojawi się nowe okno.



Ustawienia skanowania

Opcje skanowania są zorganizowane jako rozwijalne menu.

Opcje skanowania są podzielone na pięć kategorii:

- **Opcje skanowania wirusowego**
- **Opcje oprogramowania szpiegującego**
- **Opcje działania**
- **Opcje raportów**
- **Inne opcje**

Kliknij okienko "+" aby otworzyć opcję lub "-" aby zamknąć opcję.

WAŻNE

Dla zadania **Szukaj Rootkit'ów** dostępne są tylko 3 kategorie: **Opcje szukania Rootkit'ów**, **Opcje raportów** i **Inne opcje**. Z pierwszej kategorii możesz wybrać elementy do skanowania i możesz ustawić działania podjęte na wykrytych obiektach (**Żadne (elementy logów)/Zmień nazwę pliku**). Ostatnie dwie kategorie są identyczne jak poprzednie.

- Wybierz typ obiektów do skanowania (archiwa, wiadomości email, itp.) i inne opcje. Dokonuje się tego poprzez wybór odpowiednich opcji z kategorii **Opcje skanowania wirusowego**.

Opcja		Opis
Skanuj pliki	**Skanuj wszystkie pliki**	Wszystkie pliki zostaną przeskanowane podczas otwierania, bez względu na ich typ.
	Skanuj tylko pliki programowe	Wyłącznie pliki programowe zostaną przeskanowane tzn. pliki z następującymi rozszerzeniami: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` i `nws`.
	Skanuj tylko zdefiniowane rozszerzenia	Przeskanowane zostaną wyłącznie pliki z rozszerzeniami określonymi przez użytkownika. Rozszerzenia muszą być oddzielone przez ";".
	Wyłącz zdefiniowane przez użytkownika rozszerzenia	Pliki z rozszerzeniami określonymi przez użytkownika NIE będą skanowane. Rozszerzenia muszą być oddzielone przez ";".
Skanuj boot sektory		Skanuje boot sektory systemu.
Skanuj pamięć		Skanuje pamięć pod kątem wirusów i innego oprogramowania złośliwego.
Wykryj ryzykowne pliki		Skanuje w poszukiwaniu zagrożeń innych niż wirusy, takie jak dialery i adware'y. Pliki te będą traktowane jako zainfekowane. Oprogramowanie zawierające elementy adware może przestać pracować, jeżeli ta opcja będzie uruchomiona. Wybierz **Wyklucz aplikacje i dialery** jeżeli chcesz pominąć te pliki podczas skanowania.
Zaawansowane opcje skanowania	**Otwórz spakowane programy**	Skanuje spakowane pliki.
	Otwórz archiwa	Skanuje wewnątrz archiw.
	Otwórz archiwa email	Skanuje wewnątrz archiwów email.

Opcja		Opis
	Użyj wykrywania heurystycznego	Aby używać skanowania heurystycznego plików. Celem skanowania heurystycznego jest identyfikacja nowych wirusów, bazująca na konkretnych wzorach i algorytmach, zanim wyjdzie definicja wirusa. Mogą pojawić się fałszywe alarmy. Kiedy tego typu plik zostaje wykryty, automatycznie jest klasyfikowany jako podejrzany. W tych przypadkach zalecamy wysłąnie pliku do laboratorium BitDefender w celu analizy.
	Wykryj niekompletne kody wirusów	Wykrywa niekompletne wirusy.

- Określ miejsca skanowania antyspyware'owego (rejestry, cookie). Robi się to przez wybór odpowiednich opcji z kategorii **Opcje skanowania antyspyware'owego**.

Opcja	Opis
Skanuj rejestry	Skanuje wpisy do rejestru.
Skanuj cookie	Skanuje pliki cookie.

- Ustaw reakcje na zainfekowane albo podjrzane pliki. Otwórz **Opcje działania** jeśli chcesz zobaczyć wszystkie możliwe opcje.

  Wybierz reakcje gdy zostanie wykryty zainfekowany lub podejrzany plik. Możesz ustawić inną reakcje na zainfekowane i podejrzane pliki. Możesz także wybrać drugą reakcje gdy pierwsza zawiedzie.

Działanie	Opis
Żadna (tylko raportowanie)	Żadna reakcja nie będzie podjęta na zainfekowane pliki. Pliki te będą zawarte w raporcie.
Zapytaj użytkownika o reakcje	Kiedy zainfekowany plik zostanie wykryty, pojawi się okienko w którym będzie można dokonać wyboru danego działania. Zależnie od ważności pliku, możesz wybrać odinfekowanie pliku, odizolowanie pliku przenosząc go do kwarantanny lub usunięcie go.

Działanie	Opis
Wylecz pliki	Leczy zainfekowany plik.
Usuń pliki	NatychmiastuUsuwa zainfekowane pliki, bez żadnego ostrzeżenia.
Przenieś do kwarantanny	Przenosi zainfekowane pliki do kwarantanny.
Zmień nazwę plików	Zmienia rozszerzenie zainfekowanego pliku. Nowe rozszerzenie zainfekowanego pliku jest następujące `.vir`. Zmieniając nazwę zainfekowanych plików, możliwość rozprzestrzeniania się infekcji jest zablokowana. W tym samym czasie pliki mogą być zapisane w celu dalszej analizy.

WAŻNE

Zmień nazwę plików działa podobnie na pliki ukryte (rootkit'y). Nowe rozszerzenie wykrytych plików jest następujące `.bd.ren`. Zmieniając nazwę zainfekowanych plików, możliwość rozprzestrzeniania się infekcji jest zablokowana. W tym samym czasie pliki mogą być zapisane w celu dalszej analizy.

- Ustaw opcje dla plików raportu. Otwórz kategorię **Opcje raportu** jeśli chcesz zobaczyć wszystkie możliwe opcje.

Opcja	Opis
Pokaż wszystkie przeskanowane pliki	Pokazuje wszystkie przeskanowane pliki i ich status (zainfekowane lub nie) w pliku raportu. Ta opcja spowalnia pracę komputera.
Usuń logi starsze niż [x] dni	Jest to pole edycji, które pozwala określić jak długo raporty będą trzymane w sekcji Logi Skanowania. Wybierz tą opcję i wpisz nowy przedział czasu. Domyślny przedział czasu to 180 dni.

Notatka

Pliki raportu można zobaczyć w sekcji Logi Skanowania w oknie **Właściwości**

- Ustaw inne opcje. Otwórz kategorię **Inne opcje** gdzie możesz wybrać następujące opcje:

Opcja	Opis
Wyślij podejrzane pliki do Laboratorium BitDefender	Będziesz poproszony o wysłanie wszystkich podejrzanych plików po zakończeniu procesu skanowania.

Jeśli klikniesz przycisk **Poziom Domyślny** wczytasz domyślne ustawienia.

Kliknij **OK** aby zapisać zmiany i zamknąć okno.

Inne Ustawienia

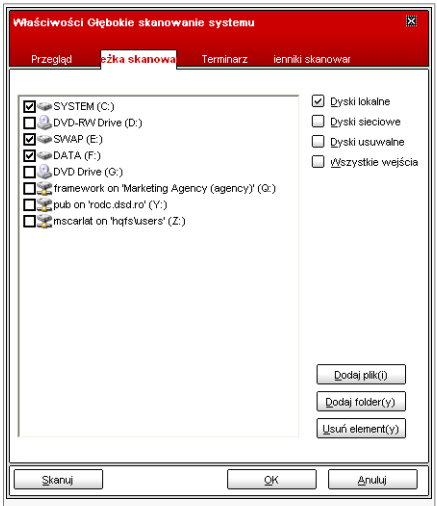
Ponadto dostępna jest cała lista opcji skanowania:

Opcja	Opis
Uruchom zadanie z Niskim priorytetem	Obniża priorytet procesu skanowania. Pozwala innym programom działać szybciej i zwiększa czas potrzebny na zakończenie skanowania.
Wyłącz komputer po zakończeniu skanowania	Wyłącza komputer po zakończeniu procesu skanowania.
Wyślij podejrzane pliki do Laboratorium BitDefender	Będziesz poproszony o wysłanie wszystkich podejrzanych plików po zakończeniu procesu skanowania.
Minimalizuj okno skanowania do paska systemowego	Minimalizuje okno skanowania do paska systemowego. Kliknij dwukrotnie ikonę BitDefender aby otworzyć okno skanowania.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

Miejsca Skanowania

Zaznacza zadanie, kliknij **Właściwości**, a następnie kliknij zakładkę **Scieżka skanowania** aby wejść do tej sekcji.



Miejsca Skanowania

Możesz tutaj ustawić miejsce skanowania.

Ta sekcja zawiera następujące klawisze:

- **Dodaj plik(i)** - otwiera okno przeglądania, gdzie możesz wybrać plik(i), które chcesz skanować.
- **Dodaj folder(y)** - to samo co powyżej, ale wybierasz folder(y).

Notatka

Użyj przeciągnij i upuść, aby dodać pliki/foldery do listy.

- **Usuń element(y)** - usuwa plik(i) / folder(y), które poprzednio zostały wybrane z listy obiektów do skanowania.

Notatka

Tylko plik(i) / folder(y), które zostały dodane mogą być usunięte, lecz te które zostały automatycznie wykryte przez BitDefender'a nie mogą być usunięte.

Poza przyciskami opisanymi powyżej , jest jeszcze kilka opcji, które pozwalają szybko wybrać lokalizacje do skanowania.

- **Dyski lokalne** - aby skanować dyski lokalne.
- **Dyski sieciowe** - aby skanować wszystkie dyski sieciowe.
- **Dyski usuwalne** - aby skanować usuwalne dyski (CD-ROM, stacja dyskietek, itp.)
- **Wszystko** - aby skanować wszystkie dyski, bez względu na to czy są lokalne, sieciowe czy usuwalne.

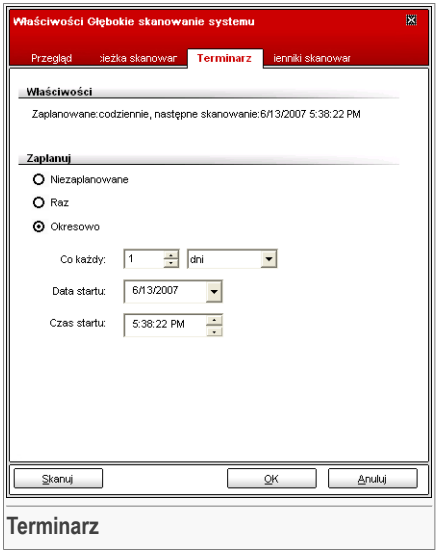
Notatka

Jeżeli chcesz skanować cały swój komputer w poszukiwaniu wirusów, wybierz opcję **Wszystko**.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

Terminarz

Zaznacz zadanie, kliknij **Właściwości**, a następnie kliknij zakładkę **Terminarz**, aby wejść do tej sekcji.



Terminarz

Tutaj możesz zobaczyć czy zadanie jest zaplanowane czy też nie oraz możesz zmienic tę opcję.

WAŻNE

Z aktywnymi wszystkimi zadaniami proces skanowania zajmie trochę czasu i będzie działał lepiej jeżeli zamkniesz wszystkie inne programy. Dlatego najlepszym rozwiązaniem będzie zaplanowanie zadań wtedy, gdy nie korzystasz z komputera.

Podczas planowania zadania musisz wybrać jedną z opcji:

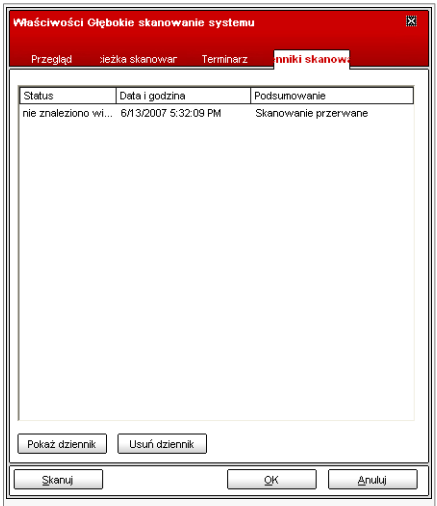
- **Nie zaplanowane** - Uruchamia zadanie tylko na prośbę użytkownika.
- **Raz** - uruchamia skanowanie tylko raz w określonym momencie. Ustaw datę i czas rozpoczęcia w polu **Rozpocznij Data/Czas**.
- **Okresowo** - uruchamia skanowanie okresowo, w określonym przedziale (godziny, dni, tygodnie, miesiące, lata) uruchamia o ustalonej dacie i czasie.

  Jeżeli chcesz żeby skanowanie było powtarzane w danym przedziale, wybierz **Okresowo** i wpisz w oknie edycji **Kazdego** ilość minut / godzin / dni / tygodni / miesięcy / lat, kiedy chcesz powtarzać ten proces. Musisz także określić datę i czas rozpoczęcia w polu **Rozpocznij Data/Czas**.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

Logi Skanowania

Zaznacz zadanie, kliknij **Właściwości**, a następnie kliknij zakładkę **Logi Skanowania**, aby wejść do tej sekcji.



Logi Skanowania

Możesz tutaj zobaczyć pliki raportów generowane za każdym razem po zakończeniu zadania. Każdy plik zawiera informację o jego statusie (wyleczony/zainfekowany), datę i czas skanowania oraz podsumowanie.

Dostępne są dwa przyciski:

- **Pokaż logi** - otwiera wybrany plik raportu;
- **Usuń log** - usuwa wybrany plik raportu;

Ponadto, aby wyświetlić lub usunąć plik kliknij na niego prawym przyciskiem i wybierz odpowiednią opcję z menu.

Kliknij **OK** aby zapisać zmiany i zamknąć okno. Aby uruchomić zadanie po prostu kliknij **Skanuj**.

7.2.4. Typy Skanowania na żądanie

BitDefender posiada trzy typy skanowania na żądanie:

- Skanowanie natychmiastowe - uruchamia zadanie skanowania z zadań użytkownika/systemu.
- Skanowanie kontekstowe - kliknij prawym przyciskiem myszy na plik lub folder i wybierz BitDefender Antivirus v10;

- Skanowanie Przeciagnij i Upuść - przeciągnij i upuść plik lub folder do Okienka Czynności Skanowania;

Skanowanie natychmiastowe

Aby przeskanować cały komputer lub jego część możesz użyć domyślnego zadania skanowania lub stworzyć swoje własne zadanie. Są dwie metody tworzenia zadania skanowania:

- Duplikuj istniejące zadanie, zmień nazwę i wprowadź niezbędne zmiany w oknie Właściwości;
- Kliknij **Nowe Zadanie** aby stworzyć nowe zadanie i je skonfigurować

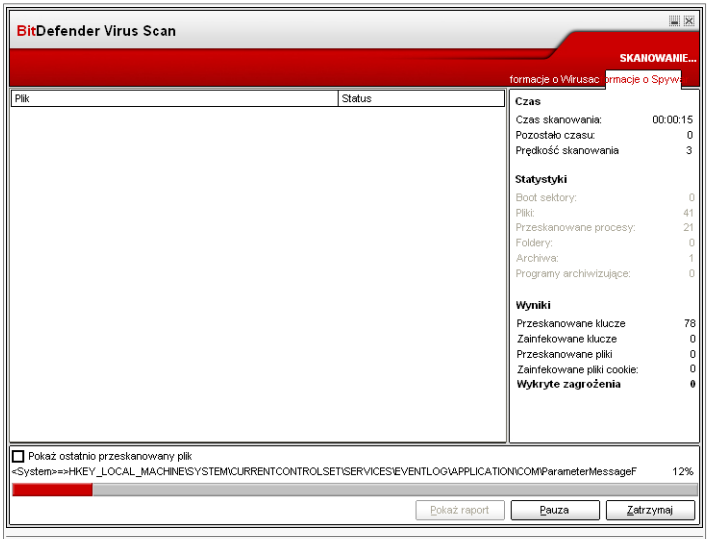
Aby BitDefender wykonał całkowite skanowanie, musisz zamknąć wszystkie otwarte programy. Szczególnie Twój klient pocztowy (tj. Outlook, Outlook Express lub Eudora) powinien być zamknięty.

Zanim uruchomisz skanowanie swojego komputera powinieneś upewnić się, że najnowsze sygnatury wirusów są zaktualizowane, ponieważ każdego dnia są odnajdywane i identyfikowane nowe wirusy. Możesz zweryfikować czas ostatniej aktualizacji w module Aktualizacja.

Aby uruchomić skanowanie skorzystaj z jednej z następujących metod:

- kliknij dwukrotnie na wybrane zadanie skanowania z listy;
- kliknij przycisk **Skanuj teraz** odpowiadający zadaniu;
- zaznacz zadanie ia następnie kliknij zakładkę **Wykonaj zadanie**.

Wyświetlone zostanie okno skanowania.



Okno Skanowania

Pojawi się ikona w pasku systemowym kiedy proces skanowania będzie uruchomiony.

Podczas skanowania BitDefender pokazuje postęp i alarmuje gdy znajdzie jakieś zagożenia. Po prawej możesz zobaczyć statystyki dotyczące procesu skanowania. W zależności od miejsca skanowania informacja o wirusach i/lub spyware'ach jest dostępna. Jeżeli obie są dostępne kliknij odpowiednią zakładkę aby dowiedzieć sie więcej o procesie skanowania.

Zaznacz opcję **Pokaż ostatni przeskanowany plik** i tylko informacja o ostatnim przeskanowanym pliku będzie widoczna.

Notatka

Proces skanowania może chwilę potrwać, w zależności od opcji skanowania.

Dostępne są trzy przyciski:

- **Stop** - pojawi się nowe okno, w którym możesz zakończyć proces skanowania. Kliknij **Tak** i **Zamknij** aby wyłączyć okno skanowania.

Notatka

Jeżeli w czasie skanowania wykryte zostaną podejrzane pliki zostaniesz poproszony o przekazanie ich do laboratorium BitDefender.

- **Pauza** - skanowanie zostanie chwilowo przerwane – możesz kontynuować skanowanie przez kliknięcie **Przywróć**.
- **Pokaż raport** - otwiera raport skanowania.

Notatka

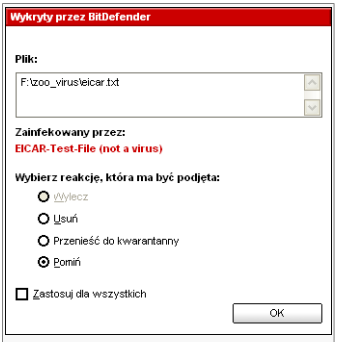
Jeżeli klikniesz prawym przyciskiem na uruchomione zadanie pojawi się skrócone menu pozwalające na zarządzanie oknem skanowania. Opcje (**Pauza/Wznów**, **Zatrzymaj** oraz **Zatrzymaj i Zamknij**) są podobne do tych w oknie skanowania.

Jeżeli opcja **Pytaj użytkownika o reakcję** jest włączona w oknie Właściwości, podczas wykrycia zagrożenia pojawi się okno z wyborem reakcji.

Możesz zobaczyć nazwę pliku i nazwę wirusa.

Możesz wybrać jedno z następujących działań na zainfekowanym pliku:

- **Wylecz** - leczy zainfekowany plik;
- **Usuń** - usuwa zainfekowany plik;
- **Przenieś do kwarantanny** - przenosi zainfekowany plik do strefy kwarantanny;
- **Pomiń** - aby zignorować infekcję. Nie będzie podejmowana żadna czynność na zainfekowanym pliku.



Wybór Reakcji

Jeżeli skanujesz folder i chcesz żeby czynność na zainfekowanych plikach była taka sama dla wszystkich pozostałych, wybierz opcję **Zastosuj dla wszystkich**.

Notatka

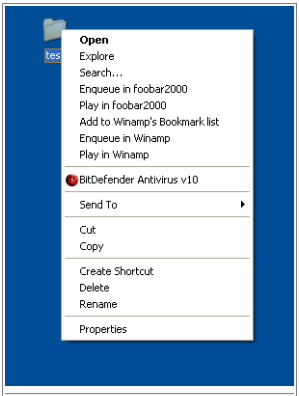
Jeżeli opcja **Wylecz** nie jest włączona, plik nie może być odinfekowany. Najlepiej usunąć plik lub przenieść do strefy kwarantanny i przesłać go do nas w celu analizy.

Kliknij **OK**.

Notatka

Plik raportu jest zapisywany automatycznie w sekcji Logi Skanowania w oknie **Właściwości**.

Skanowanie Kontekstowe



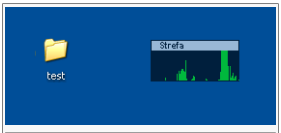
Skanowanie Kontekstowe

Kliknij prawym przyciskiem myszy plik lub folder, który ma być przeskanowany i wybierz opcję **BitDefender Antivirus v10**.

Możesz modyfikować opcje skanowania i zobaczyć pliki raportu poprzez dostęp do okna Właściwości zadania **Skanowanie Kontekstowe**

Skanowanie Przeciagnij i Upusc

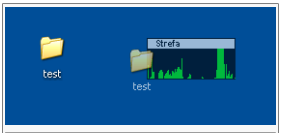
Przeciągnij plik lub folder, który chcesz żeby był przeskanowany i upuść na **Okienko Czynności Skanowania**, jak na obrazku poniżej.



Przeciągnij plik

Jeżeli zainfekowany plik zostanie wykryty pojawi się okno alarmowe z możliwością wyboru działania na zainfekowanym pliku.

W obydwu przypadkach pojawi się okno skanowania.



Upuść plik

7.2.5. Szukanie Rootkit'ów

BitDefender eliminuje najnowsze zagrożenia wprowadzając wykrywanie rootkit'ów wraz z wydajnymi silnikami skanującymi. BitDefender jest teraz w stanie wykryć rootkit'y

szukając ukrytych plików, folderów lub procesów. Ponadto może chronić Twój system zmieniając nazwy grożnych plików, które używają rootkit'y.

Aby przeskanować komputer pod kątem rootkit'ów uruchom zadanie **Szukaj Rootkit'ów**. pojawi się okno skanowania.

WAŻNE

Kiedy skanujesz komputer w poszukiwaniu rootkit'ów silnie zalecane jest ustawienie BitDefendera tak, aby nie wykonywał żadnej reakcji na ukryte pliki.

Na końcu skanowania możesz zobaczyć wyniki. Jeżeli ukryte pliki zostały wykryte sprawdź je uważnie: obecność ukrytych plików może oznaczać potencjalny atak.

Jeżeli jesteś pewien, że wykryty plik należy do oprogramowania złośliwego, zalecamy ustawienie reakcji **Zmień nazwę pliku** i uruchom ponownie zadanie **Szukaj Rootkit'ów**. Wtedy ukryte pliki zostaną zablokowane.

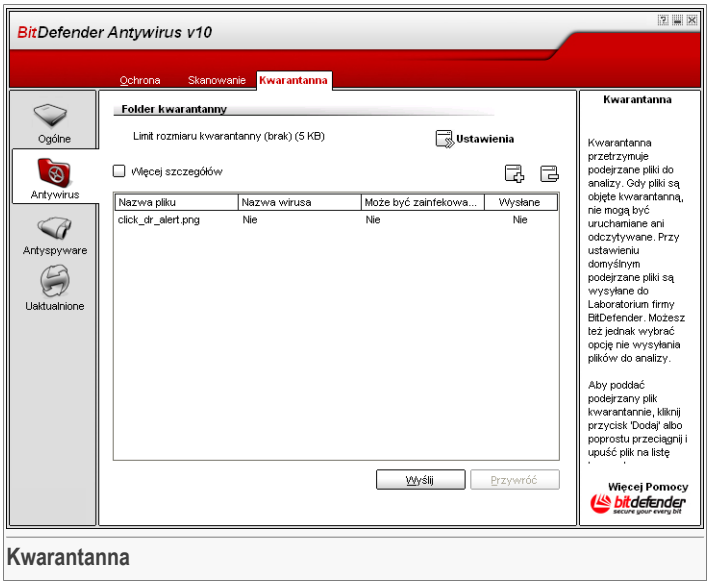
Ostrzeżenie

NIE WSZYSTKIE UKRYTE ELEMENTY SĄ OPROGRAMOWANIEM ZŁOŚLIWYM! Zanim zmienisz nazwę ukrytych plików sprawdź czy nie należą one do jakiejś aplikacji lub systemu. Zmiana nazwy tych plików może przerwać działanie systemu.

WAŻNE

Jeżeli Twój system został zaatakowany jest tylko jeden bezpieczny sposób całkowitego pozbycia się intruza: przeinstalowanie systemu.

7.3. Kwarantanna



Kwarantanna

BitDefender pozwala na izolowanie zainfekowanych lub podejrzanych plików w bezpiecznym obszarze o nazwie kwarantanna. Przez izolowanie tych plików w kwarantannie ryzyko zainfekowania znika i w tym samym czasie masz możliwość wysłać te pliki do laboratorium BitDefender w celu dalszej analizy.

Składnik zapewniający administrowanie odizolowanymi plikami nazywa się **Kwarantanna**. Moduł ten został zaprojektowany z funkcją automatycznego wysyłania zainfekowanych plików do laboratorium BitDefender.

Możesz zauważyć, że sekcja **Kwarantanna** zawiera listę wszystkich plików dotychczas odizolowanych. Każdy plik ma załącznik z nazwą, rozmiarem, datą izolacji i datą wysłania. Jeżeli chcesz zasięgnąć więcej informacji o plikach znajdujących się w kwarantannie, kliknij **Więcej informacji**.

Notatka

Kiedy wirus znajduje się w kwarantannie jest nieszkodliwy ponieważ nie może być wykonywany lub czytany.

Kliknij przycisk **Dodaj** aby dodać podejrzany plik do kwarantanny. Otworzy się okno, w którym będziesz mógł wybrać plik. Tym sposobem plik zostanie skopiowany do kwarantanny. Jeżeli chcesz przenieść plik do kwarantanny musisz zaznaczyć opcję **Usuń z pierwotnej lokalizacji**. Szybszym sposobem dodawania plików do kwarantanny jest metoda "przeciągnij i upuść".

Aby usunąć zaznaczony plik z kwarantanny kliknij przycisk **Usuń**. Jeżeli chcesz przywrócić zaznaczony plik do jego pierwotnej lokalizacji kliknij **Przywróć**.

Możesz wysłać zaznaczony plik z kwarantanny do laboratorium BitDefender klikając **Wyślij**.

WAŻNE

Musisz określić pewne informacje zanim prześlesz te pliki. Aby to zrobić kliknij **Ustawienia** i wypełnij pola z sekcji **Ustawienia wysyłania** jak opisano poniżej.

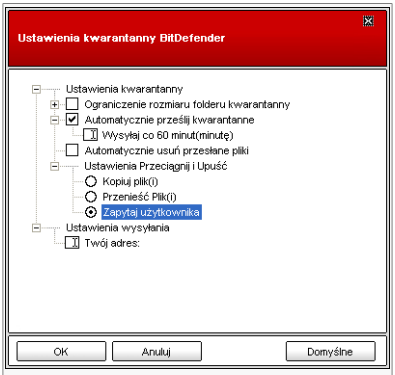
Kliknij **Ustawienia** aby otworzyć zaawansowane opcje dla strefy kwarantanny. Pojawi się nowe okno.

Opcje kwarantanny pogrupowane są w dwie kategorie:

- **Ustawienia kwarantanny**
- **Ustawienia wysyłania**

Notatka

Kliknij okienko "+" aby otworzyć opcję lub "-" aby zamknąć opcję.



Ustawienia Kwarantanny

Ustawienia kwarantanny

- **Ogranicz wielkość folderu kwarantanny** - utrzymuje pod kontrolą wielkość folderu kwarantanny. Domyślna wielkość wynosi 12000 kB. Jeśli chcesz zmienić tą wartość to wpisz nową wartość w odpowiednim polu.

Jeżeli zaznaczysz opcję **Automatycznie usuwaj stare pliki**, przy pełnym folderze kwarantanny, podczas dodawania nowego pliku najstarszy będzie usuwany w celu zwolnienia miejsca na nowy plik.

Notatka

Domyślnie, wielkość folderu kwarantanny nie jest ograniczona.

- **Automatycznie przeslij kwarantanne** - automatycznie wysyła pliki kwarantanny do laboratorium BitDefender w celu dalszej ich analizy. Możesz ustawić czas pomiędzy dwoma kolejnymi procesami wysyłania w minutach w polu **Wysylaj co x minut**.
- **Automatycznie usuń przeslane pliki** - automatycznie usuwa pliki znajdujące się w kwarantannie po wysłaniu ich do laboratorium BitDefender w celu dalszej ich analizy.
- **Ustawienia Przeciagnij i Upuść** - jeżeli używasz metody Przeciągnij i Upuść aby dodać pliki do kwarantanny tutaj możesz określić działanie: kopiowanie, przenoszenie lub działanie w prompt user.

Ustawienia wysyłania

- **Twój adres** - wprowadź swój adres email, jeżeli chcesz otrzymywać emalie dotyczące podejrzanych plików, od naszych specjalistów, wysłanych w celu wykonania analizy.

Automatycznie usuń przesłane pliki - automatycznie usuwa pliki znajdujące się w kwarantannie po wysłaniu ich do laboratorium BitDefender w celu dalszej analizy.

8. Moduł Antyspyware

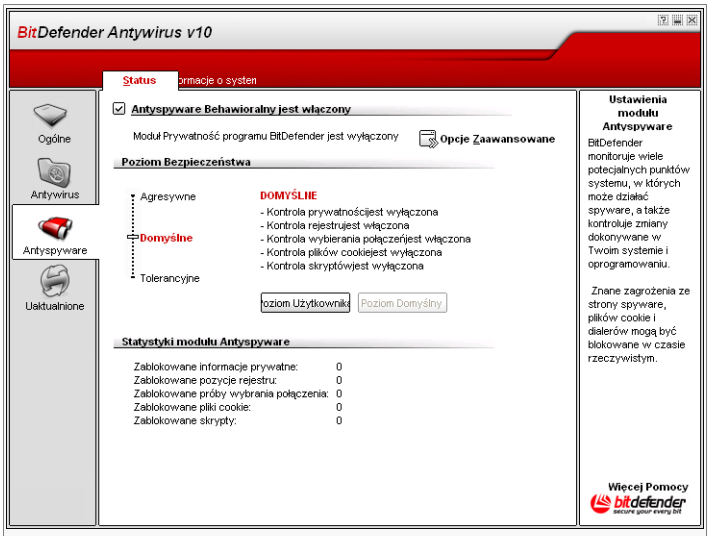
Rozdział **Antyspyware** tej instrukcji zawiera następujące tematy:

- Status Antyspyware'a
- Ustawienia Zaawansowane - Kontrola Prywatności
- Ustawienia Zaawansowane - Kontrola Rejestru
- Ustawienia Zaawansowane - Kontrola Połączeń Modemowych
- Ustawienia Zaawansowane - Kontrola Cookie
- Ustawienia Zaawansowane - Kontrola Skryptów
- Informacje Systemowe

Notatka

Szczegóły dotyczące modułu **Antyspyware** są umieszczone w rozdziale *„Moduł Antyspyware”* (p. 25).

8.1. Status Antyspyware'a



Status Antyspyware'a

W tej sekcji możesz konfigurować moduł **Antyspam Behawioralny** i możesz zobaczyć informacje dotyczące jego działania.

WAŻNE

Aby spyware nie mógł zainfekować Twojego komputera musisz mieć włączony **Antyspyware Behawioralny**.

W dolnej części tej sekcji możesz zobaczyć **Statystyki Antyspyware**.

Moduł **Antyspyware** chroni Twój komputer przed Antyspywarem poprzez zastosowanie pięciu ważnych kontroli:

- Kontrola Prywatności - chroni Twoje prywatne dane filtrując cały wychodzący ruch HTTP i SMTP zgodnie z regułami stworzonymi w sekcji Prywatność.
- Kontrola Rejestrów – pyta o Twoją zgodę za każdym razem, gdy jakiś program chce wprowadzić zmiany do rejestru.
- Kontrola Połączeń Modemowych - pyta o Twoją zgodę za każdym razem, gdy wykonywana jest próba połączenia z modemem.

- Kontrola Cookie - pyta o Twoją zgodę za każdym razem, gdy nowa strona chce ustawić cookie.
- Kontrola Skryptów - pyta o Twoją zgodę za każdym razem, gdy strona próbuje uruchomić skrypt lub inną aktywną zawartość.

Aby skonfigurować ustawienia dla tych kontroli kliknij Ustawienia Zaawansowane.

8.1.1. Poziom Bezpieczeństwa

Możesz wybrać poziom bezpieczeństwa, który najbardziej odpowiada Twoim potrzebom.

Dostępne są 3 poziomy bezpieczeństwa:

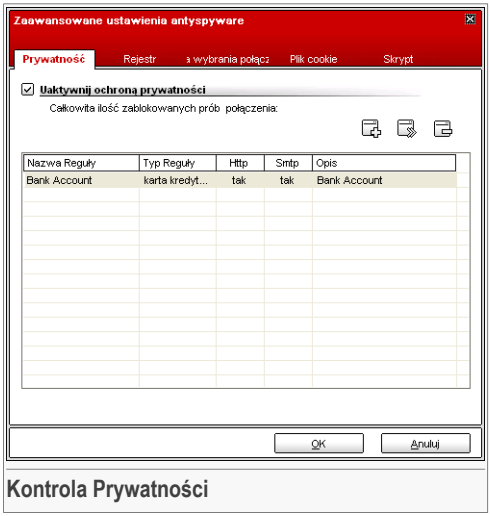
Poziom bezpieczeństwa	Opis
Tolerancyjny	Włączona jest tylko **Kontrola Rejestrów**
Domyślny	Włączone są **Kontrola Rejestrów** i **Kontrola Połączeń Modemowych**.
Agresywny	Włączone są **Kontrola Rejestrów**, **Kontrola Połączeń Modemowych** i **Kontrola Prywatności**.

Możesz dostosować poziom bezpieczeństwa klikając **Poziom Użytkownika**. Pojawi się okno, w którym możesz wybrać elementy BitDefender'a niezbędne do Twojej ochrony i kliknij **OK**.

Kliknij **Poziom Domyślny** aby uruchomić domyślne ustawienia.

8.2. Ustawienia Zaawansowane - Kontrola Prywatności

Aby wejść do tej sekcji kliknij przycisk **Ustawienia Zaawansowane** w module **Antyspyware**, w sekcji Status.



Kontrola Prywatności

Bezpieczeństwo prywatnych danych jest dla nas wszystkich bardzo ważne. Kradzieże danych opierają się na nowych metodach oszukiwania ludzi w celu zdobycia prywatnych informacji.

Nie ważne czy jest to Twój adres e-mail, czy też numer karty kredytowej, kiedy dostaną się w niepowołane ręce mogą spowodować szkody: będziesz zalewany spamem lub pozbędziesz się wszystkich środków na koncie.

Kontrola Prywatności pomoga zabezpieczyć prywatne dane. Skanuje ruch HTTP i SMTP pod kątem zdefiniowanych wzorów. Jeżeli konkretny wzór zostaje odnaleziony, strona bądź e-mail będzie zablokowana.

Reguły muszą być wprowadzane automatycznie (kliknij przycisk **Dodaj** i wybierz parametry dla reguły). Pojawi się kreator konfiguracji.

8.2.1. Kreator Konfiguracji

Kreator konfiguracji składa się z 3 kroków.

Krok 4/4 - Wybierz Dane i Typ Reguły

Wybierz Dane i Typ Reguły

Wpisz nazwę reguły w polu edycji.

Musisz ustawić następujące parametry:

- **Typ Reguły** - wybierz typ reguły (adres, imię, karta kredytowa, PIN, SSN itd.).
- **Dane Reguły** - wpisz dane reguły.

Wszystkie wprowadzane dane są szyfrowane.

Kliknij **Dalej**.

Krokp 2/3 - Wybierz Rodzaj Ruchu

Wybierz Rodzaj Ruchu

Wybierz rodzaj ruchu jaki ma być skanowany przez BitDefender'a. Dostępne są następujące opcje:

- **Skanuj HTTP** - skanuje ruch HTTP i blokuje wychodzące dane które pasują do wzoru.
- **Skanuj SMTP** - skanuje ruch SMTP i blokuje wszystkie wychodzące wiadomości e-mail, które zawierają zdefiniowane wzory.

Kliknij **Dalej**.

Krok 3/3 – Opisz Regułę

Opisz Regułę

Wprowadź krótki opis reguły w polu edycji.

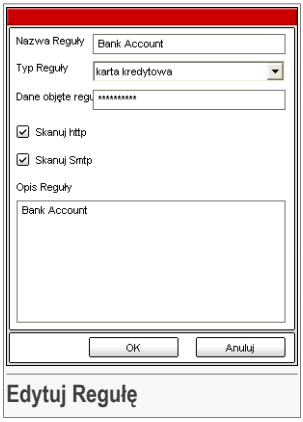
Kliknij **Zakończ**.

8.2.2. Zarządzanie Regułami

Możesz zobaczyć reguły umieszczone w tabeli.

Aby usunąć regułę z listy wybierz ją i kliknij przycisk **Usuń**. aby tymczasowo deaktywować regułę bez jej usuwania, odznacz odpowiednie okienko.

Aby edytować regułę zaznacz ją i kliknij **Edytuj** lub kliknij w nią dwukrotnie. Pojawi się nowe okno.



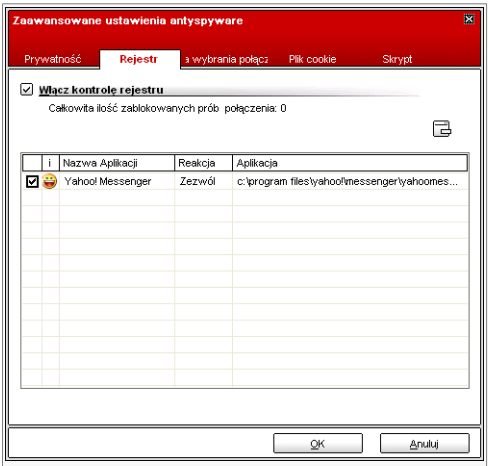
Edytuj Regułę

Możesz tutaj zmienić nazwę, opis i parametry reguły (typ, dane i ruch). Kliknij **OK** aby zachować zmiany.

Kliknij **OK** aby zapisać zmiany i zamknąć okno.

8.3. Ustawienia Zaawansowane - Kontrola Rejestru

Aby uzyskać dostęp do tej sekcji wejdź do okna **Zaawansowane Ustawienia Antyspyware** (idź do modułu **Antyspyware**, sekcji Status i kliknij **Ustawienia Zaawansowane**) i kliknij zakładkę **Rejestr**

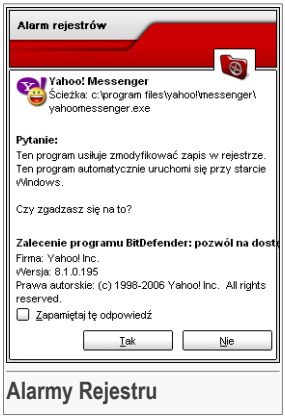


Kontrola Rejestru

Bardzo ważną częścią systemu operacyjnego Windows jest **Rejestr**. W tym miejscu Windows trzyma swoje ustawienia, zainstalowane programy, informacje użytkownika itd.

Rejestr jest także używany w celu określenia, które programy powinny być automatycznie uruchamiane, podczas startu Windows. Wirusy często wykorzystują ten fakt, aby automatycznie dostać się do systemu, kiedy użytkownik restartuje swój komputer.

Kontrola Rejestrów monitoruje rejestry Windows – jest to użyteczne przy wykrywaniu Koni Trojańskich. Kiedy program przy starcie Windows będzie próbował zmodyfikować rejestry zostaniesz o tym poinformowany.



Alarmy Rejestru

Możesz odrzucić modyfikację rejestrów poprzez kliknięcie **Nie** lub możesz zezwolić na nią przez kliknięcie **Tak**.

Jeżeli chcesz, aby BitDefender pamiętał twoją odpowiedź musisz zaznaczyć opcję: **Zapamiętaj tę odpowiedź**.

Notatka

Twoje odpowiedzi będą stanowiły podstawę listy reguł.

Aby usunąć wpis w rejestrze wybierz go i kliknij **Usuń**. Aby tymczasowo deaktywować wpis, bez jego usuwania, odznacz odpowiednią opcję.

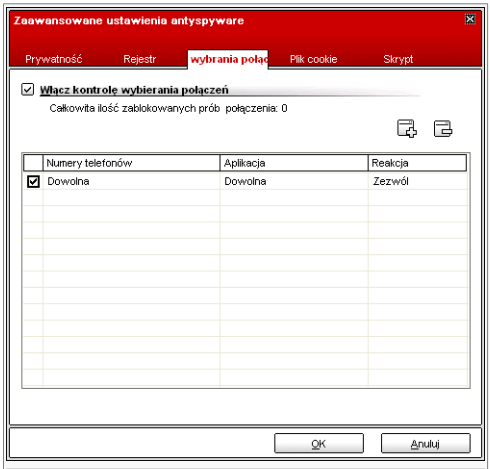
Notatka

BitDefender zwykle będzie cię ostrzegał, kiedy będziesz instalował nowe programy, które wymagają uruchomienia po restarcie komputera. W większości przypadków programy te są godne zaufania.

Kliknij **OK** aby zamknąć okno.

8.4. Zawansowane Ustawienia - Kontrola Połączeń Modemowych

Aby uzyskać dostęp do tej sekcji wejdź do okna **Zaawansowane Ustawienia Antyspyware** (idź do modułu **Antyspyware**, sekcji Status i kliknij **Ustawienia Zaawansowane**) i kliknij zakładkę **Połączenia**.



Kontrola Połączeń Modemowych

Dialery są aplikacjami, które używają modemów, aby łączyć się z różnymi numerami telefonicznymi. Zwykle dialery są wykorzystywane, aby zapewnić dostęp do różnych lokalizacji przez łączenie z drogimi numerami telefonów.

Z **Kontrolą Połączeń Modemowych** będziesz decydował o połączeniach z różnymi numerami telefonów. Funkcja ta monitoruje wszystkie połączenia modemu komputerowego, natychmiast ostrzegając użytkownika i ponaglając go, aby wybrał czy pozwala czy blokuje takie operacje:

Alarmy Połączeń

Możesz zobaczyć nazwę aplikacji i numer telefonu.

Wybierz **Zapamiętaj tę odpowiedź** i kliknij **Tak** lub **Nie** , a reguła zostanie utworzona i zapisana w tabeli reguł. Nie będziesz powiadamiany, kiedy dana aplikacja będzie próbowała łączyć się przez ten sam numer telefonu.

Do każdej reguły, która została zapamiętana, mamy dostęp w sekcji **Połączenia** .

WAŻNE

Reguły są ustawione według priorytetu, zaczynając od najwyższego. Uchwyć i przeciągnij reguły aby zmienić ich priorytet.

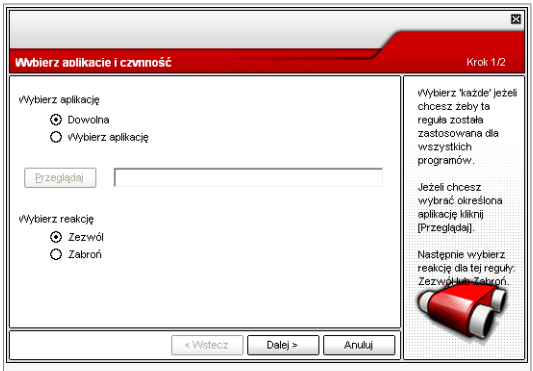
Aby usunąć regułę zaznacz ją i kliknij **Usuń**. Aby zmienić parametry reguły kliknij na nia dwukrotnie i wprowadź zmiany. Aby tymczasowo deaktywować regułę, bez jej usuwania, odznacz odpowiednią opcję.

Reguły mogą być wprowadzane automatycznie (przez okno alarmów) albo ręcznie (kliknij **Dodaj** i wybierz parametry dla reguły). Pojawi się kreator konfiguracji.

8.4.1. Kreator Konfiguracji

Kreator konfiguracji składa się z 2 kroków.

Krok 1/2 - Wybierz Aplikację i Reakcję



Wybierz Aplikację i Reakcję

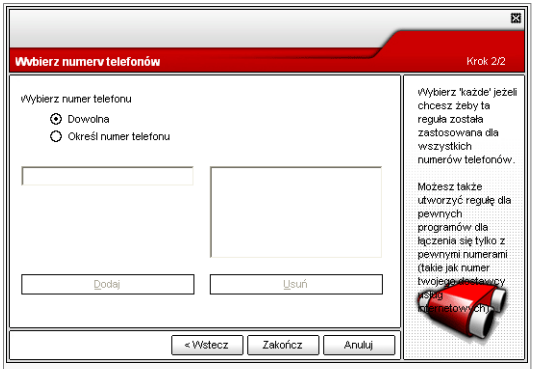
Możesz ustawić parametry:

- **Aplikacja** - wybierz aplikację dla tej reguły. Możesz wybrać wyłącznie jedną aplikację (kliknij **Wybierz aplikację**, potem **Przeglądaj** i wybierz daną aplikację) lub wszystkie aplikacje (kliknij **Każda**).
- **Reakcja** - wybierz działanie reguły.

Działanie	Opis
Zezwól	Akcja będzie dozwolona.
Zabroń	Akcja będzie zabroniona.

Kliknij **Dalej**.

Krok 2/2 - Wybierz numery telefonu



Wybierz numery telefonu

Wybierz **Wprowadź numer telefonu**, wpisz numer telefonu, dla którego tworzysz regułę i kliknij **Dodaj**.

Notatka

Możesz użyć listy zakazanych numerów telefonów, np. 1900* oznacza, że wszystkie numery telefonów rozpoczynające się od 1900 będą blokowane.

Wybierz **Każdy** jeżeli chcesz aby ta reguła była zastosowana dla każdego numeru telefonu. Jeżeli chcesz usunąć numer, wybierz go i kliknij **Usuń**.

Notatka

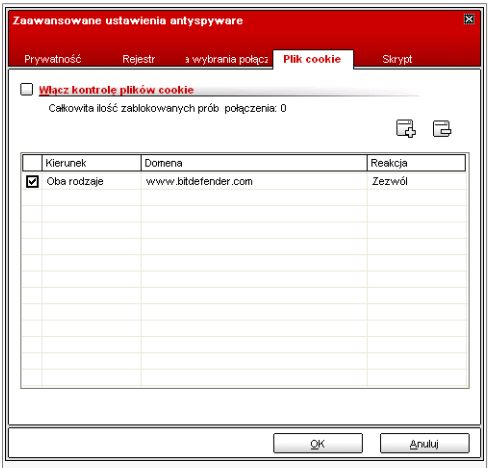
Możesz także utworzyć regułę, która pozwoli danemu programowi łączyć się tylko z określonymi numerami (np. twój dostawca usług internetowych lub numer faksu).

Kliknij **Zakończ**.

Kliknij **OK** aby zapisać zmiany i zamknąć okno.

8.5. Ustawienia Zaawansowane - Kontrola Cookie

Aby uzyskać dostęp do tej sekcji wejdź w okno **Zaawansowane ustawienia Antyspyware** (idź do modułu **Antyspyware**, sekcji Status i kliknij **Ustawienia Zaawansowane**) i kliknij zakładkę **Cookie**.



Kontrola Cookie

Cookie występują powszechnie w internecine. Są one małymi plikami przechowywanymi w twoim komputerze. Strony internetowe tworzą je, aby śledzić szczegółowe informacje na Twój temat.

Cookie są tworzone po to, aby ułatwiać Tobie pracę. Np. mogą pomóc stronie internetowej zapamiętać twoje imię i preferencje tak abyś nie musiał wpisywać ich za każdym razem.

Ale cookie mogą także zagrażać Twojej prywatności np. poprzez śledzenie twojego ruchu w internecine.

W tym przypadku pomaga **Kontrola Cookie**. Kiedy jest włączona będzie za każdym razem pytać o pozwolenie, kiedy nowa strona sieci będzie próbowała ustawić cookie:

Alarmy Cookie

Możesz zobaczyć nazwę aplikacji, która próbuje wysłać plik cookie.

Wybierz **Zapamiętaj tę odpowiedź** i kliknij **Tak** lub **Nie** a reguła będzie utworzona i zapisana w tabeli reguł. Nie będziesz więcej powiadamiany, kiedy będziesz próbował połączyć się z tą samą stroną.

Pomoże to w podjęciu decyzji, które strony są zaufane, a które nie.

Notatka

Z powodu dużej ilości cookie wykorzystywanych w internecie **Kontrola Cookie** może sprawić trochę kłopotów. Na początku będzie zadawanych dużo pytań o strony próbujące umiejscowić cookie na twoim komputerze. Jeżeli dodasz swoje regularnie odwiedzane strony do listy reguł, poruszanie się po internecie będzie tak łatwe, jak poprzednio.

Do każdej reguły, mamy dostęp w sekcji **Cookie**.

WAŻNE

Reguły są ustawione według priorytetu, zaczynając od najwyższego. Uchwyć i przeciągnij reguły aby zmienić ich priorytet.

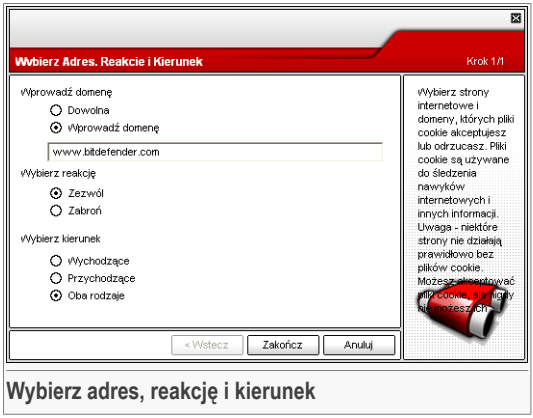
Aby usunąć regułę zaznacz ją i kliknij **Usuń**. Aby zmienić parametry reguły kliknij na nia dwukrotnie i wprowadź zmiany. Aby tymczasowo deaktywować regułę, bez jej usuwania, odznacz odpowiednią opcję.

Reguły mogą być wprowadzane automatycznie (przez okno alarmów) albo ręcznie (kliknij **Dodaj** i wybierz parametry dla reguły). Pojawi się kreator konfiguracji.

8.5.1. Kreator Konfiguracji

Kreator konfiguracji składa się z 1 kroku.

Krok 1/1 - Wybierz adres, reakcję i kierunek.



Wybierz adres, reakcję i kierunek

Możesz ustawić parametry:

- **Adres domeny** - wpisz w domenę, do której reguła ma być zastosowana.
- **Reakcja** - wybierz działanie reguły.

Działanie	Opis
Zezwól	Cookie w domenie będą wykonane.
Zabroń	Cookie w domenie nie będą wykonane.

- **Kierunek** - wybierz kierunek ruchu.

Typ	Opis
Wychodzący	Reguła będzie zastosowana wyłącznie dla cookie, które są wysłane do połączonych stron.
Przychodzący	Reguła będzie zastosowana wyłącznie dla cookie, które są otrzymane z połączonych stron.
Oba kierunki	Reguła będzie dotyczyła obu kierunków.

Kliknij **Zakończ**.

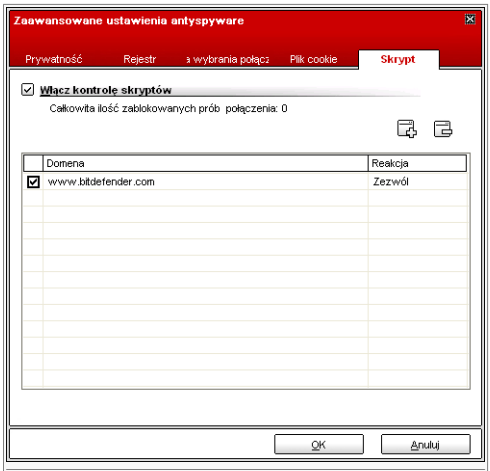
Notatka

Możesz zaakceptować cookie, ale nigdy nie ustawiaj reakcji na **Zabroń** i kierunek na **Wychodzące**.

Kliknij **OK** aby zapisać zmiany i zamknąć okno.

8.6. Zawansowane Ustawienia - Kontrola Skryptu

Aby uzyskać dostęp do tej sekcji wejdź do okna **Zaawansowane Ustawienia Antyspyware** (idź do modułu **Antyspyware**, sekcji Status i kliknij **Ustawienia Zaawansowane**) i kliknij akładkę **Skrypt**.

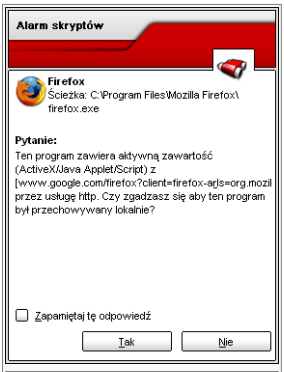


Kontrola Skryptów

Scripty i inne kody takie jak Kontrole ActiveX i Java applets, które są wykorzystywane do tworzenie interaktywnych stron w sieci. Mogą być zaprogramowane aby wywoływać szkodliwe efekty. Elementy ActiveX mogą. mieć m.in całkowity dostęp do twoich danych oraz mogą czytać dane z twojego komputera, usuwać informacje, łamać hasła i przchwytywać wiadomości gdy masz włączony internet. Powinieneś akceptować wyłącznie aktywne składniki ze stron, które dobrze znasz i którym w pełni ufasz.

BitDefender pozwala wybrać uruchamianie tych elementów albo blokować ich wykonywanie.

Ze **Skryptem Kontroli** będziesz decydował, którym stronom sieci ufasz, a którym nie. BitDefender będzie cię prosił o pozwolenie za każdym razem gdy strona sieci będzie próbowała aktywować skrypt lub inny aktywny składnik:



Alarm skryptów

Możesz obejrzeć nazwę źródła.

Wybierz **Zapamiętaj tę odpowiedź** i kliknij **Tak** lub **Nie** a reguła będzie utworzona, zastosowana i zapisana w tabeli reguł. Nie będziesz powiadamiany, kiedy ta sama strona będzie próbowała wysłać tobie aktywny składnik.

Do każdej reguły, która została zapamiętana, jest dostęp w sekcji **Skrypt** w celu dalszych dostrojeń.

WAŻNE

Reguły są ustawione według priorytetu, zaczynając od najwyższego. Uchwyć i przeciągnij reguły aby zmienić ich priorytet.

Aby usunąć regułę zaznacz ją i kliknij **Usuń**. Aby zmienić parametry reguły kliknij na nia dwukrotnie i wprowadź zmiany. Aby tymczasowo deaktywować regułę, bez jej usuwania, odznacz odpowiednią opcję.

Reguły mogą być wprowadzane automatycznie (przez okno alarmów) albo ręcznie (kliknij **Dodaj** i wybierz parametry dla reguły). Pojawi się kreator konfiguracji.

8.6.1. Kreator Konfiguracji

Kreator konfiguracji składa się z 1 kroku.

Krok 1/1 - Wybierz adres i działanie

Wybierz adres i działanie

Możesz ustawić parametry:

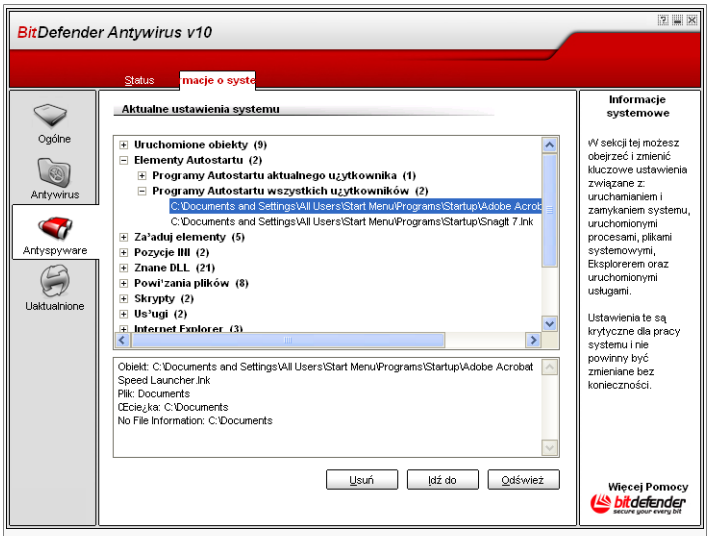
- **Adres domeny** - wpisz w domenę, do której reguła ma być zastosowana.
- **Reakcja** - wybierz działanie reguły.

Działanie	Opis
Zezwól	Skrypty w domenie będą wykonane.
Zabroń	Skrypty w domenie nie będą wykonane.

Kliknij **Zakończ**.

Kliknij **OK** aby zapisać zmiany i zamknąć okno.

8.7. Informacje Systemowe



Informacje Systemowe

Tutaj możesz zobaczyć i zmienić opcje klucza.

Lista zawiera wszystkie elementy wczytane podczas startu systemu jak również pozycje wczytane przez inne aplikacje.

Dostępne są trzy przyciski:

- **Usuń** - usuwa wybrany element.
- **Idź do** - otwiera okno gdzie znajduje się wybrany element (na przykład **Rejestr**).
- **Odśwież** - ponownie otwiera sekcję **System**.

9. Moduł Aktualizacji

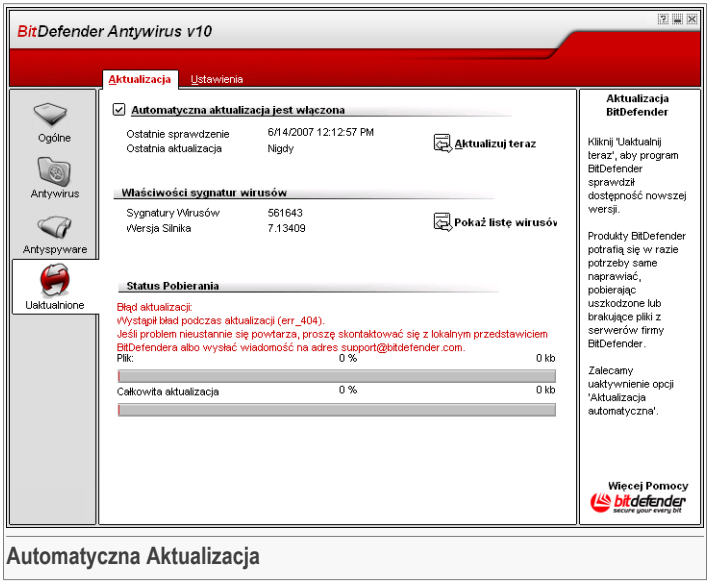
Sekcja **Aktualizacja** tej instrukcji zawiera następujące tematy:

- Automatyczna Aktualizacja
- Ręczna Aktualizacja
- Ustawienia Aktualizacji

Notatka

Aby uzyskać więcej szczegółów dotyczących modułu **Aktualizacja** sprawdź opis *„Moduł Aktualizacji”* (p. 26).

9.1. Automatyczna Aktualizacja



Automatyczna Aktualizacja

W tym dziale znajdziesz informacje dotyczące aktualizacji i zaktualizować produkt.

WAŻNE

Aby być chronionym przed najnowszymi zagrożeniami miej włączony moduł **Automatyczna Aktualizacja**.

Jeśli jesteś podłączony do Internetu za pomocą łącza szerokopasmowego BitDefender sam o siebie zadba. Sprawdza dostępność nowych sygnatur podczas uruchamiania komputera, a następnie co **godzinę**.

Jeżeli aktualizacja jest dostępna to zależnie od ustawień w Opcje automatycznej aktualizacji, zostaniesz zapytany czy chcesz aktualizować program lub aktualizacja zostanie przeprowadzona automatycznie.

Automatyczna aktualizacja może być także przeprowadzona w dowolnym czasie, klikając **Aktualizuj Taraz**. Ten rodzaj aktualizacji znany jest także jako **Aktualizacja na żądanie**.

Moduł **Aktualizacja** połączy się z serwerami aktualizacji BitDefender i sprawdzi czy są dostępne aktualizacje. Jeśli będą dostępne aktualizacje to zależnie od ustawień w Ustawienia ręcznej aktualizacji, zostaniesz zapytany czy chcesz aktualizować program albo aktualizacja zostanie przeprowadzona automatycznie.

WAŻNE

Może okazać się, że będziesz musiał ponownie uruchomić komputer po zakończeniu aktualizacji. Zalecamy to zrobić jak najszybciej.

Notatka

Jeśli łączysz się z Internetem za pomocą modemu to dobrym pomysłem są regularne aktualizacje BitDefender na żądanie.

Możesz pobrać nowe sygnatury BitDefender klikając **Pokaż listę wirusów**. Stworzony zostanie plik w formacie HTML, który będzie zawierał wszystkie dostępne sygnatury. Kliknij ponownie **Pokaż Listę Wirusów** aby zobaczyć listę. Możesz przeszukać bazę danych pod kątem konkretnego zagrożenia lub kliknąć **Lista Wirusów BitDefender** aby przejść do bazy online.

9.2. Ręczne Aktualizacje

Metoda ta pozwala na instalacje najnowszych sygnatur wirusów. Aby zainstalować najnowsze wersje programu należy użyć opcji Automatyczna aktualizacja.

WAŻNE

Użyj ręcznej aktualizacji wtedy, kiedy automatyczna aktualizacja nie może być wykonana albo komputer nie jest podłączony do Internetu.

Są dwa sposoby wykonania ręcznej aktualizacji:

- Za pomocą pliku `weekly.exe`;
- Za pomocą `archiwów zip`.

9.2.1. Ręczna Aktualizacja za pomocą `weekly.exe`

Pakiet aktualizacji `weekly.exe` jest wydawane w każdy piątek i zawiera aktualizacje sygnatur wirusów i silników antywirusowych dostępne w dniu wydania.

Aby zaktualizować BitDefender używając `weekly.exe`, należy wykonać następujące kroki:

1. Pobrać plik weekly.exe i zapisać na twardym dysku.
2. Zlokalizaować pobrany plik i dwukrotnie kliknąć go aby uruchomić kreatora aktualizacji.
3. Kliknij **Dalej**.
4. Zaznaczyć **Akceptuję warunki Umowy Licencyjnej** i kliknąć **Dalej**.
5. Kliknąć **Instaluj**.
6. Kliknij **Zakończ**.

9.2.2. Ręczna aktualizacja za pomocą `archiwów zip`

Są dwa archiwa zip na serwerze aktualizacji, zawierające aktualizacje silników antywirusowych i sygnatury wirusów: `cumulative.zip` i `daily.zip`.

- `cumulative.zip` jest wypuszczane w każdy poniedziałek i zawiera aktualizacje sygnatur wirusów i silników antywirusowych dostępne w dniu wydania.
- `daily.zip` jest wydawany codziennie i zawiera wszystkie aktualizacje definicji wirusów oraz silników antywirusowych od ostatniego cumulative do aktualnego dnia.

BitDefender bazuje na architekturze usług. Zatem procedura aktualizacji różni się w zależności od systemu operacyjnego:

- Windows NT-SP6, Windows 2000, Windows XP, Windows Vista.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP, Windows Vista

Kroki do wykonania:

1. **Pobierz odpowiednie aktualizacje.** Jeśli jest poniedziałek, to pobierz cumulative.zip i zapisz gdzieś na dysku. W innym wypadku pobierz daily.zip i zapisz na dysku. Jeśli jest to pierwsza taka aktualizacja to pobierz oba archiwa.

2. **Zatrzymaj ochronę antywirusową BitDefender.**
   - **Wyłącz konsolę zarządzającą BitDefender.** Kliknij prawym przyciskiem myszki ikonę BitDefender w pasku systemowym i wybierz **Zakończ**.
   - **Otwórz Usługi.** Kliknij **Start**, potem **Panel Sterowania**, dwukrotnie kliknij **Narzędzia Administracyjne** i kliknij **Usługi**.
   - **Zatrzymaj usługę BitDefender Virus Shield.** Wybierz usługę **BitDefender Virus Shield** z listy i kliknij **Zatrzymaj**.
   - **Zatrzymaj usługę BitDefender Scan Server.** Wybierz usługę **BitDefender Scan Server** z listy i kliknij **Zatrzymaj**.
3. **Rozpakuj zawartość archiwum.** Rozpocznij od `cumulative.zip` gdy aktualizujesz za pomocą obu archiwów. Rozpakuj zawartość do folderu `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` i zaakceptuj nadpisanie istniejących plików.
4. **Uruchom ponownie ochronę antywirusową BitDefender.**
   - **Uruchom usługę BitDefender Scan Server.** Wybierz usługę **BitDefender Scan Server** z listy i kliknij **Uruchom**.
   - **Uruchom usługę BitDefender Virus Shield.** Wybierz usługę **BitDefender Virus Shield** z listy i kliknij **Uruchom**.
   - **Otwórz konsolę zarządzającą BitDefender.**

Notatka

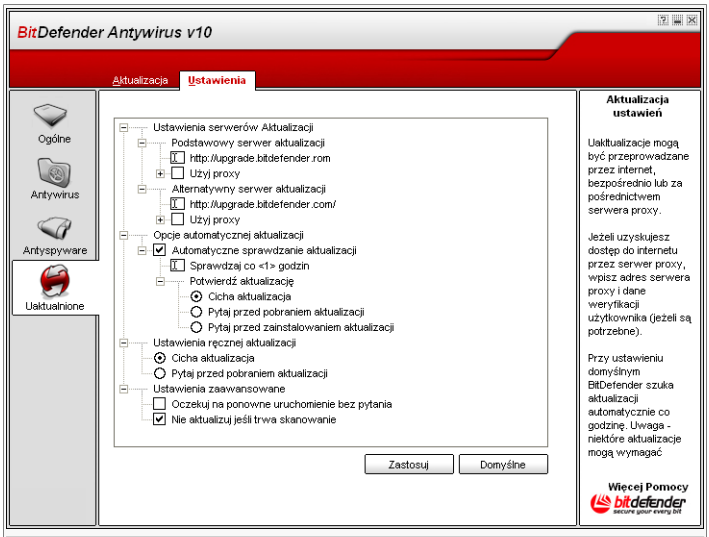
Jeżeli masz zainstalowane Windows Vista, zostaniesz poproszony o potwierdzenie większości opcji.

Windows 98, Windows Millennium

Kroki do wykonania:

1. **Pobierz odpowiednie aktualizacje.** Jeśli jest poniedziałek, to pobierz cumulative.zip i zapisz gdzieś na dysku. W innym wypadku pobierz daily.zip i zapisz na dysku. Jeśli jest to pierwsza taka aktualizacja to pobierz oba archiwa.
2. **Rozpakuj zawartość archiwum.** Rozpocznij od `cumulative.zip` gdy aktualizujesz za pomocą obu archiwów. Rozpakuj zawartość do folderu `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` i zaakceptuj nadpisanie istniejących plików.
3. **Uruchom ponownie komputer.**

9.3. Ustawienia Aktualizacji



Ustawienia Aktualizacji

Aktualizacje mogą być preprowadzone z lokalnej sieci, bezpośrednio przez Internet lub przez serwer proxy.

Okno ustawień aktualizacji zawiera 4 opcje (**Ustawienia miejsca aktualizacji**, **Opcje automatycznej aktualizacji**, **Ustawienia ręcznej aktualizacji** i **Opcje zaawansowane**) zorganizowane w rozwijane menu, podobne do tych z Windows.

Notatka

Kliknij, na „+” aby otworzyć kategorię, lub kliknij, na „-” aby zamknąć kategorię.

9.3.1. Ustawienia Miejsca Aktualizacji

Dla pewniejszych i szybszych aktualizacji, możesz ustawić dwie lokalizacje aktualizacji: **Podstawowy serwer aktualizacji** i **Alternatywny serwer aktualizacji**. Dla obu z nich musisz skonfigurować następujące opcje:

- **Miejsce aktualizacji** - Jesli jesteś podłączony do lokalnej sieci, w której sygnatury wirusów są umiejscowione lokalnie możesz zmienić lokalizacje aktualizacji. Domyślnie jest ustawione na: http://upgrade.bitdefender.com.
- **Użyj proxy** - w przypadku gdy firma używa serera proxy zaznacz tą opcje. Poniższe ustawienia muszą być sprecyzowane:
  - **Ustawienia proxy** - wpisz adres IP albo nazwę serwera proxy i port który BitDefender będzie używał do łaczenia się z serwerem proxy.

    WAŻNE
    Składnia: `nazwa:port` lub `ip:port`.

  - **Użytkownik proxy** - wpisz nazwę użytkownika rozpoznawanego przez proxy.

    WAŻNE
    Składnia: `domena\użytkownik`.

  - **Hasło proxy** - wpisz poprawne hasło dla wcześniej wpisanego użytkownika.

9.3.2. Opcje Automatycznej Aktualizacji

- **Automatyczne sprawdzanie aktualizacji** - BitDefender automatycznie sprawdza dostępność aktualizacji na naszych serwerach.
- **Sprawdzaj co x godzin** - Ustawia jak często BitDefender sprawdza dostępność aktualizacji. Domyślnie BitDefender będzie automatycznie aktualizowany co godzinę.
- **Cicha aktualizacja** - BitDefender automatycznie pobiera i implementuje aktualizacje.
- **Pytaj przed pobraniem aktualizacji** - za każdym razem, gdy jest dostępna aktualizacja, zostaniesz zapytany przed pobraniem.
- **Pytaj przed instalacją** - za każdym razem, gdy aktualizacja zostanie pobrana zostaniesz zapytany przed jej zainstalowaniem.

WAŻNE
Jeżeli wybierzesz **Pytaj przed pobraniem** lub **Pytaj przed instalacją** oraz zamkniesz wyjdź z konsoli zarządzającej to automatyczne aktualizacje nie zostaną wykonane.

9.3.3. Ustawienia Ręcznej Aktualizacji

- **Cicha aktualizacja** - ręczna aktualizacja zostanie przeprowadzona automatycznie w tle.
- **Pytaj przed pobraniem** - za każdym razem gdy uruchomisz ręczną aktualizacje zostaniesz zapytany przed pobraniem i zainstalowaniem aktualizacji.

WAŻNE

Jeżeli wybierzesz **Pytaj przed pobraniem** oraz zamkniesz wyjdź z konsoli zarządzającej to automatyczne aktualizacje nie zostaną wykonane.

9.3.4. Opcje Zaawansowane

- **Oczekuj na ponowne uruchomienie bez pytania** - jeśli aktualizacja wymaga restartu, program będzie pracował na starych plikach do momentu ponownego uruchomienia komputera. Użytkownik nie zostanie poproszony o ponowne uruchomienie komputera dzięki temu aktualizacja nie będzie przeszkadzała użytkownikowi w pracy.
- **Nie aktualizuj jeśli trwa skanowanie** - BitDefender nie przeprowadza aktualizacji, gdy trwa proces skanowania. Dzięki temu proces aktualizacji programu BitDefender nie zakłóci skanowania.

Notatka

Jeżeli program BitDefender będzie aktualizowany w trakcie procesu skanowania, wtedy skanowanie zostanie przerwane.

Kliknij **Zastosuj** aby zapisać zmiany albo kliknij **Domyślne** aby wczytać domyślne ustawienia.

Zasady dobrego postępowania

10. Zasady dobrego postępowania

Rozdział **Praktyczne wskazówki** tej instrukcji zawierają następujące tematy:

- Jak Chronić Komputer przed Zagrożeniami
- Jak Skonfigurować Zadania Skanowania

10.1. Jak Chronić Komputer przed Zagrożeniami

Podążaj za tymi krokami, aby zabezpieczyć komputer przed wirusami, spyware'ami i innymi zagrożeniami:

1. **Przejdź przez początkowego kreatora instalacji.** Podczas instalacji pojawi się kreator. Pomoże on zarejestrować BitDefender i stworzyć konto BitDefender. Ponadto pomoże Ci ustawić BitDefender'a tak, aby wykonywał najważniejsze zadania bezpieczeństwa.

   WAŻNE

   Jeżeli posiadasz dysk ratunkowy BitDefender przeskanuj swój system przed instalacją BitDefender'a, aby upewnić się, że nie masz żadnych wirusów.

2. **Uaktualnij BitDefender'a.** Jeżeli nie przeszedłeś przez początkowego kreatora instalacji, wykonaj aktualizację na żądanie (idź do modułu **Aktualizacja**, sekcji Aktualizacja i kliknij **Zaktualizuj Teraz**).

3. **Wykonaj pełne skanowanie systemu.** Wejdź do modułu **Antywirus**, sekcji Ochrona i kliknij **Skanuj Teraz**.

   Notatka

   Możesz także rozpocząć pełne skanowanie systemu z sekcji Skanuj. Wybierz zadanie **Pełne Skanowanie Systemu** i kliknij **Uruchom Zadanie**.

4. **Zapobiegaj infekcjom.** W sekcji **Ochrona** włącz opcję ochrona czasu rzeczywistego, aby być chronionym przed wirusami, spyware'ami i innymi zagrożeniami. Ustaw poziom bezpieczeństwa na taki, który najbardziej odpowiada Twoim potrzebom. Możesz użyć opcji dostosuj klikając **Poziom Użytkownika**.

   WAŻNE

   Ustaw BitDefender Antywirus v10 tak, aby skanował system przynajmniej raz na tydzień używając w terminarzu **Pełne Skanowanie Systemu** w sekcji Skanuj.

5. **Utrzymuj BitDefender'a zaktualizowanego.** W module **Aktualizacja**, sekcji Aktualizacja kliknij **Automatyczna Aktualizacja**.
6. **Zaplanuj pełne skanowanie systemu.** Idź do sekcji **Skanuj** i ustaw BitDefendera aby skanował twój system przynajmniej raz w tygodniu przy pomocy zadania **Pełne Skanowanie Systemu**.

10.2. Jak skonfigurować Zadanie Skanowania

Podążaj za następującymi krokami aby stworzyć i skonfigurować zadanie skanowania:

1. **Utwórz nowe zadanie.** Idź do sekcji Skanuj i kliknij **Nowe Zadanie**. Pojawi się okno Właściwości.

Notatka

Możesz także utworzyć nowe zadanie poprzez duplikację już istniejącego zadania. Aby to zrobić kliknij prawym przyciskiem na zadanie i zaznacz **Duplikuj** ze skróconego menu. Zaznacz duplikat i kliknij **Właściwości**, aby otworzyć okno **Właściwości**.

2. **Ustaw poziom skanowania.** Idź do sekcji **Przegląd** aby ustawić poziom skanowania. Jeżeli chcesz możesz dostosować ustawienia skanowania poprzez kliknięcie **Użytkownika**.
3. **Ustaw cel skanowania:** Idź do sekcji **Ścieżka Skanowania** i wybierz elementy, które chcesz przeskanować.
4. **Zaplanuj zadanie.** Jeżeli zadanie skanowania jest złożone, może okazać się, że będziesz musiał je zaplanować. Pomoże to BitDefenderowi wykonać dokładne skanowanie systemu. Idź do sekcji **Terminarz** aby zaplanować zadanie.

Dysk Ratunkowy BitDefender

BitDefender Antywirus v10 jest dostarczany z bootowalnym CD (Dysk Ratunkowy BitDefender Bazujący na LinuxDefender) zdolnym do skanowania i leczenia wszystkich istniejących dysków twardych zanim system operacyjny zostanie uruchomiony.

Powinieneś użyć Dysku Ratunkowego BitDefender za każdym razem, gdy twój system przestanie pracować poprawnie z powodu infekcji wirusami. Taka sytuacja występuje zawyczaj wtedy, gdy nie jest używany żaden program antywirusowy.

Aktualizacja sygnatur wirusów jest wykonywana automatycznie, bez interwencji użytkownika przy każdym uruchomieniu Dysku Ratunkowego BitDefender.

LinuxDefender jest przerobioną przez BitDefender dystrybucją Knoppix, która integruje najnowsze rozwiązanie bezpieczeństwa BitDefender dla Linux w GNU/Linux Knoppix Live CD, oferując stałą ochronę SMTP antywirus/antyspam i desktopowy program antywirusowy, który może skanować i odinfekować istniejące dyski (nawet partycje Windows NTFS), udostępnione Samba/Windows lub punkty montowania NFS. Zawiera także interfejs konfiguracji typu web-based.

11. Przegląd

Najważniejsze Cechy

- Stała ochrona email (Antywirus & Antyspam)
- Rozwiązanie Antywirusowe dla twojego dysku twardego
- Wsparcie zapisu NTFS
- Leczenie zainfekowanych plików z partycji Windows XP

11.1. Co to jest KNOPPIX?

http://knopper.net/knoppix:

„ KNOPPIX is a bootable CD with a collection of GNU/Linux (http://www.linux.com/) software, automatic hardware detection, and support for many graphic cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk. ”

11.2. Wymagania systemowe

Przed uruchomieniem LinuxDefender, sprawdź czy twój system spełnia poniższe wymagania.

Typ Procesora
Kompatybilny z x86, minimum 166 MHz, ale nie oczekuj wysokiej wydajności w tym przypadku. Zalecamy procesor generacji i686 z 800MHz.

Pamięć
Minimalnie 64MB, zalecane jest 128MB dla lepszej wydajności.

CD-ROM
LinuxDefender uruchamiany jest z CD-ROM-u, ponadto CD-ROM i BIOS zdolny do bootowania z niego jest wymagany.

Połączenie z Internetem
Mimo że LinuxDefender uruchomi się bez połączenia z Internetem, procedury aktualizacji wymagają aktywnego linka HTTP, nawet przez serwer proxy. Ponadto dla zaktualizowanej ochrony połączenie z Internetem jest WYMAGANE.

Rozdzielczość ekranu

Zalecana rozdzielczość ekranu to conajmniej 800x600 dla administracji web-based.

11.3. Dołączone oprogramowanie

Dysk Ratunkowy BitDefender zawiera następujące pakiety oprogramowania.

- BitDefender SMTP Proxy (Antyspam i Antywirus)
- BitDefender Remote Admin (konfiguracja web-based)
- BitDefender Linux Edition (skaner antywirusowy) +Interfejs GTK
- Dokumentacja BitDefender (w formacie PDF i HTML)
- BitDefender Extras (Artwork, Leaflets)
- Linux-Kernel 2.6
- Captive NTFS write project
- LUFS - Linux Userland File System
- Narzędzia do odzyskiwania danych i naprawy systemu, nawet dla innych systemów operacyjnych
- Narzędzia alalizy sieci i bezpieczeństwa dla administratorów sieci
- Amanda backup solution
- thttpd
- Analizator ruchu internetowego Ethereal, IPTraf IP LAN Monitor
- Nessus audytor bezpieczeństwa sieci
- Parted, QTParted i partimage, zmiany wielkości partycji, rozwiązania zapisywania i odzyskiwania
- Adobe Acrobat Reader
- Przeglądarka Mozilla Firefox

11.4. BitDefender rozwiązania Linux Security

LinuxDefender CD zawiera BitDefender SMTP Proxy Antywirus/Antyspam dla Linux, BitDefender Remote Admin (interfejs web-based do konfiguracji BitDefender SMTP Proxy) i BitDefender Linux Edition skaner antywirusowy.

11.4.1. BitDefender SMTP Proxy

BitDefender dla Linux Mail Servers - SMTP Proxy jest bezpiecznym rozwiązaniem nadzoru zawartości, które dostarcza ochronę antywirusową i antyspamową na poziomie bramy, skanując cały ruch e-mail i sprawdzając czy nie zawierją złośliwego oprogramowania. Unikalna własna technologia BitDefender dla Mail Servers jest kompatybilna z głownymi istniejącymi platformami e-mail i certyfikowana jako "RedHat Ready".

Te rozwiązanie Antywirusowe i Antyspamowe skanuje, odinfekowywuje i filtruje ruch email dla każdego istniejącego serwera poczty, bez względu na platformę i system operacyjny. BitDefender SMTP Proxy uruchamia się podczas bootowania i scanuje cały wchodzący ruch email. Aby skonfigurować BitDefender SMTP Proxy użyj BitDefender Remote Admin według instrukcji poniżej.

11.4.2. BitDefender Remote Admin

Możesz skonfigurować i zarządzać usługami BitDefender zdalnie (po skonfigurowaniu sieci) albo lokalnie, po wykonaniu następujących kroków:

1. Uruchom przeglądarkę Firefox i uruchom BitDefender Remote Admin URL: https://localhost:8139 (albo dwukrotnie kliknij ikonę BitDefender Remote Admin na pulpicie)
2. Zaloguj się jako użytkownik "bd" z hasłem "bd"
3. Wybierz "SMTP Proxy" z lewego menu
4. Ustaw Real SMTP server i nasłuchujący port
5. Dodaj domenę email do relay
6. Dodaj domenę sieciową do relay
7. Wybierz "AntiSpam" z lewego menu aby skonfigurować możliwości antyspamu
8. Wybierz "Antywirus" aby skonfigurować reakcje BitDefender Antywirus (co zrobić gdy zostanie znaleziony wirus, lokalizacja kwarantanny)
9. Dodatkowo, możesz skonfigurować "Mail notifications" (powiadomienia) i logowanie ("Logger")

11.4.3. BitDefender Linux Edition

Skaner antywirusowy zawarty w LinuxDefender jest zintegrowany bezpośrednio z pulpitem. Tą wersje cechuje interfejs graficzny GTK+.

Po prostu przeglądasz twardy dysk (albo dyski udostępnione), kliknij prawym przyciskiem na jakikolwiek plik albo folder i wybierz "Przeskanuj BitDefender". BitDefender Linux Edition będzie skanował wybrane pozycje i wyświetli raport. Dla dokładniejszego poznania opcji przeczytaj dokumentacje BitDefender Linux Edition (w folderze BitDefender Documentation) i program **/opt/BitDefender/lib/bdc**.

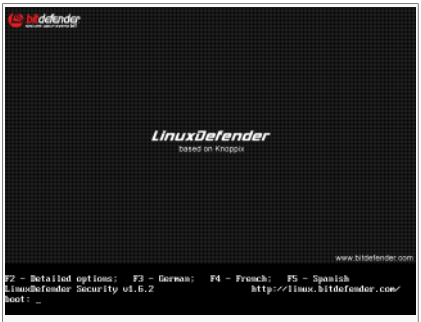
12. LinuxDefender - jak to zrobić?

12.1. Uruchom i Wyłącz

12.1.1. Uruchamianie LinuxDefender

Aby uruchomić CD ustaw w BIOSie twojego komputera bootowanie z CD, włóż CD do napędu i uruchom ponownie komputer. Upewnij się że twój komputer ma możliwość bootowania z CD.

Poczekaj aż na ekranie pojawią się instrukcje i postepuj według nich aby uruchomić LinuxDefender.



Ekran boot splash

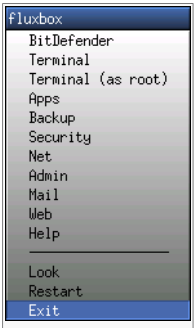
Naciśnij `F2` dla dalszych opcji. Naciśnij `F3` dla dalszych opcji w języku niemieckim. Naciśnij `F4` dla dalszych opcji w języku francuskim. Naciśnij `F5` dla dalszych opcji w języku hiszpańskim. Aby uruchomić z domyślnymi opcjami naciśnij `ENTER`.

Gdy zakończy się process bootowania zobaczysz pulpit. Możesz używać LinuxDefender.

Pulpit

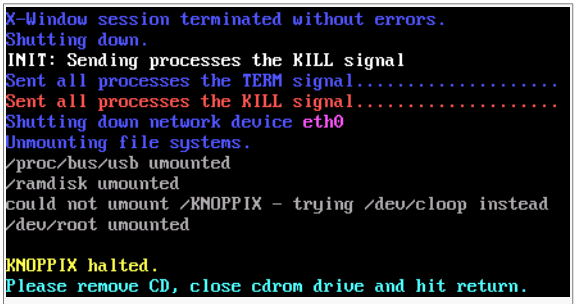
12.1.2. Wyłącz LinuxDefender

Aby poprawnie wyjśc z LinuxDefender zalecane jest odłączenie wszystkich podłączonych partycji używając komendy **odłącz** albo kliknięcie prawym przyciskiem na ikonie dysku i wybranie **Odłącz**. Wtedy możesz bezpiecznie wyłaczyć komputer wybierając **Wyjdź** z menu LinuxDefender (kliknięcie prawym przyciskiem aby otworzyć) albo wysyłając komendę **stop** w terminalu.



Wybierz "WYJDŹ"

Gdy LinuxDefender poprawnie zamknie wszystkie programy wyświetli na ekranie podobne komunikaty jak na poniższym rysunku. Możesz wyciągnąć CD aby bootować system z twardego dysku.



Poczekaj na ten komunikat gdy wyłączasz komputer

12.2. Konfigurowanie Połączenia Internetowego

Jeśli jesteś podłączony do sieci z serwerem DHCP i posiadasz ethernetową kartę sieciową to połączenie z Internetem powinno być automatycznie wykryte i skonfigurowane. Aby ręcznie skonfigurować sieć należy wykonać następujące kroki.

1. Otwórz menu LinuxDefender (kliknięcie prawym przyciskiem) i wybierz **Terminal** aby otworzyć konsole.
2. Wpisz **netcardconfig** w otwartym terminalu aby uruchomić narzędzie konfiguracji sieci.
3. Jeśli twoja sieć używa DHCP wybierz **tak** (jeśli nie jesteś pewien zapytaj administratora twojej sieci).
4. Połączenie sieciowe powinno być teraz automatycznie skonfigurowane. Możesz zobaczyć adres IP i ustawienia karty sieciowej za pomocą komendy **ifconfig**.
5. Jeśli masz statyczny adres IP (nie używasz DHCP), wybierz **Nie** przy pytaniu o DHCP.
6. Postępuj według instrukcji na ekranie. Jeśli nie jesteś pewien co wpisać skontaktuj się z administratorem sieci.

Jeśli wszystko pójdzie dobrze możesz przetestować twoje połączenie z Internetem za pomocą „pingowania” `bitdefender.com`.

```
$ ping -c 3 bitdefender.com
```

Jeśli używasz połączenia wdzwanianego wybierz **pppconfig** z menu LinuxDefender /Admin. Potem postępuj według instrukcji na ekranie aby ustawić połączenie PPP z Internetem.

12.3. Aktualizacja BitDefender

Pakiet BitDefender dla LinuxDefender używa ramdysku systemowego dla aktualizowanych plików. W ten sposób możesz zaktualizować wszystkie sygnatury wirusów, silniki programu oraz bazy danych antyspamu, nawet jeśli uruchamiasz system z nośnika tylko do odczytu, taki jakim jest LinuxDefender CD.

Upewnij się, że masz działające połaczenie z Internetem. Na początku otwórz BitDefender Remote Admin i wybierz **Live! Update** z lewego menu. Naciśnij **Aktualizuj Teraz** aby sprawdzić dostępność nowych aktualizacji.

Alternatywnie, możesz wprowadzić nową komendę w terminalu.

```
# /opt/BitDefender/bin/bd  update
```

Cały proces aktualizacji będzie zapisany domyślnie w raporcie BitDefender. Możesz obejrzeć go za pomocą następnej komendy.

```
# tail  -f /ramdisk/BitDefender/var/log/bd.log
```

Jeśli używasz proxy dla wychodzących połączeń skonfiguruj ustawienia Proxy w menu **Live! Update** w zakładce **Konfiguracja**.

12.4. Skanowanie Wirusowe

12.4.1. Jak mogę uzyskać dostęp do moich danych z Windows?

Obsługa zapisu NTFS

Obsługa zapisu NTFS jest dostępna za pomocą Captive NTFS write project. Potrzebne są dwa pliki sterowników z twojej instalacji Windows: `ntoskrnl.exe` i `ntfs.sys`. Aktualnie tylko sterowniki Windows XP są obsługiwane. Możesz ich użyć także do uzyskania dostępu do partycji Windows 2000/NT/2003.

Instalowanie dysków NTFS

Aby mieć dostęp do partycji NTFS Windows i móc zapisywać na nich dane, musisz najpierw zainstalować sterowniki NTFS. Jeśli nie używasz NTFS dla partycji Windows tylko FAT, albo wystarczy ci tylko dostęp do odczytu danych, możesz bezpośrednio

zamontować dyski i uzyskać dostęp do dysków Windows jak do każdego napędu w Linux.

Aby dodać obsługę partycji NTFS musisz najpierw zainstalować sterowniki NTFS z twojego dysku twardego, miejsc udostępnionych, dysków USB albo z Windows Update. Zalecamy korzystać z pewnych lokalizacji ponieważ dyski lokalne mogą być zawirusowane.

Dwa razy kliknij na ikonie **Instaluj sterowniki NTFS** aby uruchomić **Instalator BitDefender Captive NTFS**. Wybierz pierwszą opcje jeśli chcesz zainstalować sterowniki z lokalnego twardego dysku.

Jeśli dyski są w standardowej lokalizacji użyj **Szybkie Szukanie** aby znaleźć dyski.

Alternatywnie, możesz wskazać gdzie są dyski. Albo możesz pobrać sterowniki z Windows Update SP1.

Sterowniki nie są instalowane na twardym dysku, ale tymczasowo używane przez LinuxDefender aby uzyskać dostęp do partycji Windows NTFS. Jeśli program zainstalował sterowniki NTFS, możesz dwukrotnie kliknąć na pulpicie na ikonę partycji NTFS i przeglądać zawartość. Jeśli potrzebujesz wydajnego menadżera plików użyj Midnight Commander z menu LinuxDefender (albo wpisz **mc** w konsoli).

12.4.2. Jak przeprowadzić skanowanie antywirusowe?

Przeglądając folder możesz kliknąć prawym przyciskiem na plik lub katalog i wybrać **Wyślij do**. Następnie wybrać **Skaner BitDefender**.

Możesz także wydać komendę z terminala. **Skaner Antywirusowy BitDefender** przeskanuje wybrany plik albo folder.

```
# /opt/BitDefender/bin/bdgtk2 /path/to/scan/
```

Następnie kliknij **Rozpocznij Skanowanie**.

Jeśli chcesz skonfigurować opcje programu antywirusowego kliknij zakładkę **Konfiguruj Antywirus** z lewego panelu programu.

12.5. Utwórz Stały Filtr Poczty

Możesz użyć LinuxDefender do stworzenia rozwiązania filtrującego pocztę ad-hoc, bez instalacji jakiegokolwiek oprogramowania albo modyfikowania serwera poczty. Pomysł polega na wystawieniu systemu LinuxDefender przed twoim serwerem pocztowym, pozwalając BitDefender'owi skanować pod kątem spamu i wirusów cały ruch SMTP i przekazywać go do rzeczywistego serwera poczty.

12.5.1. Warunki wstępne

Potrzebujesz PC z procesorem kompatybilnym z Pentium 3 albo nowszym, conajmniej 256MB pamięci RAM i bootowalny napęd CD/DVD. System LinuxDefender będzie odbierał ruch SMTP zamiast rzeczywistego serwera poczty. Jest kilka sposobów na ustawienie tego.

1. Zmień IP twojego rzeczywistego serwera poczty i przypisz stary IP dla sytemu LinuxDefender
2. Zmień twój rekord DNS tak aby wpis MX dla twoich domen wskazywał na system LinuxDefender
3. Ustaw aby klienty email korzystały z nowego systemu LinuxDefender jako serwera SMTP
4. Zmień ustawienia firewalla aby przekazywać/przekierowywać wszystkie połączenia SMTP do systemu LinuxDefender zamiast rzeczywistego serwera poczty

"LinuxDefender jak to zrobić" nie wyjaśnia żadnych z powyższych sposobów. Dla dokładniejszych informacji możesz sprawdzić Linux Networking guides i dokumentacje Netfilter.

12.5.2. Ochrona email

Uruchom LinuxDefender CD i poczekaj aż system Windows zostanie wczytany.

Aby skonfigurować BitDefender SMTP Proxy, dwukronie kliknij ikonę **BitDefender Remote Admin**. Pojawi się następujące okno. Użyj nazwy użytkownika `bd` i hasła `bd` aby zalogować się do BitDefender Remote Admin.

Po poprawnym zalogowaniu się będziesz mógł skonfigurować BitDefender SMTP Proxy.

Wybierz **SMTP Proxy** aby skonfigurować rzeczywisty serwer poczty, który chcesz chronić przed spamem i wirusami.

Wybierz zakładkę **Domeny Email** aby wpisać wszystkie domeny email, dla których chesz akceptować pocztę.

Naciśnij **Dodoaj Domenę Email** albo **Dodaj Wiele Domen** i postępuj według instrukcji na ekranie aby ustawić domeny email.

Wybierz zakładkę **Domeny sieciowe** aby wprowadzić wszystkie sieci, z których chcesz otrzymywać pocztę.

Naciśnij **Dodaj Domenę Sieciową** albo **Dodaj Wiele Domen Sieciowych** i postępuj według instrukcji na ekranie aby ustawić zaufane domeny sieciowe.

Wejdź do **Antywirus** z lewego menu, aby wybrać co zrobić, gdy wirus zostanie znaleziony i skonfigurować inne opcje antywirusowe.

Teraz, cały ruch SMTP jest skanowany i filtrowany przez BitDefender. Domyślnie, wszystkie zawirusowane wiadomości są leczone albo usuwane i wszystkie wiadomości spam wykryte przez BitDefender są oznaczane w temacie słowem `[SPAM]`. Nagłówek email (`X-BitDefender-Spam: Yes/No`) jest dodawany do wszystkich emaili aby wyczyścić je filtrem po stronie klienta.

12.6. Przeprowadź Audyt Bezpieczeństwa Sieci

Poza swoim możliwościami antymalware'owymi, odzyskiwaniem danych i filtrowaniem poczty LinuxDefender jest dotsrczany z zestawem narzędzi, które pozwalają przeprowadzić audyty in-depth host i bezpieczeństwa sieci. Przeczytaj ten mały przewodnik aby dowiedzieć się jak możesz rozpocząć szybki audyt bezpieczeństwa twoich hostów albo sieci.

12.6.1. Poszukiwanie Rootkit'ów

Możesz przeprowadzić skanowanie antywirusowe zainstalowanych twardych dysków albo możesz przeskanować system w poszukiwaniu Unix rootkits.

Najpierw podłącz wszystkie partycje dysków twardych klikając dwa razy na ich ikony lub używając komendy **podłącz** z konsoli. Potem dwa razy kliknij ikonę **ChkRootKit** aby sprawdzić zawartość CD albo uruchom komende **chkrootkit** z konsoli, z użyciem parametru `-r NEWROOT` do wprowadzenia nowego katalogu hosta.

```
# chkrootkit -r /dev/hda3
```

Jeśli rootkit zostanie znaleziony to chkrootkit zaznaczy go **POGRUBIENIEM**, z użyciem dużych liter.

12.6.2. Nessus – Skaner Sieciowy

> Nessus jest najbardziej popularnym open-source'owym skanerem używanym przez ponad 75,000 organizacji na całym świecie. Wiele organizacji zaoszczędza wiele kosztów używając Nessus'a do audytowania firmowych urządzen i aplikacji.
>
> *—www.nessus.org*

Nessus może być użyty do zdalnego przeskanowania komputerów w sieci. Jest także zalecany w niektórych wypadkach do zminimalizowania niebezpieczeństwa.

Dwukrotnie kliknij ikonę na pulpicie **Nessus Security Scanner** albo uruchom **startnessus** z terminala. Poczekaj aż pojawi się okno. Zależnie od twoich zasobów sprzętowych może to zająć do 10 minut zanim Nessus zostanie załadowany, zawiera on ponad 5000 wtyczek z bazami danych słabych punktów. Użyj użytkownika `knoppix` i hasła `knoppix` do zalogowania.

Kliknij zakładkę **Wybór miejsca skanowania** i wpisz adres IP komputera albo nazwę hosta, który chcesz przeskanować. Upewnij się, że dostosowałeś wszystkie opcje do twojej sieci i konfiguracji systemu zanim uruchomisz skanowanie w celu zaoszczędzenia pasma i zasobów oraz uzyskania bardziej dokładnych rezultatów skanowania. Następnie kliknij **Rozpocznij skanowanie**.

Gdy proces skanowania się zakończy Nessus wyświetli wszystkie problemy, które znajdzie wraz z zaleceniami. Możesz zapisać raport w kilku formatach, między innymi w HTML z wykresami. Zapisany raport może być oglądany w ulubionej przeglądarce.

12.7. Sprawdź Pamięci RAM

Zazwyczaj gdy system zachowuje się nieprzewidywalnie (zwiesza się albo resetuje się od czasu do czasu), może to być problem z pamięcią. Możesz przetestować moduły pamięci RAM za pomocą programu **memtest** według opisu poniżej.

Uruchom komputer bootując z LinuxDefender CD. Wpisz **memtest** podczas bootowania i wciśnij Enter.

Program Memtest uruchomi się i wykona kilka testów aby sprawdzić staust pamięci RAM. Możesz skonfigurować jakie testy uruchomi i inne opcje Memtest wciskając klawisz `c`.

Pełny test Memtest po uruchomieniu może zająć nawet 8 godzin, zależnie od wielkości i szybkości pamięci RAM w twoim systemie. Zalecane jest pozwolić programowi Memtest wykonać wszystkie testy i dokładnie sprawdzić czy nie ma usterek pamięci RAM. Możesz przerwać w każdym momencie naciskając klawisz `ESC`.

Jeśli masz zamiar kupić nowy sprzęt (kompletny system albo tylko kilka komponentów) zalecane jest użycie LinuxDefender i memtest aby sprawdzić czy nie ma usterek pamięci.

Otrzymywanie pomocy

13. Wsparcie

13.1. Dział Wsparcia

Jako wartościowy dostawca, SOFTWIN robi wszystko co może, aby zapewnić swoim klientom szybką i skuteczną pomoc. Centra pomocy technicznej z poniższej listy są ciągle aktualizowane o nowe opisy wirusów i odpowiedzi na często zadawane pytania.

Z BitDefenderem, pomagamy klientom zaoszczędzić ich czas i pieniądze, dostarczając im najbardziej zaawansowane produkty. Ponadto wierzymy, że biznes opiera się na dobrej komunikacji i porozumieniu przy wsparciu klienta

Możecie kierować swoje prośby o pomoc na adres <support@bitdefender.com>, kiedy tylko zajdzie taka potrzeba. Aby uzyskać szybką odpowiedź, prosimy dołączyć adres e-mail jak również wszystkie możliwe szczegóły o twoim produkcie BitDefender. Spróbuj także opisać problem w sposób jasny i precyzyjny.

13.2. Pomoc on-line

13.2.1. Baza Wiedzy BitDefender

Baza wiedzy BitDefender jest informatyczną bazą on-line poświęconą oprogramowaniu BitDefender. Zawiera ona w łatwo dostępnym formacie raporty ze zdarzających się czasami problemów technicznych oraz ogólne artykuły o działaniu antywirusa, rozwiązaniach BitDefender, szczegółowych informacjach i wiele innych.

Baza wiedzy BitDefender dostępna dla wszystkich i korzystanie z niej jest bezpłatne. Wszystkie ważne zapytania o informacje albo raporty odnośnie błędów przychodzące od klientów BitDefender znajdują się w bazie danych BitDefender, dzięki temu klienci mogą znaleźć tam takie informacje jak raporty błędów, prace związane z programem, artykuły informacyjne czy też pliki pomocy dla produktów.

Baza wiedzy BitDefender jest dostępna cały czas na http://kb.bitdefender.com.

13.3. Informacje kontaktowe

Skuteczna komunikacja jest kluczem do udanej współpracy. Jeśli miałbyś jakiekolwiek problemy czy pytania, nie wahaj się skontaktować z nami.

13.3.1. Adresy internetowe

Dział sprzedaży: <sales@bitdefender.com>
Wsparcie Techniczne: <support@bitdefender.com>
Dokumentacja: <documentation@bitdefender.com>
Program Partnerski: <partners@bitdefender.com>
Marketing: <marketing@bitdefender.com>
Rzecznik prasowy: <pr@bitdefender.com>
Oferty pracy: <jobs@bitdefender.com>
Wysyłanie próbek wirusów: <virus_submission@bitdefender.com>
Wysyłanie próbek Spamu: <spam_submission@bitdefender.com>
Nadużycie Raportów: <abuse@bitdefender.com>
Strona internetowa produktu: http://www.bitdefender.com
Archiwa ftp produktu: ftp://ftp.bitdefender.com/pub
Lokalni dystrybutorzy: http://www.bitdefender.com/partner_list
Baza wiedzy BitDefender: http://kb.bitdefender.com

13.3.2. Biura

Listę adresów biur BitDefender'a znajdziecie Państwo poniżej.

Niemcy

Softwin GmbH
Siedziba w Europie Zachodniej
Karlsdorferstrasse 56
88069 Tettnang
Niemcy
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Wsparcie Techniczne: <support@bitdefender.com>

Anglia i Irlandia

One Victoria Square
Birmingham
B1 1BD
Phone: +34 932189615
Fax: +40 21 2330763

Email: <info@bitdefender.com>
Sales: <sales@bitdefender.com>
Web: http://www.bitdefender.com
Wsparcie Techniczne: <support@bitdefender.com>

Hiszpania

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Wsparcie Techniczne: <soporte@bitdefender-es.com>
<comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Strona produktu: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Wsparcie Techniczne: <support@bitdefender.com>
Obsługa Klienta: 954-776-6262
Web: http://www.bitdefender.com

Rumunia

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bukareszt
Wsparcie Techniczne: <suport@bitdefender.ro>
Sprzedaż: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Strona produktu: http://www.bitdefender.ro

Słownik

ActiveX

ActiveX jest modelem do pisania programów, używanym po to aby inne programy i systemy operacyjne mogły je używać. Technologia ActiveX jest wykorzystywana w Microsoft Internet Explorer, aby tworzyć interaktywne strony sieci, które raczej wyglądałyby i zachowywałyby się jak programy komputerowe, niż jak statyczne strony. Z ActiveX użytkownik może zadawać pytania lub na nie odpowiadać. Może także współpracować w inny sposób ze stronami sieci. Kontrole ActiveX są często pisane w Visual Basic.

Active X nie zapewnia kontroli bezpieczeństwa, a eksperci komputerowi do spraw bezpieczeństwa nie zalecają jego używania.

Adware

Adware jest często łączone z aplikacją, która jest dostarczana bez opłat tak długo jak użytkownik zgadza się na adware. Ponieważ aplikacje adware są zazwyczaj instalowane po zaakceptowaniu licencji która określa cele aplikacji, ochrona przed takim adwere nie jest wymagana.

Jednak reklamy pop-up mogą być kłopotliwe i w niektórych wypadkach obniżyć wydajność systemu. Ponadto informacje jakie te aplikacje kolekcjonują mogą naruszać prywatność w pełni nie powiadamiając użytkownika w umowie licencyjnej.

Archiwa

Dysk, taśma, lub katalog, który zawiera pliki.

Plik, który zawiera jeden lub więcej plików w skompresowanym formacie.

Backdoor

Dziura w systemie pozostawiona przez projektantów. Celem tych dziur nie zawsze jest atak, ponieważ niektóre systemy operacyjne wychodzą z kontami uprzywilejowanymi używanymi przez serwis techniczny.

Boot sektor

Sektor na początku każdego dysku, który identyfikuje budowę dysku (rozmiar sektora, rozmiar cluster itd.). Boot sektor zawiera również program ładujący system operacyjny.

Boot wirus

Wirus, który infekuje boot sektor lub stację dyskietek. Próba startowania z zainfekowanej dyskietki wirusem boot sektor spowoduje, że wirus stanie się aktywny w pamięci. Za każdym razem, kiedy postępujesz w ten sposób bootował komputer wirus będzie aktywny w pamięci.

Przeglądarka

Aplikacja używana do wyświetlania stron internetowych. Najpopularniejszymi przeglądarkami są: Netscape Navigator i Microsoft Internet Explorer. Obie są graficznymi przeglądarkami, co oznacza, że mogą pokazywać grafikę oraz tekst. W dodatku większość nowoczesnych przeglądarek może pokazywać informacje multimedialne wraz z dźwiękiem i wizją, chociaż wymagają one wtyczek dla niektórych formatów.

Linia poleceń

W linii poleceń użytkownik wpisuje polecenia w okno znajdujące się na ekranie, używając języka poleceń.

Cookie

W przemyśle internetowym cookie są określane jako małe pliki zawierające informacje o komputerach osobistych, które mogą być analizowane i używane przez reklamodawców, aby śledzić online twoje zainteresowania i gusty. Technologia cookie nadal się rozwija. Intencją cookie jest dostosowanie reklamam bezpośrednio do twoich zainteresowań. Cookie z jednej strony jest wydajne, ponieważ widzisz reklamę zgodną z twoimi zainteresowaniami, z drugiej strony śledzi i podążania za każdym twoim ruchem oraz kliknięciem.

Sterownik Dysku

Jest to urzadzenie, które czyta i zapisuje dane na dysku.

Sterownik dysku czyta i zapisuje dane na twardym dysku.

Sterownik dyskietek czyta i zapisuje dane na dyskietce.

Dyski mogą być zarówno wewnętrzne (wewnątrz komputera) jak i zewnętrzne (w oddzielnej obudowie na zewnątrz komputera).

Ściąganie

Aby kopiować dane (zwykle cały plik) z głównego źródła do peryferyjnego urządzenia. Termin ten jest często używany, aby opisać proces kopiowania pliku z usługi online na komputer. Ładowanie może także oznaczać kopiowanie pliku z serwera sieciowego na komputer.

E-mail

Poczta elektroniczna. Usługa, która przesyła wiadomości na komputery za pomocą sieci lokalnych lub globalnych.

Dziennik zdarzeń

Działanie lub wydarzenie wykryte przez program. Zdarzenia mogą być czynnościami użytkownika takimi jak: klikanie myszą, naciskanie klawisza lub systemem wydarzeń takim jak kończenie się pamięci.

Falszywie pozytywny

Pojawia się, kiedy skaner identyfikuje plik jako zainfekowany, gdy w rzeczywistości nie jest zainfekowany.

Rozszerzenie nazwy pliku

Część nazwy pliku, która wskazuje na rodzaj danych przechowywanych w pliku.

Wiele systemów operacyjnych używa rozszerzeń nazw pliku takich jak Unix, VMS, i MS-DOS. Zwykle posiadają od jednego do trzech znaków. Przykłady obejmują „c" jak kod źródłowy C, „ps" jak PostScript, "txt" jak text.

Heurystyczny

Metoda oparta na regule identyfikowania nowych wirusów. Ta metoda skanowania nie polega na wyszczególnieniu nowych sygnatur wirusów. Zaletą skanowania heurystycznego jest to, że nie jest podatna na zmylenie przez nowy wariant obecnych wirusów. Jednakże może czasami zapisać podejrzany kod w normalnych programach generując tzw. "fałszywie pozytywne".

IP

Protokół internetowy – protokół w stosie protokołów TCP/IP który jest odpowiedzialny za adresowanie IP, routing, fragmentację oraz defragmentację pakietów IP.

Java applet

Program Java, który jest zaprojektowany, aby uruchamiał wyłącznie strony sieci. Aby użyć applet na stronie sieci, powinieneś określić nazwę applet i rozmiar (długość i szerokość w pikselach), które applet może używać. Kiedy strona sieci jest dostępna przeglądarka załadowuje applet z serwera i uruchamia go na komputerze użytkownika (klienta). Applety różnią się od aplikacji tym, że są zarządzane zgodnie ze ściśle określonym protokołem bezpieczeństwa.

Na przykład, nawet jeśli aplety pracują u klienta, nie mogą czytać ani zapisywać danych na tej maszynie. Dodatkowo, aplety są później poddawane restrykcjom dzięki którym mogą one tylko czytać i zapisywać dane z tej samej domeny z jakiej pochodzą.

Makro wirus

Typ wirusa komputerowego, który jest zakodowany jako makro w danym dokumencie. Wiele aplikacji takich jak Microsoft Word i Excel, wspierają makro języki.

Wszystkie aplikacje pozwalają tobie umiejscowić makro w dokumencie i wykonywać je za każdym razem, kiedy dokument jest otwierany.

Klient poczty

Klient e-mail jest aplikacją, która umożliwia tobie wysyłanie i otrzymywanie email.

Pamięć

Wewnętrzny obszar przechowywania informacji w komputerze. Termin pamięć identyfikuje przechowywane dane. Każdy komputer posiada pewną ilość pamięci zwykle nazywanej pamięcią główną lub RAM.

Nie-heurystyczny

Ta metoda skanowania polega na określonych sygnaturach wirusów. Zaletą skanowania nie heurystycznego jest to, że nie jest on wprowadzony w błąd przez wirus metod nie generuje on fałszywych alarmów.

Spakowane programy

Plik w formacie skompresowanym. Wiele systemów operacyjnych i aplikacji zawiera polecenia, które umożliwiają tobie pakowanie pliku tak, aby zabierał on mniej pamięci. Np. masz plik tekstowy zawierający 10 kolejnych znaków. Normalnie wymagałoby to przechowania 10 bajtów.

Jednakże program pakujący pliki powoduje, że ilość miejsca zajmowanego po spakowaniu ulega redukcji. W tym przypadku plik po spakowaniu może zawierać 2 bity. To tylko jedna z wielu technik pakowania - jest ich wiele więcej.

Ścieżka

Dokładne umiejscowienie pliku na komputerze. Umiejscowienia są zwykle opisywane jako sposób hierarchicznego wypełniania systemu od góry w dół.

Droga pomiędzy pewnymi punktami, takimi jak kanały komunikacyjne pomiędzy dwoma komputerami.

Phishing

Proces wysyłania wiadomości pocztowych z nieprawdziwymi danymi, często danymi zafałszowanymi w ten sposób, aby użytkownik myślał, ze wiadomość pochodzi z prawidłowego źródła, przez co proceder taki służy oszustom do wyciągania poufnych danych od użytkownika. E-maile kierują użytkownika na stronę Internetową gdzie są proszeni o aktualizacje informacji osobistych, takich jak hasło, karta kredytowa, ubezpieczenie socjalne i nr konta bankowego. Strona Internetowa jest sfałszowana i istnieje tylko po to, aby wykraść informacje o użytkowniku.

Wirus Polimorficzny

Wirus, który zmienia swoją formę w każdym zainfekowanym pliku. Ponieważ wirusy nie mają stałego wzoru binarnego, są one trudne do identyfikacji.

Port

Interface na komputerze, do którego podłączasz urządzenie. Komputery osobiste mają różne typy portów. Wewnętrznie, znajduje się kilka portów dla połączeń dyskowych, monitorów i klawiatur. Zewnętrznie, komputery osobiste mają port dla połączeń modemowych, drukarek, myszy i innych urządzeń peryferyjnych.

W sieciach TCP/IP i UDP zakończenie logicznego połączenia. Numer portu identyfikuje typ portu. Np. port 80 jest używany dla ruchu HTTP.

Plik raportu

Plik, który zapisuje akcje, które się zdarzyły. BitDefender utrzymuje plik raportu zapisując skanowaną ścieżkę, foldery, ilość archiwów i skanowanych plików, ile zainfekowanych i podejrzanych plików zostało znalezione.

Rootkit

Rootkit jest zestawem narzędzi programowych, który oferuje dostęp do komputera na poziomie administratora. Termin ten był początkowo używany dla systemów UNIX.

Głównym zadaniem rootkit'ów jest ukrywanie procesów, plików, loginów i logów.

Rootkity z natury nie są zagrożeniem. Na przykład systemy i nawet niektóre aplikacje ukrywają krytyczne pliki używając rootkit'ów. Jednak często są one używane do ukrywania oprogramowania złośliwego. Mogą monitorować ruch, tworzyć backdoor do systemu, zmieniać pliki i logi.

Skrypt

Inna nazwa dla makr; skrypt jest listą komend, które mogą być wykonywane bez udziału użytkownika.

Spam

Śmieci elektronicznej poczty. Ogólnie znane jako niechciane wiadomości e-mail.

Spyware

Każde oprogramowanie, które zbiera dane o użytkowniku podczas połączenia z Internetem bez jego wiedzy, zazwyczaj w celach reklamowych. Aplikacje spyware występują zazwyczaj jako ukryte komponenty programów freeware albo shareware, które mogą być pobrane z Internetu. Raz zainstalowane spyware nasłuchuje poruszanie się użytkownika po Internecie i przesyła te informacje w tle do kogoś innego. Spyware mogą także wykradać informacje o adresach e-mail, a nawet o hasłach i numerach kart kredytowych.

Spyware jest prostym programem podobnym do konia trojańskiego, którego użytkownicy instalują nieświadomie podczas instalacji czegoś innego. Pospolitym sposobem by zostać ofiarą spyware jest pobranie niektórych programów peer-to-peer.

Poza kwestiami etyki i prywatności, spyware okrada użytkownika używając pamięci komputera i także zmniejszając przepustowość połączenia Internetowego podczas wysyłania informacjji do bazy spyware. Ponieważ spyware zużywa pamięć i zasoby systemowe aplikacje pracujące w tle mogą zawieszać i powodować niestabilność systemu.

Elementy startowe

Wszystkie umiejscowione pliki w tym folderze będą uruchomione podczas statru systemu. Np. ekran startowy, plik dźwiękowy odtwarzany podczas pierwszego startu komputera, przypominacz lub aplikacje programowe, które uruchamiają jakieś elementy.

Pasek systemowy

Wprowadzony przez Windows 95 pasek systemowy jest zlokalizowany w pasku zadań Windows (zwykle na dole, obok zegara) i zawiera miniaturowe ikony, służące łatwemu dostępowi do funkcji systemowych tj. fax, drukarki, modemu, itd. Podwójne kliknięcie lub kliknięcie prawym klawiszem myszy na ikonę spowoduje dostęp do danego elementu.

TCP/IP

Transmission Control Protocol/Internet Protocol – zespół protokołów sieciowych szeroko używanych w internecine, który zapewnia komunikację przez połączenia sieciowego komputerów z różną architekturą sprzętową i różnymi systemami operacyjnymi. TCP/IP zawierają standardy dotyczące komunikacji komputerów oraz połączeń sieciowych i ruchu.

Trojan

Niszczycielski program, który ukrywa się jako aplikacja. W przeciwieństwie do wirusów, konie trojańskie nie powielają się. Jednym z najniebezpieczniejszych typów koni trojańskich jest program zapewniający, że pozbył się wirusów z twojego komputera a w rzeczywistości wprowadza wirusy do komputera.

Nazwa pochodzi z powieści Homera “Iliada”, w której Grecy podarowali olbrzymiego konia wrogom jako znak pokoju. Ale gdy trojanie wprowadzili konia do miasta, żołnierze greccy wyszli z konia i otworzyli bramy miasta pozwalając pozostałym na wejście i podbicie Troi.

Aktualizacja

Element oprogramowania zaprojektowany po to, aby zamienić starszą wersję na nowszą. Proces instalacji, w celu uaktualnień, często przyczynia się do tego, że starsza wersja jest już zainstalowana na twoim komputerze. Gdyby nie była zainstalowana, nie mógłbyś dokonać uaktualnień.

BitDefender posiada wlasny moduł uaktualnienia, który pozwala tobie manualnie wprowadzać uaktualnienia lub przeprowadzać je automatycznie.

Wirus

Program lub część kodu, która jest załadowana do twojego komputera bez twojej wiedzy i uruchamia się wbrew twojej woli. Większość wirusów może się powielać. Wszystkie wirusy komputerowe są tworzone przez człowieka. Prosty wirus, który umie się kopiować kilka razy jest stosunkowo łatwy do utworzenia. Nawet tak prosty wirus jest niebezpieczny, ponieważ szybko wykorzysta całą dostępną

pamięć i przyczyni się zatrzymania pracy systemu. Bardziej niebezpiecznym typem wirusa jest ten, który jest zdolny przenosić się prze sieci i łamać systemy bezpieczeństwa.

Definicja wirusa

Wzór binarny wirusa używany przez program antywirusowy, aby wykryć i wyeliminować wirusa.

Robak

Program, który propaguje się przez sieć mnożąc, się w czasie poruszania. Robak nie może się przyłączać do innych programów.