

Outpost Firewall Pro

Outpost Firewall Pro firmy Agnitum jest osobistym systemem zaporowym zabezpieczającym komputer przed zagrożeniami w czasie połączenia z siecią lokalną lub Internetem. Doskonała i dobrze już znana na polskim rynku technologia Agnitum uzupełniona została o moduł chroniący przed programami spyware. Outpost jest doskonałym rozwiązaniem zarówno dla pojedynczych użytkowników zabezpieczających swoje prywatne komputery, jak i dla administratorów poszukujących dodatkowego zabezpieczenia stacji roboczych w sieci.

Dlaczego personal firewall jest potrzebny

Wraz ze wzrostem dostępności i jakości łącz internetowych pojawia się coraz więcej zagrożeń, przed którymi użytkownik powinien skutecznie się zabezpieczyć. Atak lub zainstalowanie oprogramowania szpiegowskiego na komputerze nieświadomego użytkownika może być przykładem złośliwości hakera. Jednak równie często celem ataku może być zniszczenie lub kradzież danych takich jak bazy klientów, umowy, dane księgowe czy też nasze hasło do prywatnego konta bankowego. Zabezpieczenie przed tego typu atakami i ryzykiem utraty danych zapewnia Outpost Firewall Pro firmy Agnitum.

Sprawdzona technologia

Outpost Firewall kontroluje cały ruch przychodzący i wychodzący, blokując nieautoryzowanym programom możliwość łączenia się z Internetem i zamykając nieużywane porty. Przy próbie nawiązania połączenia po raz pierwszy, użytkownik jest informowany, jaki program próbuje nawiązać połączenie. Użytkownik ma możliwość podjęcia wtedy decyzji, czy połączenie ma zostać nawiązane, czy też zablokowane. Użytkownik może również zdecydować, czy chce, aby takie połączenie zostało nawiązane jednorazowo (na próbę), czy też ma być nawiązywane lub blokowane za każdym razem. Początkujący użytkownik może skorzystać z usługi ImproveNet, w ramach której Outpost samodzielnie decyduje, czy należy zezwolić na połączenie, na podstawie informacji zwrotnych zbieranych od innych użytkowników Outpost Firewalla. Program oferuje możliwość pracy w trybie ukrytym (stealth mode) dzięki czemu komputer jest niewidoczny dla pozostałych użytkowników Internetu. Filtrowanie ARP (Address Resolution Protocol) chroni przed podszyciem się intruza pod inne komputery w sieci lokalnej, zapewniając także ochronę przed nieautoryzowanymi próbami połączeń w sieciach Wi-Fi.

Dla początkujących i zaawansowanych

Outpost Firewall oferuje specjalne ułatwienia początkującym użytkownikom, zapewniając jednak możliwość zaawansowanej konfiguracji, której zwykle wymagają doświadczeni administratorzy. Dzięki usłudze ImproveNet, reguły firewalla mogą być pobierane i stosowane automatycznie. Początkujący użytkownik nie musi się już martwić, jak poprawnie odpowiedzieć na nieoczekiwane pytanie o zezwolenie na połączenie. Baza reguł tworzona jest na podstawie informacji zbieranych od użytkowników programu Outpost, który wyrazili na to zgodę i przystąpili do społeczności ImproveNet. Reguły weryfikowane są na bieżąco przez ekspertów bezpieczeństwa Agnitum, a następnie udostępniane użytkownikom Outpost Firewalla. Aktualizacje dystrybuowane są codziennie, dzięki czemu konieczność ręcznego ustawiania reguł jest zredukowana do minimum. Zaawansowani użytkownicy mają możliwość ręcznego konfigurowania ustawień, samodzielnego definiowania reguł dla poszczególnych aplikacji i protokołów oraz korzystania ze szczegółowych logów ruchu sieciowego.



Autoochrona

Złośliwe programy często zamiast pokonywać zabezpieczenia po prostu je wyłączają. Coraz więcej wirusów, trojanów oraz spyware zamiast bezpośrednio atakować będzie próbowało obejść istniejące zabezpieczenia. Funkcja autoochrony w Outpostcie doskonale zabezpiecza przed takimi działaniami. Skuteczność autoochrony została również wykazana w testach przeprowadzonych przez Guillaume Kaddouch, niezależnego eksperta w dziedzinie bezpieczeństwa IT. W przeprowadzanych przez niego testach Outpost jako jedyny z pośród 13 testowanych firewallei odparł pomyślnie wszystkie próby ataków.

Moduł Antyspyware

Połączenie technologii personal firewall z modułem antyspyware gwarantuje użytkownikowi jeszcze lepsze zabezpieczenie komputera. Ochronę przed programami szpiegowskimi zapewnia skaner rezydentny oraz skaner na żądanie. Wykryte programy szpiegowskie są automatycznie blokowane i usuwane, zapewniając bezpieczne surfowanie w sieci. Zintegrowanie modułu antyspyware z technologią personal firewalla pozwala zablokować atak programów szpiegowskich już na firewallu, zanim dostaną się one na nasz komputer.

Dodatkowe zabezpieczenie dla bankowości online

Outpost Firewall oferuje dodatkowe zabezpieczenie przed tzw. „kradzieżą tożsamości”, czyli kradzieżą poufnych danych identyfikujących użytkownika takich jak hasła dostępu do poczty, kont bankowych, serwisów aukcyjnych czy numery kart kredytowych. Przeznaczona do tego opcja „Ochrona prywatnych informacji” po odpowiednim skonfigurowaniu blokuje wysłanie poufnych danych przez dowolny program. Zamiast naszych poufnych danych, usiłujące je zdobyć programy otrzymują nieczytelny tekst w formie gwiazdek. Dla wygodnego korzystania z bankowości elektronicznej, możemy zdefiniować listę zaufanych witryn, które nadal będą mogły otrzymywać poufne informacje.

Funkcja Anti-leak dodatkowo zabezpiecza przed nieautoryzowanym wyciekiem poufnych danych, kontrolując czynności na stacji roboczej oraz blokując wszystkie techniki wykradania poufnych danych, które bardzo często są wykorzystywane przez oprogramowanie szpiegowskie.

Wtyczki rozszerzające możliwości

Poza funkcjonalnością firewalla i antyspyware Outpost oferuje użytkownikowi szereg innych wtyczek, które podnoszą poziom bezpieczeństwa i usprawniają korzystanie z Internetu.

- **Blokowanie reklam** pozwala blokować irytujące reklamy w Internecie zarówno według ciągu znaków jak również według rozmiaru obrazka reklamowego
- **Filtrowanie aktywnej zawartości** skutecznie blokuje niebezpieczną zawartość stron internetowych taką jak skrypty Java czy Active X
- **Filtrowanie załączników poczty elektronicznej** wspomaga działanie programu antywirusowego dodatkowo ostrzegając użytkownika przed otwarciem potencjalnie niebezpiecznego załącznika poczty
- **Filtrowanie zawartości** blokuje dostęp do stron internetowych na podstawie adresu strony internetowej (www.sex.pl) lub poszczególnych słów w treści strony
- **Pamięć DNS** przechowuje w pamięci adresy ostatnio otwieranych stron WWW wraz z odpowiadającymi im numerami IP, co przyspiesza surfowanie w Internecie
- **Wykrywanie ataków** obejmuje system wizualnych komunikatów o atakach, które są również rejestrowane w Dziennikach zdarzeń, a także umożliwia blokowanie adresu IP intruza zapobiegając atakom z danego adresu IP w przyszłości



Wymagania systemowe:

System operacyjny Windows 98/ME/2000/2003/XP, Pentium 450 lub szybszy, 50MB wolnego miejsca na dysku, 64MB RAM (Windows 98/ME), 128 RAM (Windows 2000/XP/2003).