

G Data MailSecurity

Podręcznik użytkownika

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

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

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

ISBN 978-83-61624-10-3

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

G Data Software Sp. z o.o.

Spis treści

I Wstęp	1
1 Pomoc techniczna	1
2 Kontynuacja licencji	2
3 Warunki licencji	2
II Przed instalacją	5
1 Instalacja programu na serwerze poczty (SMTP)	6
2 Instalacja programu na osobnym komputerze (SMTP)	7
3 Wymagania programu	9
III Instalacja	9
IV Składnik G Data MailSecurity	10
V Składnik G Data MailSecurity Administrator	11
VI Uruchamianie programu (logowanie)	12
VII Widoki składnika Administrator	13
1 Widok Status	14
2 Widok Filtr	17
3 Widok Kolejki	23
4 Widok Działanie	24
5 Widok Wykryte wirusy	25
VIII Pasek narzędzi	25
1 Opcje	26
2 Aktualizacja	38

II Podręcznik G Data MailSecurity

3 Filtr spamu 40

1 Wstęp

Program G Data MailSecurity współpracuje z każdym serwerem poczty elektronicznej działającym w dowolnym systemie operacyjnym. Oprogramowanie funkcjonuje jako brama pocztowa SMTP i POP3, skutecznie blokująca niechciane wiadomości. Zintegrowany filtr zawartości jest w stanie wyeliminować także nieznanne dotychczas wirusy.

Życzymy przyjemnej i bezpiecznej pracy z programem G Data MailSecurity.

G Data Software

1.1 Pomoc techniczna

Pomoc techniczna przysługuje wszystkim zarejestrowanym użytkownikom przez rok czasu od rejestracji programu lub wykupienia abonamentu. Zgłoszenia problemów z programem przyjmujemy telefonicznie, pocztą elektroniczną i faksem.

telefon: 094 3729 650

e-mail: helpdesk@gdata.pl

W rozwiązaniu wielu problemów pomoże konfrontacja z tekstami pomocy lub podręcznikiem, prosimy więc najpierw tam poszukać odpowiedzi na pytania. Wiele odpowiedzi można znaleźć na stronie pomocy technicznej: <http://www.gdata.pl>.

Przed rozmową prosimy o przygotowanie danych na temat sieci i komputerów ze zwróceniem szczególnej uwagi na:

- numer wersji programu G Data MailSecurity,
- Numer Klienta otrzymany w potwierdzeniu rejestracji,
- rodzaj i wersję stosowanego serwera poczty,
- adresację IP i topologię sieci komputerowej,

- wersje klienckich systemów operacyjnych,
- dodatkowo zainstalowane oprogramowanie i sprzęt.

Przygotowanie powyższych informacji ułatwi i przyspieszy korespondencję lub rozmowę z serwisantem.

1.2 Kontynuacja licencji

W momencie zarejestrowania zakupionej licencji otrzymujesz prawo do korzystania z aktualizacji sygnatur wirusów i plików produktu, jak i z usługi pomocy technicznej w odniesieniu do używanego oprogramowania przez okres jednego roku, lub dłuższy, w zależności od wniesionej opłaty licencyjnej. W każdej chwili możesz dokonać przedłużenia wykupionej licencji kontaktując się z nami:

telefon:	094 3729 650
----------	--------------

W sprawach problemów technicznych zapraszamy do kontaktu z działem pomocy technicznej. Patrz rozdział [Pomoc techniczna](#).

1.3 Warunki licencji

G Data Software Sp. z o.o.

Ogólne warunki użytkowania programu G Data MailSecurity.

1. Przedmiot umowy

Przedmiotem umowy zawartej między firmą G Data Software Sp. z o.o., zwaną dalej Producentem, a Użytkownikiem jest program G Data MailSecurity zwany dalej Oprogramowaniem. Producent dostarcza Użytkownikowi Oprogramowanie na nośniku danych lub w postaci pliku pobranego ze strony internetowej Producenta. Producent zwraca uwagę na fakt, że technicznie nie jest możliwe wyprodukowanie Oprogramowania współpracującego bezbłędnie z wszystkimi aplikacjami i z każdą kombinacją sprzętowo-programową.

2. Zakres stosowania

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

3. Szczególne ograniczenia

Użytkownik nie może modyfikować Oprogramowania bez pisemnej zgody Producenta.

4. Prawo własności

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

5. Powielanie

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

6. Czas trwania umowy

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

7. Złamanie warunków umowy

Użytkownik ponosi odpowiedzialność za wszystkie szkody poniesione przez

Producenta w związku z naruszeniem praw autorskich, wynikłe ze złamania warunków tej umowy.

8. Zmiany i aktualizacje

Obie strony obowiązują najnowszą wersją tej umowy. Warunki umowy mogą ulec zmianie w każdej chwili, bez powiadamiania Użytkownika i podawania przyczyn.

9. Gwarancja i odpowiedzialność Producenta:

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

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

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

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

10. Właściwość sądu

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

11. Postanowienia końcowe

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

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

Copyright © 2009 G Data Software AG

Skaner A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2009 BitDefender SRL.

Skaner B: © 2009 Alwil Software

OutbreakShield: © 2009 Commtouch Software Ltd.

2 Przed instalacją

G Data MailSecurity jest bramą pocztową dla protokołów SMTP i POP3 zintegrowaną filtrem antyspamowym i ochroną antywirusową.

- SMTP: Poczta przychodząca będzie odbierana najpierw przez G Data MailSecurity. Program przepuści wiadomość do serwera pocztowego dopiero po odfiltrowaniu spamu i przeprowadzeniu kontroli antywirusowej.
- POP3: G Data MailSecurity kontroluje także maile odbierane przez protokół POP3. Brama odbiera wiadomości skanuje na obecność spamu i wirusów, a następnie przekazuje do programu pocztowego.

Przed instalacją programu G Data MailSecurity należy zastanowić się gdzie go umiejscowić w sieci. Moduł sterujący programem - Administrator można zainstalować na dowolnym komputerze podłączonym do sieci. Sam program wymaga zainstalowania w odpowiednim miejscu topologii sieci.

Generalnie zaleca się instalację programu bezpośrednio za zaporą

sprzętową (o ile jest stosowana), lub na komputerze funkcjonującym jako brama pocztowa w przedsiębiorstwie. W przypadku stosowania Windowsowego serwera poczty Exchange, aplikację można zainstalować bezpośrednio na komputerze z serwerem poczty. W przypadku serwera działającego w innym systemie operacyjnym, potrzebna będzie dodatkowa maszyna z systemem Windows.

Pamiętaj o dostosowaniu konfiguracji Firewalla (adres IP i/lub port) tak, aby umożliwić kontrolę przepływu strumienia danych przez program.

2.1 Instalacja programu na serwerze poczty (SMTP)

Jeśli Twój serwer SMTP zezwala na zmianę numerów portów, możesz zainstalować G Data MailSecurity na tym samym komputerze co serwer SMTP. W takim przypadku nadaj nowy numer portu dla serwera pocztowego (np. 7100 lub wyższy). MailSecurity stosuje do edycji poczty przychodzącej port o numerze 25.

Jeśli zainstalujesz MailSecurity na komputerze z programem Microsoft Exchange, program przestawi port wiadomości wychodzących.

W tym celu należy zmodyfikować wpis SMTP w pliku `\winnt\system32\drivers\etc\services`, i ponownie uruchomić usługę Internet Mail Service programu Microsoft Exchange.

Przykład:

1. Konfiguracja serwera poczty

- Port poczty przychodzącej: 7100 (przykładowo)
- Przesyłanie wiadomości: Wszystkie wiadomości przesyłaj do hosta 127.0.0.1

2. Konfiguracja G Data MailSecurity - Przychodzące (SMTP)

- Port poczty przychodzącej: 25
- Użyj serwera DNS do przesyłania wiadomości: Wyłączone
- Przekazuj wiadomości na ten serwer SMTP: 127.0.0.1
- Port: 7100 (przykład)

3 Konfiguracja G Data MailSecurity - Wychodzące (SMTP)

- Edycja poczty wychodzącej: Włączona
- Adresy IP lub podsieci komputerów wysyłających wiadomości: 127.0.0.1;<IP serwera poczty>
- Użyj serwera DNS do przesyłania wiadomości: Włączone

Oznaczenia

- <IP serwera poczty> = Adres IP komputera z zainstalowanym serwerem poczty.

2.2 Instalacja programu na osobnym komputerze (SMTP)

W tym przypadku poczta przychodząca muszą być odbierane najpierw przez G Data MailSecurity, a nie bezpośrednio przez serwer poczty.

Można to zrobić na kilka różnych sposobów:

- a) dopasować rekord MX w DNS danej domeny
- b) zdefiniować obejście w Firewallu (jeśli jest stosowany)
- c) zmienić adres IP serwera poczty, a oryginalny adres serwera poczty przyporządkować komputerowi z programem MailSecurity

Przykład

1. Konfiguracja serwera poczty

- Port poczty przychodzącej: 25
- Przesyłanie wiadomości: Wszystkie wiadomości przesyłaj do hosta <IP G Data MailSecurity>

2. Konfiguracja G Data MailSecurity - Przychodzące (SMTP)

- Port poczty przychodzącej: 25
- Użyj serwera DNS do przesyłania wiadomości: Wyłączone
- Przekazuj wiadomości na ten serwer SMTP: <IP serwer poczty>
- Port: 25

3. Konfiguracja G Data MailSecurity wychodzące (SMTP)

- Edycja wiadomości wychodzących: Włączona
- Adresy IP lub podsieci komputerów wysyłających wiadomości: <IP serwera poczty>
- Użyj serwera DNS do przesyłania wiadomości: Włączone

Oznaczenia

- <IP serwera poczty> = Adres IP komputera z zainstalowanym serwerem poczty.
 - <IP G Data MailSecurity> = Adres IP komputera z zainstalowanym programem G Data MailSecurity.
-

2.3 Wymagania programu

Wymagania sprzętowe i programowe składnika G Data MailSecurity:

- Windows XP SP2, Windows Vista, Windows 2003 Server lub Windows Server 2008
- 256 MB RAM
- 50 MB wolnego miejsca na dysku twardym

Wymagania sprzętowe i programowe składnika G Data MailSecurity Administrator:

- Windows XP SP2, Windows Vista, Windows 2003 Server lub Windows Server 2008
- 32 MB RAM
- 50 MB wolnego miejsca na dysku twardym

Aplikacja G Data MailSecurity działa także w 64-bitowych systemach Windows.

3 Instalacja

Przed zainstalowaniem programu zamknij wszystkie aplikacje Windows. Instalacja programu podczas pracy innych aplikacji może powodować problemy. Upewnij się także czy dysponujesz odpowiednią ilością wolnego miejsca na dysku twardym. Jeśli zabraknie miejsca program wyświetli podczas instalacji stosowny komunikat.

Instalacja programu jest zupełnie prosta. Po uruchomieniu Windows włóż płytę z programem do napędu. Instalator uruchomi się automatycznie i zaoferuje następujące opcje:

- Instaluj: Rozpoczęcie instalacji programu na komputerze.
- Przeglądaj: Uruchomienie Eksploratora Windows co umożliwi przeglądanie zawartości płyty CD-ROM z programem.

- Anuluj: Zamknięcie okna autostartu.

Instaluj program zgodnie ze wskazówkami kreatora instalacji. W oknie wyboru modułu wybierz program G Data MailSecurity i rozpocznij instalację na wybranym komputerze. Najlepiej, jeśli jest to brama będąca przed serwerem pocztowym, ale możliwa jest także instalacja programu na tym samym komputerze co serwer pocztowy. Komputer ten musi oczywiście spełniać minimalne wymagania systemowe oprogramowania G Data MailSecurity.

Program jest teraz gotowy do konfiguracji. Oprócz programu G Data MailSecurity, automatycznie został zainstalowany jego interfejs graficzny - moduł Administrator, umożliwiający obsługę właściwego programu. Program administrujący uruchamia się poleceniem G Data MailSecurity z menu Start > Wszystkie programy > G Data MailSecurity. W kolejnych rozdziałach opisane są wszystkie opcje dostępne w programie.

Podczas instalacji programu, możesz zdecydować, czy chcesz zainstalować składnik prowadzący szczegółowe statystyki strumienia poczty. Statystyki poczty dostępne są do wglądu po kliknięciu przycisku Statystyki w widoku Statusu. Opcje statystyk można modyfikować w zakładce Opcji o nazwie Baza danych.

4 Składnik G Data MailSecurity

Program jest teraz zainstalowany i gotowy do konfiguracji. Program kontroluje przychodzące i wychodzące wiadomości SMTP i POP3 na obecność spamu, wirusów, złośliwych programów oraz niechcianych treści. Poza tym program pobiera automatycznie najnowsze sygnatury wirusów i aktualizacje programu przez Internet. Wraz z pośrednikiem poczty w systemie instalowany jest automatycznie składnik G Data MailSecurity Administrator, czyli jego graficzny interfejs. Administrator umożliwia modyfikowanie ustawień programu i podgląd statystyk.

Możesz dodatkowo zainstalować składnik G Data MailSecurity Administrator na dowolnym komputerze w sieci spełniającym wymagania programu. Umożliwi to zarządzanie ochroną bezpośrednio z tego komputera.

Zamknięcie modułu Administrator nie oznacza wyłączenia programu G Data MailSecurity. Program pozostaje aktywny w tle i steruje procesami przepływu poczty elektronicznej zgodnie z dokonanymi ustawieniami.

Odbiór i wysyłka wiadomości elektronicznych zachodzi z reguły przy użyciu protokołów SMTP i POP3. SMTP (Simple Mail Transfer Protocol) służy do wysyłania wiadomości, podczas gdy POP3 (Post Office Protocol 3) odbiera i przechowuje wiadomości w specjalnej skrzynce pocztowej zabezpieczonej hasłem przez użytkownika.

W zależności od budowy Twojej sieci, MailSecurity chroni strumień wiadomości w różnych jej miejscach:

- Jeśli korzystasz z serwera SMTP, MailSecurity ma możliwość kontroli wiadomości jeszcze zanim wpłyną do serwera pocztowego. Konfiguracja tej opcji dostępna jest w zakładce Przychodzące (SMTP).
- Jeżeli odbierasz pocztę elektroniczną bezpośrednio przez protokół POP3 (np. poprzez zbiorcze konto POP3), MailSecurity może skanować maile zanim zostaną otwarte przez użytkownika. Konfiguracja tej opcji dostępna jest w zakładce Przychodzące (POP3).

Program może także dokonywać kontroli wychodzących wiadomości przed wysłaniem do adresata. Konfiguracja tej opcji dostępna jest w zakładce Wychodzące (SMTP).

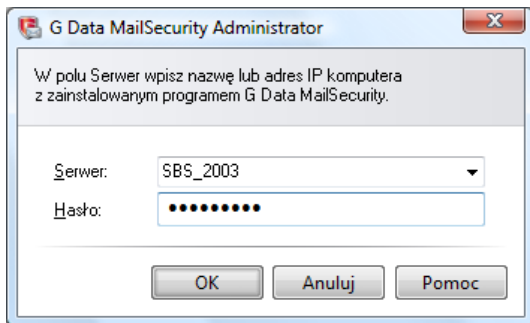
5 Składnik G Data MailSecurity Administrator

Składnik G Data MailSecurity Administrator jest graficznym interfejsem programu G Data MailSecurity, umożliwiającym zarządzanie kompleksową ochroną protokołów SMTP i POP3. Jeżeli składnik Administrator zainstalowany jest na innym komputerze niż główny składnik G Data MailSecurity, w oknie logowania należy wpisać nazwę komputera z zainstalowaną bramą poczty. Dostęp do G Data MailSecurity można zabezpieczyć hasłem.

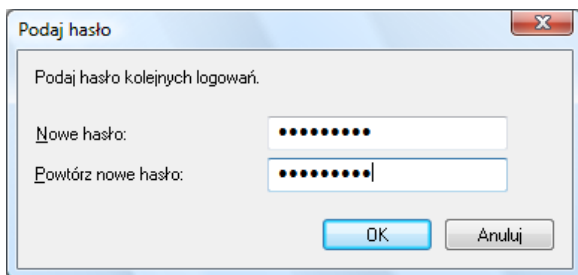
6 Uruchamianie programu (logowanie)



Aby uruchomić moduł sterujący programem G Data MailSecurity Administrator, kliknij skrót na pulpicie lub uruchom polecenie G Data MailSecurity w grupie programowej menu Start > Wszystkie programy > G Data MailSecurity. Przy pierwszym uruchomieniu program zapyta o nazwę serwera oraz hasło.



W polu Serwer wpisz nazwę lub adres IP komputera, na którym zainstalowany jest program G Data MailSecurity. Jeżeli nie chcesz ustawiać hasła dostępu do programu, po prostu kliknij przycisk OK bez wpisywania hasła, a następnie kliknij klawisz Anuluj.



Hasło można ustawić lub zmodyfikować w oknie Opcje > [Inne](#) klikając przycisk Zmień hasło.

7 Widoki składnika Administrator

Interfejs programu jest skonstruowany przejrzysto i intuicyjnie. Całość podzielona jest na tematyczne okna widoków, przełączane w panelu po lewej stronie:



[Status](#)



[Filtr](#)



[Kolejki](#)



[Działanie](#)



[Wykryte wirusy](#)

Przyciski paska zadań:



[Opcje](#): Możliwość dostosowania podstawowych ustawień sterowania programem oraz dopasowania ich do własnych potrzeb.



[Filtr spamu](#): Filtr spamu umożliwia skuteczne blokowanie wiadomości o określonych treściach lub pochodzące od niepożądanych nadawców.



[Aktualizacja](#): Opcje i ustawienia związane z pobieraniem aktualizacji baz wirusów oraz plików programowych przez Internet. Istnieje możliwość zaplanowania automatycznych aktualizacji programu MailSecurity.



Leksykon: Link do internetowego leksykonu wirusów. Baza danych zawiera informacje o aktualnie rozprzestrzeniających się wirusach oraz archiwum wszystkich wirusów wykrywanych przez program.



Pomoc: Wywołanie pliku pomocy.



Informacje: Informacje o wersji programu.

7.1 Widok Status

W oknie statusu znajduje się spis podstawowych informacji o stanie systemu komputera oraz MailSecurity.



Taki symbol widnieje z lewej strony pozycji listy spełniającej optimum wymogów bezpieczeństwa komputera.



Jeśli któryś ze składników nie jest zoptymalizowany (np. nieaktualne sygnatury wirusów), obok jego opisu pojawia się symbol ostrzeżenia.

Aby dokonać zmian w ustawieniach, kliknij dwukrotnie opis pożądanego składnika lub przejdź do odpowiedniego okna programu (ewentualnie wybierz składnik i kliknij przycisk Edycja).



Lista okna statusu obejmuje pozycje:

- Edycja poczty przychodzącej: Jeśli opcja jest aktywna, program ma dostęp do poczty przychodzącej zanim zostanie ona dostarczona do użytkownika. Klikając dwukrotnie opis utworzysz okno ustawień. Patrz też rozdział [Opcje > Przychodzące \(SMTP\)](#).
- Kontrola poczty przychodzącej: Skanowanie przychodzących wiadomości zapobiega przedostaniu się zawartych w nich wirusów do Twojej sieci. Klikając dwukrotnie opis utworzysz okno ustawień.
- Edycja poczty wychodzącej: Jeśli opcja jest aktywna, program ma dostęp do poczty wychodzącej zanim zostanie ona wysłana do odbiorcy. Klikając dwukrotnie opis utworzysz okno ustawień. Patrz też rozdział [Opcje > Wychodzące \(SMTP\)](#).

- Kontrola poczty wychodzącej: Skanowanie przychodzących wiadomości zapobiega wysyłaniu wirusów. Klikając dwukrotnie opis otworzysz okno ustawień.
- OutbreakShield umożliwia rozpoznanie i zwalczanie wirusów jeszcze przed opracowaniem odpowiednich sygnatur wirusów. Moduł OutbreakShield łącząc się z odpowiednim serwerem ustala czy wiadomość stanowi zagrożenie na podstawie jej cech charakterystycznych. Dzięki temu jest w stanie zareagować na zagrożenie dużo wcześniej przed stworzeniem i dostarczeniem odpowiednich sygnatur wirusów. Moduł jest zintegrowany z ochroną poczty elektronicznej.
- Automatyczna aktualizacja: Generalnie zaleca się włączenie opcji automatycznej aktualizacji. Klikając dwukrotnie opis otworzysz okno ustawień. Patrz też rozdział [Aktualizacja](#).
- Data ostatniej aktualizacji: Im nowsze bazy wirusów, tym skuteczniejsza ochrona przed wirusami. Należy przeprowadzać aktualizacje tak często jak się da. Klikając dwukrotnie opis otworzysz okno ustawień. Patrz też rozdział [Aktualizacja](#).
- Filtr spamu umożliwia skuteczne wykrywanie i blokowanie wiadomości zawierających niepożądane treści lub pochodzące od niechcianych nadawców.
- Spam-OutbreakShield: Jest to moduł, który skutecznie wykrywa i blokuje wiadomości masowe. Łącząc się z odpowiednim serwerem ustala czy wiadomość jest powiązana z wysyłką masową.

Podczas instalacji programu, możesz zdecydować, czy chcesz zainstalować składnik prowadzący szczegółowe statystyki strumienia poczty. Statystyki poczty dostępne są do wglądu po kliknięciu przycisku Statystyki w widoku Statusu. Opcje statystyk można modyfikować w zakładce Opcji o nazwie Baza danych.

7.2 Widok Filtr

Widok Filtr umożliwia definiowanie kryteriów filtrowania, zatrzymywania i usuwania wiadomości przychodzących i wychodzących. Kliknij przycisk Nowy... aby utworzyć nowy filtr lub Edycja aby zmodyfikować zapisane ustawienia.



Lista zdefiniowanych filtrów znajduje się w środkowej części okna. Aktywne filtry oznaczone są haczykami w polach przed ich nazwami. Klikając pole przed nazwą filtra możesz go włączyć lub wyłączyć.

W dolnej części okna znajduje się szereg przycisków ułatwiających zarządzanie filtrami.

- Import: Przycisk umożliwia wczytanie zapisanego wcześniej zestawu filtrów z pliku XML.
- Eksport: Przycisk służy do eksportowania zdefiniowanych filtrów do pliku w formacie XML. Zaznacz filtry, które chcesz wyeksportować i kliknij

przycisk Eksport. Aby zaznaczyć więcej niż jeden filtr, przytrzymaj klawisz Ctrl lub Shift.

- **Nowy:** Kliknij ten przycisk aby utworzyć nowy filtr. W oknie wyboru zaznacz pożądaną szablon, na podstawie którego chcesz utworzyć nowy filtr. Informacje o poszczególnych szablonach i objaśnienia ustawień znajdziesz kolejnych rozdziałach.
- **Edycja:** Zaznacz filtr, który chcesz zmodyfikować i kliknij przycisk Edycja, aby zmienić ustawienia filtra.
- **Usuń:** Ten przycisk umożliwia usunięcie zaznaczonego filtra.
- **Statystyki:** Zaznacz jeden filtr i kliknij ten przycisk, aby wyświetlić okno statystyk dotyczących stosowania filtra.
- **Protokół:** Wbudowany filtr (Filtr spamu) wyposażony jest w narzędzie raportujące wydarzenia związane z filtrowaniem wiadomości. Protokołowane są wiadomości zaindeksowane przez program jako niechciane. Z okna protokołu można dowiedzieć się, jakie kryteria wykrywania spamu zadecydowały o detekcji (wartości indeksów spamu). To okno umożliwia zgłoszenie fałszywego wykrycia wysyłki masowej do serwera OutbreakShield. Wiadomość zostanie w takim przypadku powtórnie przeskanowana. W przypadku potwierdzenia błędu, program zakwalifikuje wiadomość jako niegroźną. Uwaga: Do serwera przysyłana jest tylko suma kontrolna wiadomości, nie zaś jej treść.

Niezależnie od stosowanych filtrów program G Data MailSecurity skanuje pocztę elektroniczną na obecność złośliwego oprogramowania. Filtry dodatkowo minimalizują prawdopodobieństwo przedostania się do skrzynek pocztowych spamu, podejrzanych skryptów i reklam.

Nazwa i komentarz

Zalecamy stosowanie wymownych i jednoznacznych nazw podczas tworzenia filtrów. Można również skorzystać z opcji dodania komentarza, co pozwoli na łatwiejszą identyfikację filtrów w przyszłości.

Reakcja

W sekcji Reakcja można ustalić, co program ma zrobić w momencie nadejścia wiadomości spełniającej regułę filtra.

Istnieje możliwość powiadomienia nadawcy wiadomości lub dowolnego użytkownika poczty o wykryciu anomalii w mailu.

Wiadomość z powiadomieniem można dowolnie skonstruować korzystając z oferowanych przez program zmiennych:

- %s Nadawca
- %r Odbiorca
- %c DW
- %d Data
- %u Temat
- %h Nagłówek
- %i IP nadawcy

7.2.1 Filtr potwierżeń odbioru

Ten filtr automatycznie usuwa uciążliwe żądania potwierzenia odczytu wiadomości. Żądanie potwierzenia odczytu wiadomości można wymusić za pomocą większości stosowanych programów do odbioru poczty.

7.2.2 Filtr skryptów HTML

Filtr wykrywa w wiadomościach HTML aktywne skrypty, które mogą pobierać i uruchamiać złośliwe programy.

7.2.3 Filtr zewnętrznych referencji

Bardzo często wiadomości w formacie HTML zawierają linki do danych, które uruchamiają się lub ukazują dopiero po otwarciu wiadomości. Mogą to być np. zdjęcia, nie wysyłane bezpośrednio w wiadomości, a pobierane w momencie jej otwarcia. Zdarza się też, że wiadomość zawiera link do złośliwego programu, strony lub nawet wirusa. Właśnie z tego względu zaleca się wyłączenie zewnętrznych referencji. Tekst wiadomości pozostaje bez zmian.

7.2.4 Filtr załączników

Opcja filtrowania załączników wiadomości oferuje wachlarz możliwości filtrowania załączników poczty oraz dokumentów. Większość wirusów rozprzestrzenia się właśnie przez pliki załącznika, zawierające ukryte pliki wykonywalne. Może to być zwykły plik EXE, lub też skrypt VBS ukryty w grafice, filmie lub pliku muzycznym. Podczas otwierania załączników należy zachować szczególną ostrożność. W wątpliwych przypadkach lepiej zwrócić się przed otwarciem pliku do nadawcy z pytaniem, czy naprawdę go wysyłał.

W polu Rozszerzenia plików można zdefiniować filtrowane typy plików. Najbardziej niebezpieczne są pliki wykonywalne (EXE oraz COM), można także uwzględnić duże formaty (MPEG, AVI, MP3, JPEG, ZIP) obciążające serwer pocztowy ze względu na swój rozmiar. Wszystkie rozszerzenia należy wpisywać oddzielając je średnikami: np. *.exe; *.dll.

Włączenie opcji Filtruj także zagnieżdżone wiadomości spowoduje filtrowanie wiadomości załączonych w innych wiadomościach. Zaleca się, aby opcja była zawsze włączona.

Jeśli zaznaczona zostanie opcja Zmień nazwy załączników, filtr nie będzie automatycznie usuwał wiadomości spełniających kryteria. Zmieniona zostanie nazwa pliku (przez dodanie rozszerzenia), co zapobiegnie jego uruchomieniu. Przed uruchomieniem załącznika, użytkownik będzie musiał zapisać go na dysku i zmienić nazwę na pierwotną. Jeśli natomiast opcja nie będzie zaznaczona, załączniki będą usuwane.

W polu Dodaj wpisz tekst, który ma zostać dodany do nazwy pliku (np. *.exe.danger). W polu Dodaj komunikat do w treści wiadomości można ustalić treść komunikatu dodawanego przez program do zmodyfikowanej wiadomości.

7.2.5 Filtr treści

Za pomocą tego narzędzia można odfiltrować i zablokować wiadomości zawierające w treści lub temacie określone ciągi znaków. Zdefiniuj regularne wyrażenie wpisując słowa kluczowe i ciągi znaków, na które program MailSecurity ma reagować, i określ Zakres wyszukiwania w odpowiednim polu. Następnie trzeba ustalić reakcję programu na wykrycie zdefiniowanego ciągu znaków (powiadomienie nadawcy, odrzucenie wiadomości, powiadamianie innych osób o uruchomieniu filtra zawartości).

Obok pola Regularne wyrażenie znajduje się przycisk Nowy.... Kliknij aby otworzyć edytor wyrażenia logicznego. Tekst można dowolnie skonfigurować dzięki zastosowaniu funkcji logicznych I oraz LUB. Wyrażenia oddzielone parametrem I muszą wystąpić jednocześnie, aby filtr zadziałał, parametr LUB uruchomi filtr także jeśli tylko jedno z wyrażen zostanie odnalezione.

W oknie Wyrażenie logiczne można ręcznie skonstruować dowolne wyrażenie logiczne przy użyciu znaków zastępujących funkcje logiczne:

LUB	na klawiaturze	(Alt + <)	
I	na klawiaturze	(Shift + 6)	&

7.2.6 Filtr nadawców

Filtr ten pozwala na zablokowanie wiadomości pochodzących od konkretnych nadawców lub z konkretnych domen. W polu Adresy/Domeny wystarczy wpisać adresy lub domeny oddzielone średnikiem. MailSecurity nie przepuści wiadomości pochodzących z wpisanych domen i kont.

Dzięki tej funkcji można odfiltrować również wiadomości wysłane bez wypełnionego pola nadawcy.

7.2.7 Filtr odbiorców

Filtr ten pozwala na zablokowanie wiadomości wysyłanych do konkretnych osób lub domen. W polu Adresy/Domeny wystarczy wpisać adresy lub domeny oddzielone średnikiem. MailSecurity nie przepuści wiadomości wychodzących, zaadresowanych do wpisanych domen i kont.

Dzięki tej funkcji można odfiltrować również wiadomości wysłane bez wypełnionego pola odbiorcy (np. wiadomości z wypełnionym jedynie polem DW (do wiadomości)).

7.2.8 Filtr spamu

Filtr spamu umożliwia skuteczne i elastyczne blokowanie wiadomości o niepożądanych treściach lub pochodzących od niechcianych nadawców (np. konkretnych serwerów wysyłających spam). Program jest wyczulony na wszystkie cechy wiadomości typowe dla wysyłek masowych. Na podstawie wykrytych właściwości tworzony jest indeks spamu odzwierciedlający prawdopodobieństwo, że dana wiadomość jest spamem. Do dyspozycji jest szereg zakładek zawierających tematycznie pogrupowane funkcje filtra. Więcej informacji znajdziesz w rozdziale [Filtr](#).

7.2.9 Filtr adresów

Umożliwia blokowanie wiadomości wysyłanych przez konkretne komputery. Aby dodać adres IP do listy blokowanych serwerów, wpisz go w polu Odrzucaj wiadomości od następujących adresów i kliknij przycisk Dodaj.

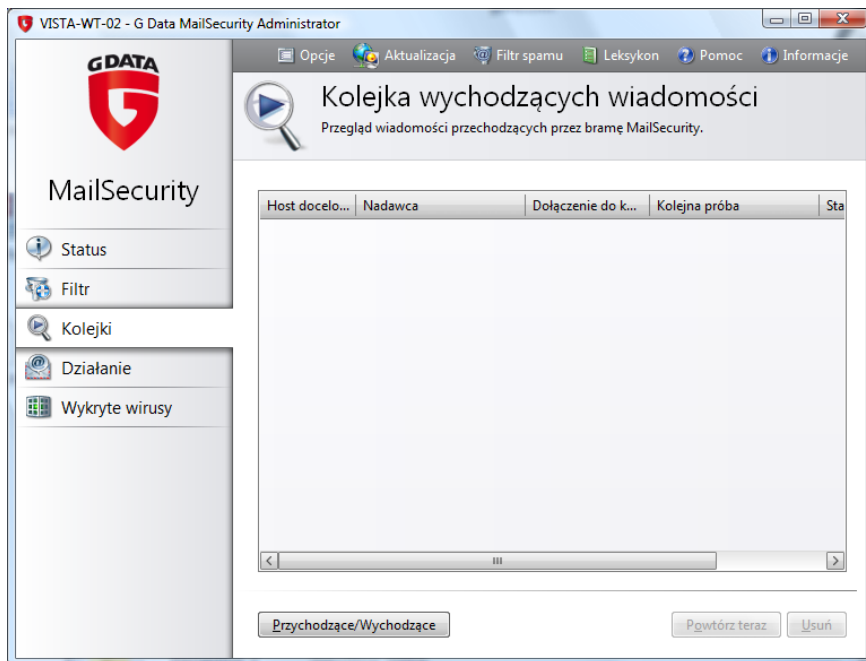
Można importować i eksportować listę adresów IP z/do pliku *.txt.

7.2.10 Filtr języków

Filtr języków umożliwia rozpoznawanie języka, w którym napisana jest wiadomość. Duża część niechcianych wiadomości to spam obcojęzyczny, zazwyczaj w języku angielskim. Zaznaczenie na liście języka angielskiego spowoduje odfiltrowanie wszystkich wiadomości w języku angielskim.

7.3 Widok Kolejki

W oknie Kolejki można obserwować przychodzące i wychodzące wiadomości czekające na kontrolę antywirusową, lub na ponowne przesłanie, jeśli adresat nie jest w danej chwili dostępny. Kontrola antywirusowa przebiega na bieżąco, MailSecurity powoduje jedynie nieznaczne opóźnienie ruchu. Po przesłaniu wiadomości zostają usunięte z listy. Jeśli któryś z serwerów (adresatów) jest niedostępny, przy wiadomości pojawi się odpowiednia adnotacja. Program ponawia próbę wysłania w regulowanych przez użytkownika odstępach czasowych (Opcje > Kolejka). Każde nieudana próba wysłania zostanie udokumentowana.



Przycisk Przychodzące/Wychodzące przełącza między kolejkami wiadomości przychodzących a wychodzących. Można nakazać programowi natychmiastowe wysłanie wiadomości klikając przycisk Powtórz teraz. Częstotliwość wysyłania plików ustala się w polu Interwał czasowy w zakładce Opcje > Kolejka. Przycisk Usuń powoduje usunięcie zaznaczonej wiadomości z kolejki.

7.4 Widok Działanie

W tym oknie protokolowane są wszystkie procesy wykonywane przez program MailSecurity, z określeniem godziny, numeru identyfikacyjnego oraz opisem. Za pomocą przycisku Wyczyść można usunąć wszystkie pozycje i rozpocząć protokolowanie na nowo.

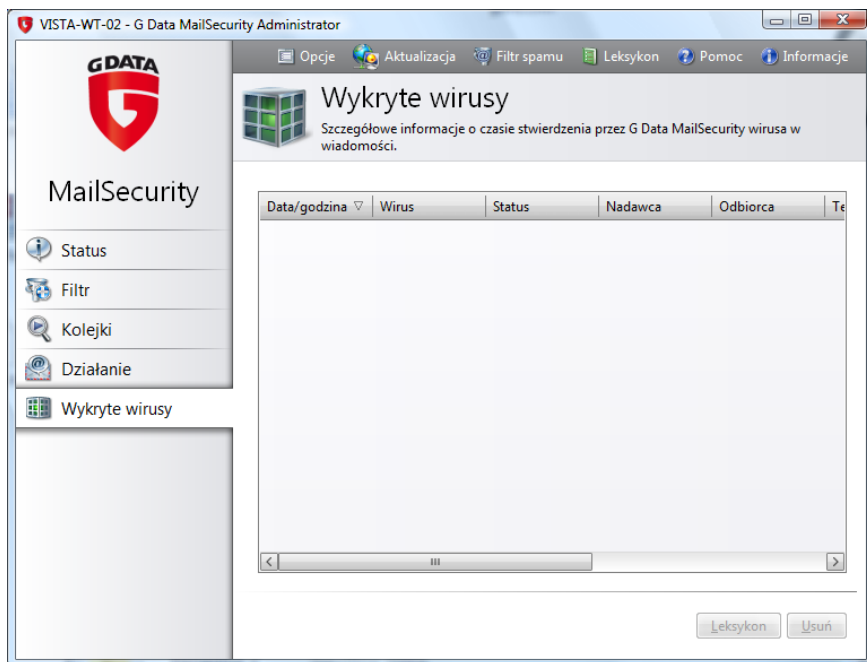


Numery ID pozwalają skojarzyć procesy z konkretnymi wiadomościami. Raporty o tym samym numerze ID dotyczą jednej wiadomości (np. 12345 wczytuję wiadomość, 12345 edytuję wiadomość, 12345 wysyłam wiadomość).

Uwaga: Bufor widoku Działanie jest czyszczony w momencie zamknięcia okna programu. Po ponownym uruchomieniu aplikacji, okno widoku Działanie jest puste, a gromadzenie danych rozpoczyna się od nowa.

7.5 Widok Wykryte wirusy

W tym oknie można znaleźć szczegółowe informacje na temat wszystkich przypadków wykrycia wirusa, włącznie z podjętymi środkami (np. Status: usunięto zainfektowany fragment, usunięto załącznik, wiadomość odrzucona) oraz adresy nadawcy i odbiorcy zainfektowanej wiadomości.



Przycisk Leksykon uruchamia serwis informacyjny o wirusach w Internecie. Poszczególne raporty z listy można usuwać za pomocą przycisku Usuń.

8 Pasek narzędzi

W pasku narzędzi znajdują się przyciski umożliwiające edycję najważniejszych ustawień programu i uruchomienie niektórych funkcji

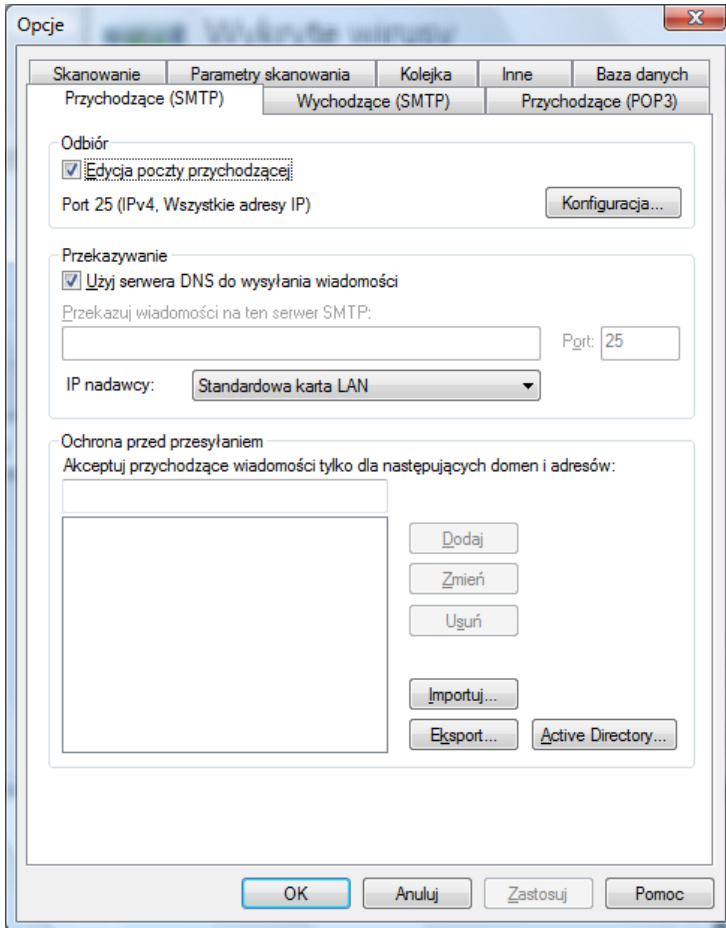
8.1 Opcje

Ustawienia zawarte w zakładkach okna Opcje pozwalają na optymalne dostosowanie pracy programu MailSecurity do warunków panujących w Twojej sieci. Wszystkie opcje pogrupowane są tematycznie w zakładkach. Kliknij wybraną zakładkę aby otworzyć grupę opcji.

Po kliknięciu przycisku OK zmiany zostaną zatwierdzone, a okno opcji zamknięte. Przycisk Anuluj spowoduje powrót do poprzednich ustawień i zamknięcie okna Opcji. Przycisk Zastosuj zatwierdza zmiany i pozostawia okno otwarte. Poszczególne ustawienia wyjaśnione zostały w następujących rozdziałach.

8.1.1 Przychodzące (SMTP)

W tej zakładce można dokonać ustawień związanych z przepływem oraz kontrolą wysyłanych wiadomości SMTP przed wysłaniem na serwer.



Odbiór i przesyłanie

W polu Port poczty przychodzącej wpisz numer portu, używanego do odbierania poczty w Twojej sieci. Aby przysłać wiadomości do serwera

pocztowego, wyłącz opcję Użyj serwera DNS do wysyłania wiadomości i w polu Przekazuj wiadomości na ten serwer SMTP wpisz nazwę serwera poczty. Należy wskazać również port, po którym poczta będzie wysyłana.

Ochrona przed przesyłaniem

Aby zapobiec wysyłaniu spamu z Twojego serwera poczty, możesz ograniczyć przesyłanie wiadomości wysyłanych do nieznanymi domen. W polu Akceptuj przychodzące wiadomości tylko dla następujących domen oraz adresów wpisz nazwy domen, do których serwer poczty może przesyłać wiadomości.

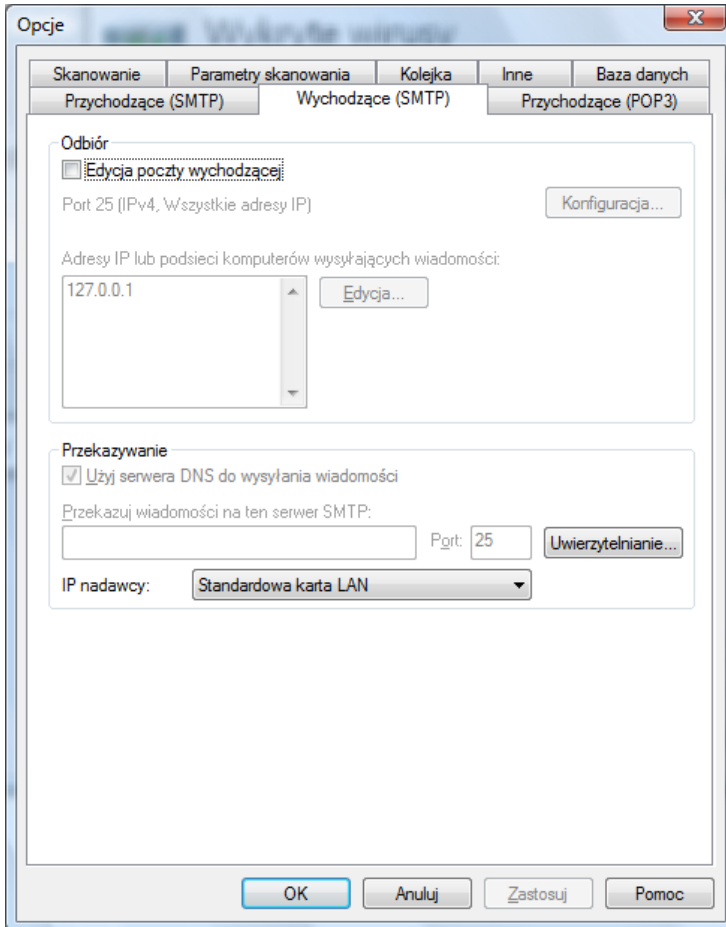
Uwaga: Jeśli nie dodasz żadnej domeny, program nie będzie odbierał wiadomości. Jak chcesz odbierać wiadomości dla wszystkich domen, wpisz wartość *.*.

Ochronę przed przesyłaniem można realizować również poprzez listę adresów e-mail. Wiadomości nie będą przesyłane do odbiorców, których nie ma na liście. Przydatnym narzędziem jest możliwość automatycznego pobierania adresów z Active Directory. Do połączenia z usługą Active Directory wymagana jest platforma .NET Framework w wersji 1.1 lub nowszej.

Wskazówka: Active Directory to baza danych stosowana w systemach Microsoft Windows do centralnego zarządzania informacjami o usługach, zasobach lub użytkownikach w sieciach Windows.

8.1.2 Wychodzące (SMTP)

W tej zakładce można dokonać ustawień związanych z przepływem oraz kontrolą wiadomości wychodzących SMTP.



Odbiór i przesyłanie

Zaznacz opcję Edycja poczty wychodzącej aby uruchomić kontrolę poczty wychodzącej na obecność wirusów. W polu Adresy IP lub podsiaci

komputerów wysyłających wiadomości wpisz adresy IP komputerów, z których wysyłane będą maile.

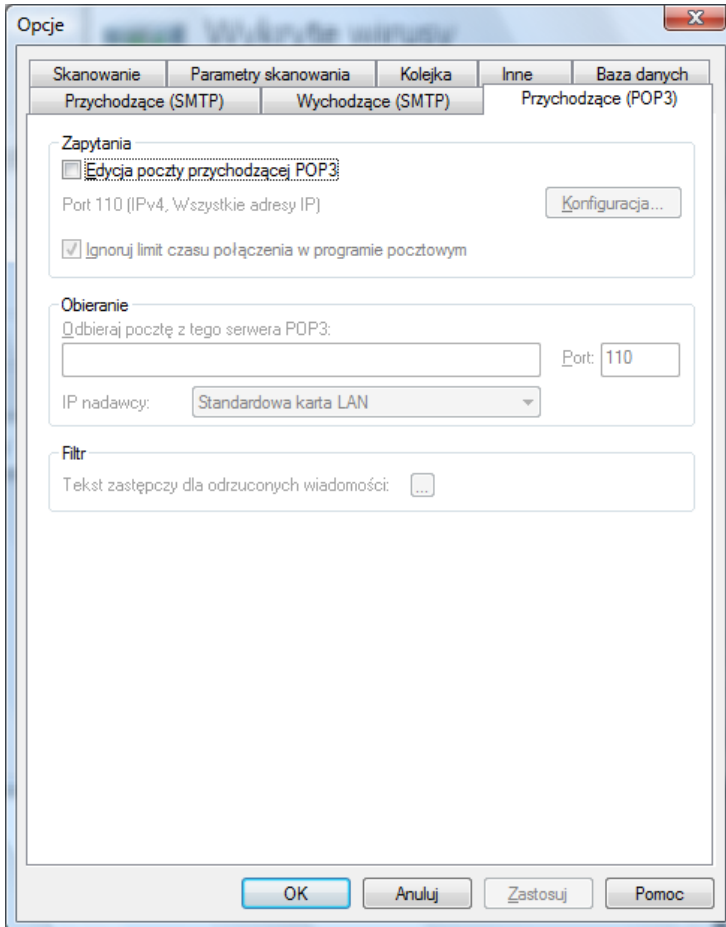
Dane te są niezbędne w celu odróżnienia poczty przychodzącej od wychodzącej.

W polu Port wiadomości przychodzących wpisz numer portu, z którego wiadomości przychodzą do programu MailSecurity.

Aby wiadomości były przesyłane bezpośrednio do domeny docelowej, należy włączyć opcję Użyj serwera DNS do wysyłania wiadomości. Jeśli strumień wiadomości ma przechodzić przez inny serwer (np providera), należy wyłączyć opcję używania serwera DNS i wpisać nazwę serwera w polu Przekazuj wiadomości na ten serwer SMTP.

8.1.3 Przychodzące (POP3)

W tej zakładce można dokonać ustawień związanych z przepływem oraz kontrolą wiadomości przychodzących POP3.



Odbiór i przesłanie

Uruchom opcję Edycja poczty przychodzącej POP3 aby włączyć ochronę antywirusową wiadomości przychodzących. Po skanowaniu poczta jest

przesyłana do odbiorców. Należy wskazać port wykorzystywany przez Twój program pocztowy do komunikacji z serwerem POP3 (zazwyczaj 110), a w polu Odbieraj pocztę z tego serwera POP3, nazwę serwera poczty POP3 (np. pop3.mojapoczta.pl). Funkcja Ignoruj limit czasu połączenia w programie pocztowym daje klientowi poczty więcej czasu na odbiór wiadomości podczas gdy MailSecurity je skanuje.

Wskazówka: Programy pocztowe oparte o protokół POP3 można skonfigurować ręcznie. Jako nazwę serwera POP3 należy wpisać 127.0.0.1 lub adres komputera z programem MailSecurity, a nazwę użytkownika trzeba poprzedzić nazwą zewnętrznego serwera poczty i dwukropkiem.

Czyli zamiast

POP3:poczta.xxx.pl / Użytkownik:Jan Nowak

należy wpisać

POP3:127.0.0.1 / Użytkownik:poczta.xxx.pl:Jan Nowak.

Dokładny opis ręcznej konfiguracji znajdziesz w dokumentacji technicznej danego programu pocztowego.

Filtr

Jeżeli wiadomość POP3 zostanie zatrzymana przez filtr treści lub skaner antywirusowy, nadawca wiadomości może zostać o tym powiadomiony. Treść standardowego powiadomienia brzmi: Wiadomość odrzucona przez administratora.

Aby zmienić treść powiadomienia, należy kliknąć przycisk ●●● obok opcji powiadomienia i skonstruować nową treść. Dozwolone jest używanie znaków specjalnych zastępujących parametry wiadomości:

%v Wirus

%s Nadawca

%r Odbiorca

%c DW

%d Data

%u Temat

%h	Nagłówek
%i	IP nadawcy

8.1.4 Skanowanie

Opcje w tej zakładce dotyczą ustawień kontroli antywirusowej wiadomości przychodzących i wychodzących.

Przychodzące

Zaleca się uruchomienie opcji Szukaj wirusów w przychodzących wiadomościach oraz wybór reakcji na wykrycie wirusa:

- Tylko protokół
- Dezynfekuj (Jeśli się nie da: tylko protokół)
- Dezynfekuj (Jeśli się nie da: zmień nazwę pliku)
- Dezynfekuj (Jeśli się nie da: usuń plik)
- Zmień nazwy zarażonych załączników
- Usuń zarażone załączniki
- Usuń wiadomość

Ustawienie Tylko protokół ma sens tylko wtedy, gdy system jest chroniony przed wirusami w inny sposób (np. programem G Data AntiVirus Business).

Wychodzące

Funkcja Szukaj wirusów w wychodzących wiadomościach oraz Nie przesyłaj zainfekowanych wiadomości powinny być stale włączone. Dzięki temu żaden wirus nie zostanie wysłany z Twojej sieci.

Do dyspozycji jest szereg możliwości konstruowania powiadomień o wykryciu wirusa. Do powiadomienia adresata można dołączyć m.in. temat oraz treść zarażonej przesyłki. Powiadomić daje się także nadawcę zarażonego maila, a także wybrane osoby, np. administratora systemu. Adresy odbiorców powiadomień oddziel przy wpisywaniu średnikami. Aby zmienić treść powiadomienia, należy kliknąć przycisk ●● obok opcji

powiadomienia i skonstruować nową treść. Dozwolone jest używanie znaków specjalnych zastępujących parametry wiadomości:

%v	Wirus
%s	Nadawca
%r	Odbiorca
%c	DW
%d	Data
%u	Temat
%h	Nagłówek
%i	IP nadawcy

Dodatkowo można uruchomić opcję dołączania raportu o dokonanej kontroli przez MailSecurity do wysyłanych nie zawirusowanych wiadomości.

Standardowo treść raportu brzmi:

Poczta sprawdzona przez G Data AntiVirus

Wersja: %x z dnia %y

Informacje: www.gdata.pl

Zmienne %x i %y oznaczają:

%x numer wersji i sygnatur wirusów

%y data sygnatur wirusów

Oczywiście istnieje możliwość modyfikacji lub wyłączenia komunikatu powiadomienia.

G Data AntiVirus Business

Jeśli stosujesz program G Data AntiVirus Business, możesz uaktywnić opcję Powiadom o infekcji program G Data AntiVirus Business. Komunikacja między tymi programami zwiększy bezpieczeństwo Twojej sieci.

8.1.5 Parametry skanowania

W tym oknie można dopasować parametry skanowania wiadomości do potrzeb Twojej sieci. Zwiększenie wydajności skanowania powoduje nieznaczne spowolnienie strumienia wiadomości.

Program MailSecurity pracuje przy użyciu dwóch niezależnych skanerów antywirusowych, odpowiedzialnych za różne partie analizy antywirusowej. Optymalne efekty daje oczywiście zastosowanie dwóch skanerów. Przy użyciu tylko jednego z nich, proces trwa krócej. Zalecamy ustawienie Dwa skanery. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor.

Dzięki tej opcji istnieje możliwość wskazania rodzajów skanowanych plików. Z reguły nie ma potrzeby kontroli plików, które się nie uruchamiają, kontrola całego systemu plików może zająć dość dużo czasu. Zaleca się ustawienie Automatyczne rozpoznanie plików – sprawdzone zostaną tylko pliki mogące teoretycznie zawierać wirusa.

Możesz samodzielnie zdefiniować rodzaje plików, które mają być uwzględnione podczas skanowania. W tym celu wybierz opcję Pliki użytkownika. Kliknij przycisk ... aby otworzyć okno, wyboru plików. Wpisane rozszerzenia zatwierdza przycisk Dodaj.

Możliwe jest stosowanie masek plików z wykorzystaniem następujących znaków zastępczych:

- ? zastępuje pojedynczy znak
- * zastępuje ciąg znaków

Aby wybrać np. wszystkie pliki z rozszerzeniem .exe, wpisz *.exe. Aby wybrać np. wszystkie pliki o formacie arkuszy kalkulacyjnych (jak np. *.xlr, *.xls), wpisz *.xl?. Jeśli chcesz sprawdzać pliki o takim samym początku nazwy wpisz np. tekst*.*.

Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując kody plików z kodami stale aktualizowanej bazy znanych wirusów, lecz rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, z jednej strony wzmacnia skuteczność skanowania, ale jest bardzo czasochłonna, a w niektórych przypadkach może powodować fałszywe alarmy.

Zalecamy również pozostawienie włączonej opcji skanowania spakowanych plików.

OutbreakShield

Moduł OutbreakShield umożliwia rozpoznanie i zwalczanie wirusów jeszcze przed opracowaniem odpowiednich sygnatur wirusów. Moduł OutbreakShield łącząc się z odpowiednim serwerem ustala czy wiadomość stanowi zagrożenie na podstawie jej cech charakterystycznych. Dzięki temu jest w stanie zareagować na zagrożenie dużo wcześniej przed stworzeniem i dostarczeniem odpowiednich sygnatur wirusów. Moduł jest zintegrowany z ochroną poczty elektronicznej.

Ze względu na specyficzną budowę, moduł OutbreakShield nie potrafi dezynfekować wiadomości, przenosić ich do Kwarantanny ani też zmieniać nazw załączników. Użytkownik informowany jest o infekcji przez tekst zastępczy. Jeśli w oknie Kontrola antywirusowa wybrana zostanie opcja Usuń wiadomość, OutbreakShield nie ma możliwości poinformowania użytkownika o wykryciu wirusa.

8.1.6 Kolejka

Ta zakładka pozwala ustalić w jakich odstępach czasowych zachodzić ma proces ponownego wysyłania wiadomości czekających w kolejce. Wiadomości zatrzymywane są w kolejce z różnych przyczyn. Np. dlatego, że adresat (albo serwer poczty) w danej chwili jest niedostępny.

Wiadomości umieszczane są w kolejce po przeprowadzeniu kontroli antywirusowej przez program MailSecurity.

Niedoreczone wiadomości

W polu Interwał czasowy wpisz, w jakich odstępach czasu program ma podejmować kolejne próby wysłania wiadomości przetrzymywanych w kolejce. Np. wpis 1, 1, 1, 4 spowoduje, że program podejmie próbę wysłania trzykrotnie co godzinę, a następnie będzie próbował co 4 godziny. W polu Czas oczekiwania na błąd (h) zdefiniuj czas, który upłynie zanim program ostatecznie usunie wiadomość z kolejki.

Istnieje również opcja powiadamiania nadawców wiadomości w określonych w polu numerycznym odstępach czasu. Jeśli nie chcesz regularnie

powiadamiać nadawców, wpisz w pole wartość zero. Nawet jeśli powiadomienie zostanie wyłączone, nadawca zostanie i tak powiadomiony o nie doręczeniu wiadomości i jej usunięciu z serwera.

Przywrócenie standardowych ustawień kolejki uzyskuje się przez kliknięcie przycisku Przywróć domyślne.

Ograniczenie rozmiaru

Program umożliwia ograniczenie rozmiaru kolejki. Dzięki temu można uniknąć przepełnienia kolejki w momencie przetwarzania dużych ilości wiadomości - np. w razie ataku typu Denial of Service.

8.1.7 Inne

W tej zakładce znajdziesz globalne ustawienia programu MailSecurity.

Nazwa komputera

W tym oknie możesz wprowadzić w pełni kwalifikowaną nazwę komputera z rozszerzeniem domeny. To ustawienie wymagane jest przez niektóre serwery poczty.

Ograniczenie

Włącz tę opcję, jeśli chcesz ograniczyć liczbę połączeń SMTP obsługiwanych przez MailSecurity. W ten sposób możesz dopasować filtrowanie wiadomości do wydajności sprzętu, na którym pracuje program.

Komunikaty systemowe

Adres nadawcy wiadomości systemowych wykorzystywany jest np. przy wysyłaniu powiadomień do nadawców i odbiorców zarażonych wiadomości. Program wysyła także niezależne od powiadomień komunikaty wiążące się z potencjalnymi zagrożeniami ze strony wirusów. Użytkownicy są także ostrzegani, jeśli ochrona antywirusowa przestaje działać z jakichkolwiek powodów. Adresy odbiorców ostrzeżeń systemowych mogą się np. pokrywać z adresami używanymi przez protokoły SMTP i POP3.

Zmień hasło

Ta opcja pozwala zmienić hasło ustalone przy pierwszym uruchomieniu programu MailSecurity. Wystarczy podać aktualne hasło, w polu poniżej

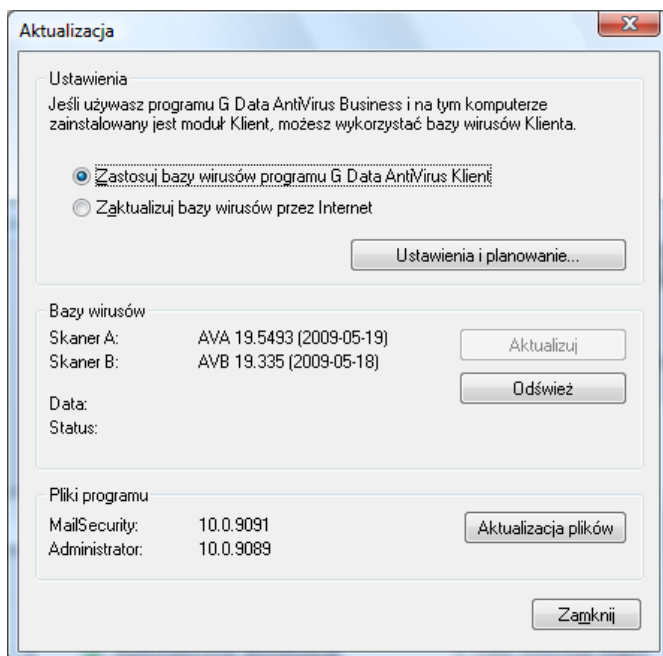
nowe, a na samym dole potwierdzić nowe hasło.

8.1.8 Baza danych

Opcje w zakładce Baza danych dotyczą przechowywania raportów usługi statystyk poczty. Ustawienia pozwalają ograniczyć rozmiary bazy danych z raportami. Podgląd okna statystyk dostępny jest poprzez kliknięcie przycisku Statystyki w widoku [Status](#).

8.2 Aktualizacja

W oknie aktualizacji można dokonać ustawień dotyczących pobierania aktualizacji sygnatur wirusów oraz plików programowych przez Internet.



8.2.1 Sekcja Ustawienia

Jeśli równocześnie z programem G Data MailSecurity używasz programu G Data AntiVirus Business, możesz wykorzystywać w programie funkcję Zastosuj bazy wirusów programu G Data AntiVirus Klient. Dzięki temu unikniesz podwójnego pobierania aktualizacji baz z Internetu. Oczywiście możliwe jest też pobieranie baz wirusów bezpośrednio z serwera aktualizacji.

Przycisk Ustawienia i planowanie otwiera okno podstawowych ustawień ręcznej i automatycznej aktualizacji programu.

8.2.1.1 Dane dostępu do aktualizacji

W polach zakładki Dane dostępu wpisz nazwę użytkownika i hasło otrzymane na potwierdzeniu rejestracji programu. Jeżeli zamierzasz teraz zarejestrować program, kliknij przycisk Rejestracja online....

Do zarejestrowania programu potrzeba jest numer rejestracyjny. Znajdziesz go w opakowaniu z zakupionym programem lub w wiadomości z realizacją zamówienia w przypadku dokonania zakupu online. Po zarejestrowaniu produktu, dane dostępu zostaną automatycznie zastosowane w programie, a także wysłane na wpisany w formularzu adres mailowy.

8.2.1.2 Planowanie

Zakładka Planowanie umożliwia ustalenie częstotliwości przeprowadzania automatycznych aktualizacji. W sekcji Wykonaj zaznacz pożądany interwał czasowy i uzupełnij szczegóły, np. godzinę i dni tygodnia, w które ma przebiegać proces aktualizacji.

8.2.1.3 Ustawienia

Jeżeli używasz urządzenia sieciowego wymagającego autoryzacji lub serwera proxy, zaznacz opcję Skorzystaj z serwera proxy. Wpisz adres serwera i port w odpowiednich polach. Jeżeli niezbędna jest autoryzacja, wpisz również nazwę użytkownika oraz hasło.

8.2.1.4 Konto użytkownika

Jeśli jest to wymagane, w polu Konto użytkownika wpisz nazwę użytkownika z dostępem do Internetu na komputerze z zainstalowanym programem G Data MailSecurity.

8.2.2 Sekcja Bazy wirusów

Za pomocą przycisków Aktualizacja baz wirusów i Odśwież status możesz przeprowadzić aktualizację niezależnie od zaplanowanych aktualizacji automatycznych.

8.2.3 Sekcja pliki programu

Przyciskiem Aktualizacja plików możesz uruchomić aktualizację plików programu G Data MailSecurity, oczywiście jeśli udostępniona jest nowsza wersja.

8.3 Filtr spamu

Filtr spamu umożliwia skuteczne i elastyczne blokowanie wiadomości o niepożądanych treściach lub pochodzących od niechcianych nadawców (np. konkretnych serwerów wysyłających spam). Program jest wyczulony na wszystkie cechy wiadomości typowe dla wysyłek masowych. Na podstawie wykrytych właściwości tworzony jest indeks spamu odzwierciedlający prawdopodobieństwo, że dana wiadomość jest spamem. Do dyspozycji jest szereg zakładek zawierających tematycznie pogrupowane funkcje filtra.

8.3.1 Filtr

Reakcja filtra spamu na stwierdzenie niechcianej wiadomości może zależeć od oszacowanego indeksu prawdopodobieństwa spamu. Program umożliwia trzy różne reakcje dla trzech progowych wartości indeksu.

W zależności od wysokości indeksu prawdopodobieństwa spamu

szacowanego na podstawie określonych kryteriów, program dzieli wiadomości na 3 grupy. Reakcję dla każdej z nich można określić po kliknięciu przycisku Zmień.

Program może odrzucić wiadomość lub tylko dołączyć komunikaty w temacie i treści wiadomości. Dodatkowo można powiadomić nadawcę wiadomości o wysłaniu niechcianej przesyłki, a także powiadomić określone osoby, np. administratora o fakcie nadejścia niechcianej wiadomości. Program umożliwia modyfikację tekstu wszelkich komunikatów dołączanych do wiadomości i wysyłanych do konkretnych adresatów.

8.3.2 Zaufana lista

Lista zaufanych nadawców pozwala na utworzenie wyjątków programu w postaci adresów e-mail lub całych domen. Wprowadź zaufany adres e-mail lub domenę i kliknij przycisk Dodaj aby utworzyć wyjątek. Listę wyjątków można także wyeksportować i zaimportować z pliku *.txt.

8.3.3 Czarna lista

Ta zakładka umożliwia stworzenie listy blokowanych adresów e-mail i domen. Wpisz adres e-mail lub domenę, z której nie chcesz otrzymywać wiadomości i kliknij przycisk Dodaj. Listę blokowanych domen można wyeksportować a także zaimportować z pliku w formacie *.txt.

8.3.4 Realtime Blacklists

W Internecie istnieją strony publikujące listy adresów serwerów wysyłających spam. Zalecamy stosowanie standardowych adresów list Realtime Blacklists. To okno umożliwia również utworzenie wyjątków od reguły. Wpisz w oknie Nie używaj "czarnych list" dla następujących domen domenę, którą chcesz wyjąć spod ochrony programem i kliknij przycisk Dodaj.

8.3.5 Słowa kluczowe (temat)

W tej zakładce można zdefiniować słowa kluczowe, na które program ma zwrócić szczególną uwagę kontrolując tematy wiadomości. Jeśli w temacie wykryte zostanie choć jedno słowo zawarte na liście, program podniesie indeks prawdopodobieństwa spamu dla danej wiadomości. Listę można modyfikować za pomocą przycisków Dodaj, Zmień i Usuń. Listę wyrażeń kluczowych można importować i eksportować do pliku *.txt. Opcja Znajdź tylko całe wyrazy spowoduje, że program nie będzie reagował jeśli wykryje słowo kluczowe zawarte w innym wyrazie, np. "dick" w "dickens".

8.3.6 Słowa kluczowe (treść)

W tej zakładce można zdefiniować słowa kluczowe, na które program ma zwrócić szczególną uwagę kontrolując treść wiadomości. Jeśli w treści wykryte zostanie choć jedno słowo zawarte na liście, program podniesie indeks prawdopodobieństwa spamu dla danej wiadomości. Listę można modyfikować za pomocą przycisków Dodaj, Zmień i Usuń. Listę wyrażeń kluczowych można importować i eksportować do pliku *.txt. Opcja Znajdź tylko całe wyrazy spowoduje, że program nie będzie reagował jeśli wykryje słowo kluczowe zawarte w innym wyrazie, np. "dick" w "dickens".

8.3.7 Filtr treści

Jest to samouczący się mechanizm wykorzystujący inteligentny filtr treści Bayesa. Wraz z upływem czasu program uczy się nowych słów kluczowych dodając je automatycznie do listy. Przycisk Sprawdź w tabeli wyświetla listę wyuczonych wyrażeń. Aby usunąć z listy wszystkie wyuczone wyrażenia kliknij przycisk Wyczyść tabelę. Proces gromadzenia wyrażeń kluczowych rozpocznie się od nowa.

8.3.8 Zaawansowane

Okno umożliwia szczegółowe ustawienia kryteriów kwalifikowania wiadomości. Zalecamy jednak pozostawienie domyślnych ustawień programu. Przycisk Indeksy prawdopodobieństwa umożliwia modyfikację wartości indeksów przyznawanych za spełnianie konkretnych kryteriów. Nierozważne modyfikowanie wartości indeksów może spowodować

nieprawidłowe działanie programu.

