Firewall. Szybki start

Autorzy: Jacek Matulewski,
Jarosław Ratkowski, Krzysztof Żebrowski
ISBN: 83-7361-350-1
Format: B5, stron: 212

Dawno już minęły czasy, kiedy wirusy „łapało się" z dyskietek i CD-ROM-ów. Dziś najwięcej wirusów atakuje nas z internetu. Jednak wirusy to nie jedyne zagrożenie czyhające na internautów. Innym, równie poważnym, są hakerzy – osoby, które włamują się do komputerów podłączonych do sieci. Na szczęście przed większością zagrożeń pochodzących z internetu możemy się zabezpieczyć, stosują aplikacje zwane zaporami sieciowymi (firewallami). Odpowiednio skonfigurowany firewall w połączeniu z programem antywirusowym ochroni nasze komputery przed atakami wirusów i hakerów.

Książka „Firewalle. Szybki start" to przewodnik po najpopularniejszych zaporach sieciowych przeznaczonych dla komputerów osobistych. Opisuje firewalle pracujące pod kontrolą systemów z rodziny Windows oraz takie, które możemy zastosować w systemie Linux. Zaprezentowane w książce aplikacje są powszechnie dostępne w sieci. Przedstawiony jest sposób ich instalacji i konfiguracji, definiowania reguł filtrowania oraz tworzenia raportów.

- Bezpieczeństwo komputera w sieci
- Kerio Personal Firewall 4
- Zone Alarm 5
- Instalacja i konfiguracja zapory sieciowej
- Konfiguracja połączeń i ostrzeżeń
- Definiowanie reguł filtracji pakietów i protokołów
- Monitorowanie poczty elektronicznej
- Zapora sieciowa dostępna w systemie Windows XP
- Firewalle dla systemów z rodziny Linux – Madrake, Fedora oraz SuSE

Przekonaj się, jak proste może być zabezpieczenie komputera

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Kerio Personal Firewall 4

3

Dostępne wersje i edycje Kerio

Zespół osób, który stworzył Kerio Personal Firewall, wywodzi się z firmy Tiny Software Inc., gdzie pracował nad Tiny Personal Firewall. Po jej opuszczeniu i stworzeniu własnej firmy Kerio Technologies Inc. wydał własny firewall Kerio Personal Firewall od razu w wersji 2. Od listopada 2003 roku nie jest on już rozwijany i nie jest dostępny na stronie producenta, ale wciąż jest bardzo popularny.

Firma skupiła się obecnie na całkowicie nowym produkcie — Kerio Personal Firewall 4, który jest nieustannie rozwijany; aktualizacje pojawiają się wręcz co kilka tygodni. W odróżnieniu od swojego ascetycznego poprzednika, Kerio 4 zaskakuje kolorowym interfejsem oraz całkiem nowym ułożeniem okien konfiguracji ze znacznie większą ilością ustawień. Dotychczasowych użytkowników Kerio 2.15, którzy przesiedli się na wersję 4, wprawia zwykle w zakłopotanie to, że nie jest to tylko proste rozwinięcie już znanego produktu. Zmienił się nie tylko wygląd interfejsu, ale także ilość i sposób konfigurowania opcji. Wersja 2.15 zyskała bardzo dobrą opinię wśród użytkowników chcących zabezpieczyć swoje komputery. Co niektórzy twierdzą wręcz, że ten program był, a nawet ciągle jest, najlepszą zaporą sieciową na rynku darmowego oprogramowania domowego. Niestety, oficjalnie był on dostępny tylko w wersji angielskiej[1].

Kerio 4, choć bardziej złożony, jest znacznie nowocześniejszy i pozwala na znacznie elastyczniejsze skonfigurowanie, a w związku z ciągle trwającymi nad nim pracami, coraz lepiej chroni komputery. Ponadto wersja 4 jest (poza procesem instalacji i plikami pomocy) spolszczona. Po zainstalowaniu Kerio rozpoznaje język używany przez system i automatycznie dostarcza polską wersję interfejsu[2]. Wersja 4 posiada wszystkie rozwiązania wcześniejszego produktu, ale rozszerza je o nowe możliwości. Tu jednak kryje się haczyk. Aby w pełni skorzystać z nowych rozwiązań, należy za program zapłacić i to wcale niemało: obecnie 49 dolarów plus 22 dolary za subskrypcję.

[1] W sieci można było znaleźć spolszczenie firmowane przez Pabla (*http://www.kerio.tk/*)

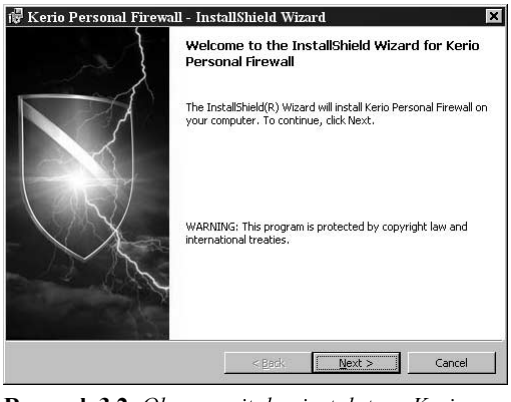
[2] Wykonaną również przez Pabla. W spolszczeniu można napotkać literówki i niezręczne sformułowania, ale nie wpływa to znacząco na jego zrozumiałość.

Program możemy ściągnąć ze strony producenta i testować przez 30 dni. Jeżeli do tego czasu za niego nie zapłacimy — zostanie uszczuplony o niektóre opcje (zobacz tabela 3.1). Należy jednak podkreślić, że darmowa wersja Kerio 4 jest jak najbardziej wystarczającym narzędziem do ochrony komputera. Opcje dodatkowe, np. dotyczące blokowania reklam na stronach WWW oraz kontrola plików cookies, które zostaną dezaktywowane po 30 dniach, można zastąpić używając opcji przeglądarek oraz innych programów.

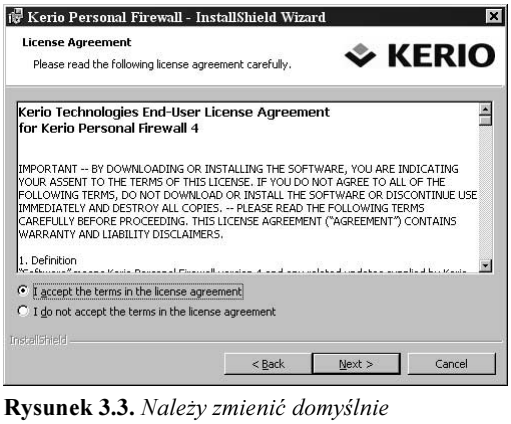
Tabela 3.1. *Podstawowe różnice pomiędzy poszczególnymi dystrybucjami*

	Kerio 2.15	Kerio 4 (darmowy)	Kerio 4 (komercyjny)
Ochrona sieci			
kontrola dostępu aplikacji do sieci	tak	tak	tak
filtr pakietów	tak	tak	tak
wykrywanie ataków	nie	tak	tak
tryb pracy dla routera (brama internetowa)	tak	nie	tak
Ochrona systemu			
kontrola uruchamiania aplikacji	nie	tak	tak
kontrola uruchamiania aplikacji przez inne aplikacje	nie	tak	tak
kontrola modyfikacji plików aplikacji	tak	tak	tak
Filtrowanie zawartości stron WWW			
kontrola plików cookies	nie	nie	tak
kontrola wysyłanych informacji	nie	nie	tak
blokowanie skryptów (JavaScript, VB Script)	nie	nie	tak
blokowanie reklam i okien pop-up	nie	nie	tak
Statystyki, rejestrowanie zdarzeń (logi) oraz serwis firewalla			
statystyka wykrytych prób ataków	nie	tak	tak
statystyka i rejestracja zdarzeń związanych z siecią	nie	tak	tak
rejestracja zdarzeń związanych z systemem	tak	nie	tak
Administracja i serwis firewalla			
automatyczna aktualizacja programu	nie	tak	tak
zdalna administracja	tak	nie	tak
konfiguracja chroniona hasłem	tak	nie	tak

Rysunek 3.1. *Wybór języka instalacji*



Rysunek 3.2. *Okno powitalne instalatora Kerio*



Rysunek 3.3. *Należy zmienić domyślnie zaznaczone pole*

Instalacja

Kerio można ściągnąć ze strony *http://www.kerio.com/kpf_download.html*. Instalacja, przygotowana za pomocą Install Shield, jest typowa dla programów Windows.

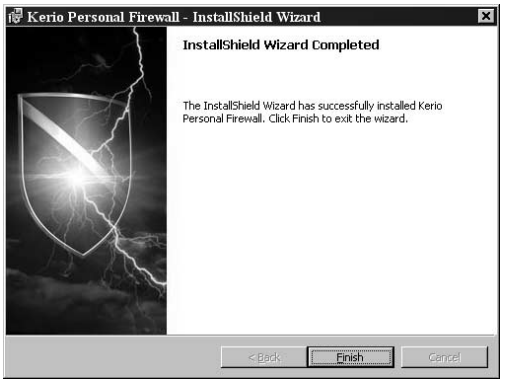
Aby zainstalować Kerio 4:

1. Uruchamiamy program instalacyjny (np. *kerio-pf-4.0.16-en-win.exe*).
2. Wybieramy język instalacji z rozwijanej listy (rysunek 3.1; dostępny jest tylko angielski i niemiecki) i klikamy *OK*.
3. Po wstępnym rozpakowaniu plików niezbędnych do instalacji do katalogu tymczasowego zobaczymy okno powitalne instalatora Kerio Personal Firewall (rysunek 3.2).
4. Klikamy *Next* (dalej).
5. Następny krok instalatora pokazuje historię rozwoju Kerio 4. Ponownie klikamy *Next*.
6. W kolejnym kroku[3] wyrażamy zgodę na warunki licencji (rysunek 3.3), tzn. zaznaczamy pole *I accept the terms in the licencse agreement* (godzę się na warunki umowy licencyjnej) i klikamy *Next*.

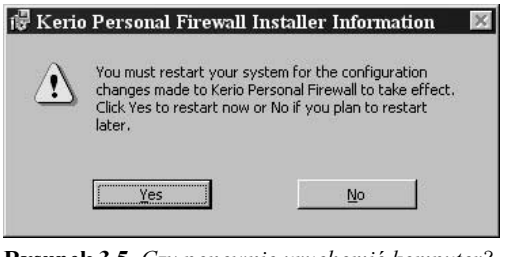
[3] Po uprzednim przeczytaniu umowy licencyjnej.

7. Kolejny krok to wybór katalogu, w którym zainstalowany zostanie Kerio. Najlepiej pozostawić domyślną lokalizację w katalogu *Program Files\Kerio*. Klikamy ponownie *Next*.
8. W następnym kroku instalacji potwierdzamy wybrane ustawienia za pomocą przycisku *Install* (instaluj).
9. Po krótkiej chwili pojawi się okno informujące o zakończeniu instalacji (rysunek 3.4). Należy nacisnąć *Finish* i w nowym oknie (rysunek 3.5) potwierdzić chęć ponownego uruchomienia komputera klikając przycisk *Yes* (tak).

W systemach opartych na technologii NT po zainstalowaniu Kerio 4 i restarcie komputera uruchomiona zostanie usługa o nazwie Kerio Personal Firewall 4 w trybie automatycznego uruchamiania. Od tego momentu komputer jest chroniony przez ten firewall. W tabeli 3.2 przedstawiono możliwe stany Kerio prezentowane przez ikonę w zasobniku systemowym.



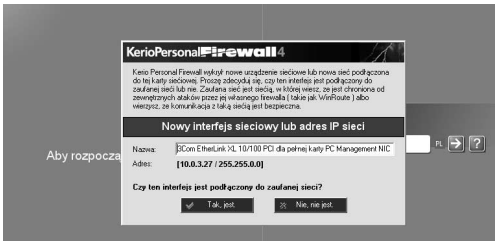
Rysunek 3.4. *Tak powinna zakończyć się instalacja Kerio 4*



Rysunek 3.5. *Czy ponownie uruchomić komputer?*

Tabela 3.2. *Informacja o stanie Kerio prezentowana za pomocą ikony w zasobniku*

Ikona	Stan Kerio
	kerio jest w stanie czuwania (aktywne); żadna aplikacja w bieżącej chwili nie korzysta z połączenia sieciowego
	połączenie jest aktywne; obecność zielonej „diody" świadczy o połączeniu wychodzącym, czerwonej — przychodzącym; wysokość „słupków" świadczy o intensywności ruchu w jedną i drugą stronę
	firewall jest aktywny, ale wszelki ruch na połączeniach sieciowych jest zablokowany
	firewall został dezaktywowany; komputer nie jest chroniony
	tymczasowe dopuszczenie reklam i okien pop-up w przeglądanych stronach WWW (naciśnięty klawisz *Ctrl* lub *F12* w zależności od ustawień)



Rysunek 3.6. *To ostrzeżenie jest dowodem, że firewall działa nawet wówczas, gdy żaden użytkownik nie jest wlogowany*

Konfiguracja połączeń stałych i modemowych

To jednak nie koniec czynności związanych z „ustawieniem" tej zapory. Po ponownym uruchomieniu komputera rozpocznie się proces konfiguracji, który w zasadzie trwa nieustannie. Na szczęście na tym etapie Kerio zna już język polski, choć pliki pomocy nadal nie są przetłumaczone. Proces konfiguracji polega na stałej interakcji z użytkownikiem: w momencie użycia nowej karty sieciowej, nowego numeru dostępowego przy łączeniu z siecią modemem, próby połączenia aplikacji z siecią, uruchamiania aplikacji przez inną aplikację itp. Kerio zada pytanie, w którym mamy możliwość dopuszczenia lub zablokowania akcji oraz, co jest właśnie istotą wspomnianej interaktywnej konfiguracji, możliwość stworzenia reguły, która pozwoli na zastosowanie podjętej przez użytkownika decyzji w następnych tego samego typu sytuacjach. W miarę upływu czasu ilość reguł się zwiększa i pytania pojawiają się coraz rzadziej, a tym samym firewall uczy się naszych preferencji.

Aby ustalić status połączenia przez stałe łącze:

1. Jeżeli komputer w momencie uruchomienia systemu (przed zalogowaniem użytkownika) jest już podłączony do sieci, przy pierwszym uruchomieniu Kerio zobaczymy pytanie o uznanie połączenia za godne zaufania (rysunek 3.6).

   ▲ Jeżeli aktywna karta sieciowa skonfigurowana jest tak, że komputer jest elementem sieci lokalnej, która jest chroniona osobnym firewallem centralnym, możemy kliknąć przycisk *Tak, jest*. Ograniczamy wówczas ochronę komputera przy łączeniu z siecią przez ten interfejs. Można to oczywiście w każdej chwili zmienić[4].

[4] W dalszej części okaże się, na czym polega owo ograniczenie ochrony, w jaki sposób można je kontrolować.

2. Po odpowiedzi na powyższe pytanie i rozpoczęciu logowania użytkownika pojawią się kolejne pytania związane z próbą połączenia ze zdalnymi komputerami (serwerami) przez serwisy uruchamiane na naszym komputerze obsługujące połączenie internetowe (rysunek 3.7). Są to w takim razie połączenia wychodzące.

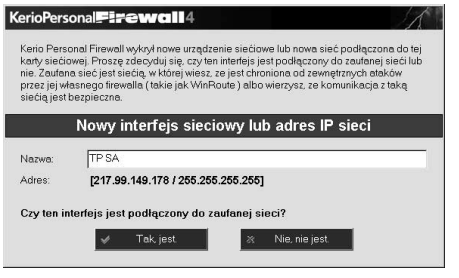
✔ Na większość z tych pytań należy odpowiedzieć twierdząco (przycisk *Dopuść*), ale póki nie zyskamy pewności co do bezpieczeństwa, nie należy tworzyć reguł, tzn. nie należy zaznaczać pola *Utwórz regułę dla tego połączenia i więcej się nie pytaj*.

Rysunek 3.7. *Aby aplikacja lub serwis mogły połączyć się ze zdalnym komputerem, należy kliknąć Dopuść*

Aby ustalić status ochrony połączeń przez modem:

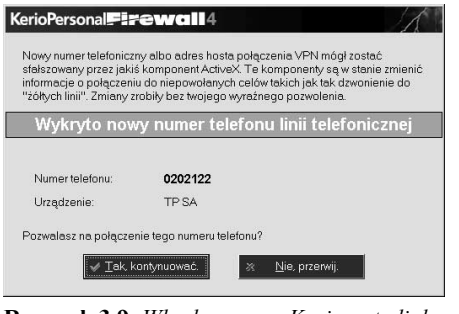
1. Pierwsze pytanie Kerio pojawia się już po połączeniu z nowym numerem, przy próbie nawiązania kontaktu ze zdalnym serwerem (rysunek 3.8). Analogicznie jak w przypadku karty sieciowej, pierwsze pytanie będzie dotyczyć uznania wybranej konfiguracji[5] (interfejsu sieciowego) za godną zaufania.

- ▲ Jeżeli, jak w tym przypadku, połączenie oznacza dostęp do i z całego internetu, należy bezwzględnie kliknąć przycisk *Nie, nie jest*.
- ▲ Natomiast jeżeli łączymy się z numerem dostępowym naszego zakładu pracy uzyskując w ten sposób np. możliwość zalogowania na dobrze zabezpieczonym serwerze — możemy kliknąć *Tak, jest*.



Rysunek 3.8. *Pytanie przy łączeniu się za pomocą modemu*

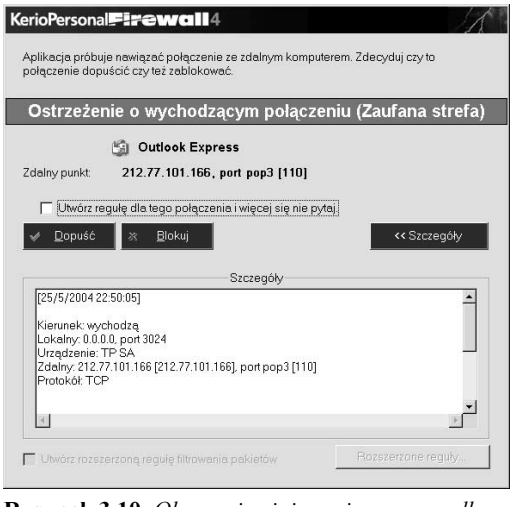
2. W przypadku modemu Kerio upewnia się również, że numer, na który chcieliśmy zadzwonić, jest rzeczywiście tym, który został wybrany (rysunek 3.9).



Rysunek 3.9. *Wbudowany w Kerio antydialer*

✔ Sprawdzanie numeru, z którym łączymy się za pomocą modemu, zapobiega sytuacjom, w których jakiś program podmienia wybrany przez nas numer dostępowy znacznie droższym numerem 0-700 lub numerem dostępowym w Korei. Jest to zatem wbudowany w Kerio antydialer.

[5] W prezentowanym na rysunku przykładzie chodzi o konfigurację połączenia z numerem dostępowym TP SA.



Rysunek 3.10. *Okno pojawiające się w przypadku próby połączenia Outlook Express z siecią przy korzystaniu z zaufanego połączenia oraz przy połączeniu zaliczonym do mniej pewnej kategorii Internet*

Ostrzeżenia

Kerio powiadamia o wielu czynnościach wykonywanych przez komputer (tabela 3.3) żądając od użytkownika decyzji w sprawie dopuszczenia lub zablokowania działania. Póki nie stworzymy reguł dotyczących najczęstszych wydarzeń, ekran ostrzeżenia będzie pojawiał się bardzo często.

Ostrzeżenie o wychodzącym połączeniu

Po ustaleniu połączenia możemy uruchomić np. program pocztowy lub przeglądarkę WWW. W momencie próby połączenia tych aplikacji z siecią (dokładniej ze zdalnymi komputerami dostępnymi w sieci) pojawi się ostrzeżenie o wychodzącym połączeniu (rysunek 3.10, porównaj rysunek 3.7).

Informacja widoczna w oknie ostrzeżenia to nazwa programu, który próbuje łączyć się ze zdalnym komputerem, adres IP i ewentualna nazwa tego komputera, port, przez który nawiązywane jest połączenie, oraz informacje szczegółowe, m.in. wykorzystywany protokół. Zazwyczaj są to informacje wystarczające, żeby podjąć decyzję o dopuszczeniu lub zablokowaniu połączenia tej aplikacji z siecią. W przypadku programu pocztowego, jakim jest Outlook Express, lub przeglądarki WWW, jest raczej jasne, że do połączenia powinniśmy dopuścić. Jednak jeżeli z siecią niespodziewanie łączy się arkusz kalkulacyjny, to połączenie można zablokować.

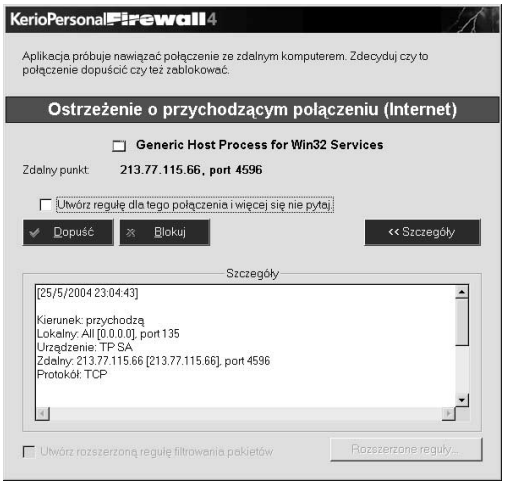
Tabela 3.3. *Barwy używane przez Kerio w oknie ostrzeżeń*

Kolor	Czego dotyczy	Rodzaj decyzji
granatowy	ochrona sieci: interfejs sieciowy lub adres IP sieci	zaufany/internet
różowy	ochrona sieci: nowy numer przy połączeniu modemowym (antydialer)	kontynuacja/przerwanie połączenia
zielony	ochrona sieci: połączenie wychodzące	dopuść/blokuj
czerwony	ochrona sieci: połączenie przychodzące	dopuść/blokuj
pomarańczowy	ochrona systemu: uruchomiona aplikacja	dopuść/blokuj
bordowy	ochrona systemu: aplikacja uruchamia inną aplikację	dopuść/blokuj
zgniłozielony	ochrona systemu: plik (*.exe*) aplikacji jest modyfikowany (ochrona przeciwwirusowa)	dopuść/blokuj

Ostrzeżenie o przychodzącym połączeniu

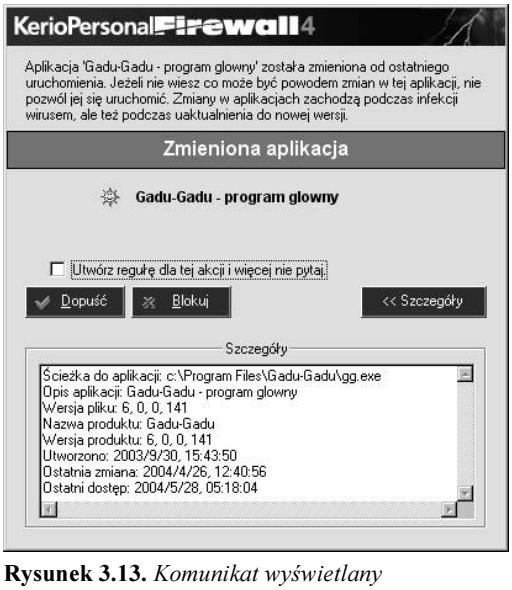
Wybranie opcji, w której nie uznajemy za godną zaufania sieci, z którą się połączyliśmy, czy to przy połączeniu modemowym, ISDN czy stałym łączu, nie oznacza wcale zablokowania połączenia. Jednak w takiej sytuacji większość prób ustalenia wychodzących i przychodzących połączeń zakończy się pytaniem o zgodę (zobacz informacje w podrozdziale o modyfikowaniu reguł dotyczących połączeń aplikacji z siecią). Np. domyślne ustawienia dla usługi Generic Host Process for Win32 Services są takie, że w połączeniu zaufanym automatycznie dozwolone są wszelkie przychodzące i wychodzące połączenia. Natomiast przy połączeniu należącym do kategorii Internet domyślnie akceptowane były jedynie połączenia wychodzące. Zatem przy próbie nawiązania połączenia przychodzącego, tzn. takiego, w którym informacja jest przesyłana do aplikacji uruchomionej na naszym komputerze, pojawi się pytanie pokazane na rysunku 3.11.

Połączenie przychodzące jest potencjalnie niebezpieczniejsze — to właśnie w ten sposób mogą odbywać się ataki na komputer (zobacz informacje w rozdziale 1.).



Rysunek 3.11. *Ostrzeżenie o połączeniu przychodzącym*

Rysunek 3.12. *Okno ostrzeżenia o uruchamianiu aplikacji przez aplikację*



Rysunek 3.13. *Komunikat wyświetlany podczas modyfikowania pliku exe*

Ostrzeżenie o uruchamianiu aplikacji z innych aplikacji

Już podczas startu systemu, gdy uruchamiane są pierwsze aplikacje, niezależnie od tego, czy jesteśmy połączeni z siecią, może dojść do sytuacji, w których jedna z nich próbuje uruchomić inną. Sytuacja taka jest przez Kerio traktowana jako potencjalnie niebezpieczna i dlatego pojawi się ostrzeżenie (rysunek 3.12).

Nie sposób podać ogólnego zalecenia w przypadku tego typu ostrzeżenia. Z jednej strony uruchamianie aplikacji przez inne aplikacje jest typową praktyką programów zawierających moduły w osobnych plikach *exe* (np. moduł update'u w Gadu-Gadu), w ten sposób mogą być uruchamiane niektóre sterowniki (np. sterownik karty graficznej SoundBlaster obejmuje plik *DevLdr32.exe*, który jest uruchamiany przy każdej próbie odtworzenia pliku dźwiękowego przez aplikacje). Jednym słowem, to, czy dopuścić, czy też zablokować uruchomienie aplikacji przez inną aplikację wymaga wiedzy i doświadczenia w używaniu systemu Windows i zainstalowanych na komputerze programów.

Ostrzeżenie o modyfikacji pliku aplikacji

To ostrzeżenie pojawia się zazwyczaj w trzech sytuacjach: po pierwsze, gdy plik *exe* jest modyfikowany przez rozprzestrzeniający się wirus, to właśnie do ochrony przed tą sytuacją jest pomyślane, po drugie — podczas instalacji nowszej wersji aplikacji i po trzecie — wówczas, gdy w środowisku programistycznym kompilujemy projekt do postaci *exe* i uruchamiamy go. Ponieważ żaden z autorów nie był szczególnie chętny, aby świadomie zainfekować komputer w celu uzyskania odpowiedniego zrzutu komunikatu, na rysunku 3.13 prezentujemy ostrzeżenie związane z instalowaniem nowszej wersji Gadu-Gadu.