PORADNIK ZABEZPIECZANIE SIECI BEZPRZEWODOWYCH

PRZYDATNE WSKAZÓWKI JAK CHRONIĆ SIEĆ DOMOWĄ PRZED INTRUZAMI

BOGDAN BOTEZATU
ZESPÓŁ ANALIZ E-ZAGROŻEŃ I KOMUNIKACJI

OPRACOWANIE WERSJI POLSKIEJ:
ANDRZEJ WITBROT, MARKEN SYSTEMY ANTYWIRUSOWE

bitdefender

Spis treści

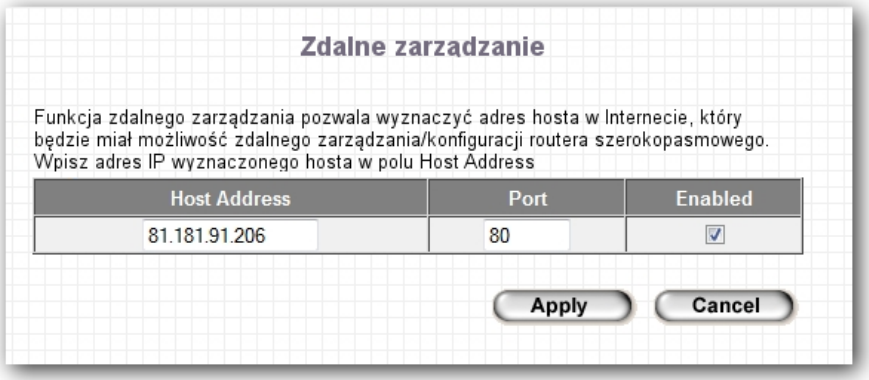
W czym sieć bezprzewodowa jest lepsza od kablowej?

Komunikacja radiowa to najlepszy sposób na pokrycie siecią dużych obszarów bez inwestowania w okablowanie, na dokonanie zmian strukturalnych w obrębie budynków lub eliminację zakłóceń. Jednakże jest ona ciągle poddawana wielu wyzwaniom z dziedziny bezpieczeństwa, ponieważ informacje swobodnie przenoszone w postaci fal radiowych, chociaż często zaszyfrowane, są publicznie dostępne dla każdego w obrębie zasięgu.

Ten poradnik nauczy cię najlepszych praktyk korzystania z sieci bezprzewodowych oraz pomoże zabezpieczyć domowy router lub access point przed włamaniem się do twojej sieci przez inne osoby.

Niektóre z oczywistych korzyści implementacji bezprzewodowych sieci 802.11 b / g / n w domu lub małym biurze to niski koszt zakupu osprzętu wifi (access point lub router oraz bezprzewodowe karty sieciowe), fakt, że ich struktura jest wyjątkowo dyskretna (nie ma konieczności wiercenia otworów i kładzenia kabli), a także swoboda poruszania się. Obecność kart bezprzewodowych w laptopach, netbookach i części telefonów komórkowych także przyczyniła się w ostatnim czasie do większej popularyzacji komunikacji bezprzewodowej.

Pomimo tego, że informacja między klientem i punktem dostępu lub routerem przepływa swobodnie, a więc jest dostępna dla wszystkich innych klientów w obrębie zasięgu, dobrze skonfigurowana sieć bezprzewodowa może być całkowicie bezpieczna.



Zdalne zarządzanie pozwala zdefiniować adresy IP, z których można zobaczyć interfejs administracyjny routera

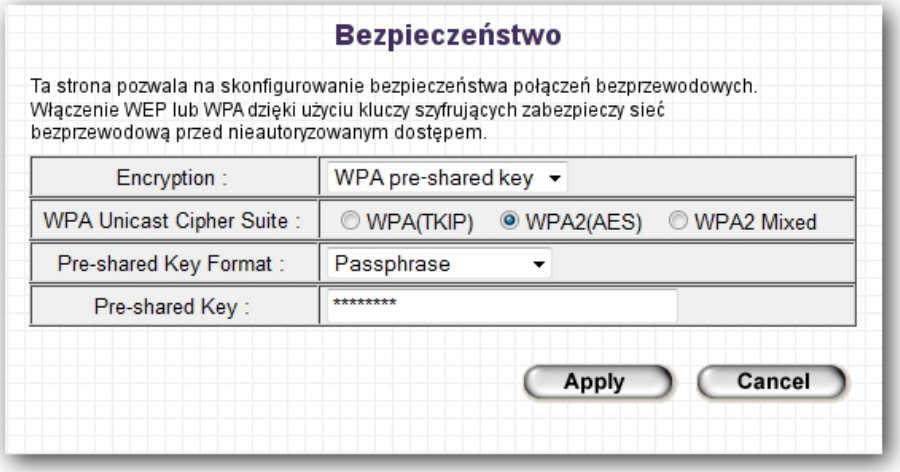
Co konkretnie wymaga szczególnej ochrony?

Z reguły, routery i access pointy opuszczają fabrykę z minimalnymi lub wręcz żadnymi ustawieniami ochrony. Większość routerów i access pointów posiada **panel administracyjny dostępny z poziomu www**, do którego podłącza się wpisując adres IP urządzenia w przeglądarce internetowej. Po udanym podłączeniu urządzenie prosi o podanie predefiniowanej nazwy użytkownika i hasła, które są typowe dla każdego modelu i publicznie dostępne w Internecie.

Dostęp administracyjny i logowanie zdalne

Większość urządzeń bezprzewodowych może poprawnie funkcjonować właściwie zaraz po wyjęciu z pudełka dzięki wielu różnorodnym technologiom i funkcjom zaimplementowanym w celu ułatwienia ich instalacji nawet przez nie-technicznych konsumentów. Najczęściej napotykanym błędem, który popełniają użytkownicy, jest pozostawienie fabrycznej konfiguracji tylko dlatego, że po prostu działa. Tymczasem, absolutnie konieczną czynnością jest zmiana hasła dostępu natychmiast po podłączeniu i pierwszym uruchomieniu urządzenia.

Zabezpieczenie dostępu administracyjnego uniemożliwi niepowołanym osobom manipulowanie przy ustawieniach sieci i/lub niektóre akcje, takie jak usunięcie logów, by pozostać niezauważonym w czasie połączenia z cudzą siecią. W celu dalszej eliminacji możliwości wtargnięcia intruza do funkcji administracyjnych, właściciel urządzenia bezprzewodowego powinien zablokować także dostęp zdalny. Większość routerów i access pointów zezwala upoważnionym użytkownikom na zmianę ustawień – nawet jeśli nie znajdują się oni w tym samym budynku – przez proste wpisanie adresu IP urządzenia w swojej przeglądarce.



Protokół WPA2 oferuje znacznie lepszą ochronę niż przestarzały standard WEP

Funkcja ta jest bezcenna dla administratorów, którzy muszą rozwiązywać problemy z połączeniem późno w nocy, gdyż pozwala im na wygodne połączenie się z domu, ale jednocześnie odsłania router przed każdym, kto spróbuje dostać się na adres IP powiązany z publicznym interfejsem urządzenia.

Jeśli router nie umożliwia utworzenia listy zaufanych adresów[1] upoważnionych do zarządzania, wskazane jest zupełne wyłączenie zdalnego interfejsu administracyjnego.

Szyfrowanie transmisji bezprzewodowej

Pomijając zabezpieczenie urządzenia bezprzewodowego od strony administracyjnej, dużo uwagi należy poświęcić samemu połączeniu wifi. Wspomnieliśmy wcześniej, że w przeciwieństwie do połączenia kablowego, które przekazuje sygnał pomiędzy komputerem i routerem – domyślnie tworząc sieć zaufaną – sygnał bezprzewodowy rozchodzi się na dużym obszarze ograniczonym jedynie mocą nadajnika. Zależnie od wielkości obszaru pokrytego zasięgiem, dziesiątki komputerów mogą próbować połączyć się z twoją siecią bez autoryzacji, albo co gorsza, podsłuchiwać strumień przepływających, niezaszyfrowanych informacji.

Z tego powodu, właściciel routera obowiązkowo powinien utworzyć silną linię obrony sieci przez włączenie szyfrowania połączeń przy użyciu predefiniowanego klucza wstępnego (PSK). W celu obniżenia kosztów i uproszczenia instalacji, domowe urządzenia bezprzewodowe zazwyczaj wyposażone są w dwa wbudowane protokoły szyfrowania: WEP (Wired Equivalent Privacy) oraz WPA /WPA2 (Wi-Fi Protected Access).

---

[1] Niektóre routery zezwalają na dostęp do konsoli administracyjnej tylko jeśli adres IP klienta ma określoną wartość lub należy do określonego zakresu adresów IP. Inne żądania są automatycznie odrzucane.

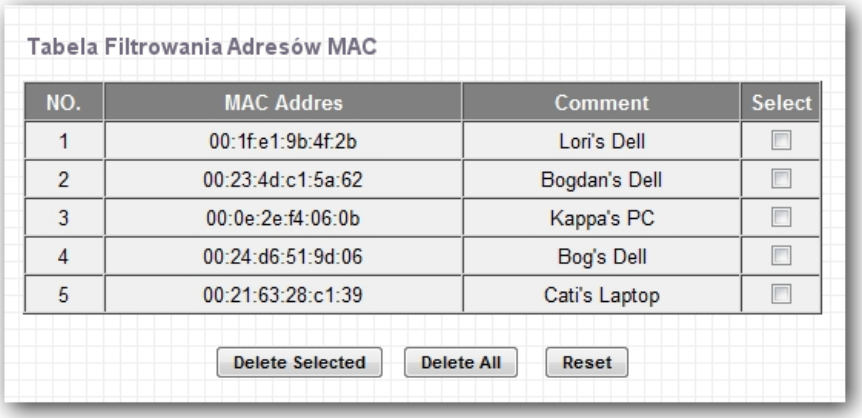


Tabela Filtrowania Adresów MAC

NO.	MAC Addres	Comment	Select
1	00:1f:e1:9b:4f:2b	Lori's Dell	☐
2	00:23:4d:c1:5a:62	Bogdan's Dell	☐
3	00:0e:2e:f4:06:0b	Kappa's PC	☐
4	00:24:d6:51:9d:06	Bog's Dell	☐
5	00:21:63:28:c1:39	Cati's Laptop	☐

Delete Selected | Delete All | Reset

Filtrowanie MAC daje pewność, że router zaakceptuje wyłącznie połączenia klientów, którzy znajdują się na liście zaufanych.

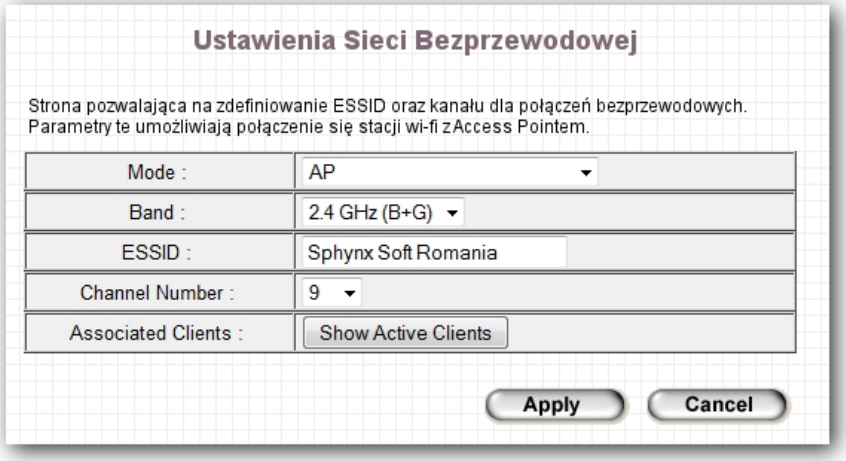
Oba protokoły opierają się na jednoczynnikowym uwierzytelnieniu przy pomocy kluczy wstępnych (pre-shared keys) działających jak hasła, jednak różnią się od siebie z punktu widzenia bezpieczeństwa. WEP funkcjonuje od 1997 roku, kiedy stał się częścią protokołu 802.11, ale uznawany jest za przestarzały ze względu na kilka poważnych wad czyniących go niezwykle łatwym do złamania. WPA i WPA2 zapewniają solidny poziom bezpieczeństwa nie wymagając przy tym pracochłonnej konfiguracji, co sprawia, że stanowią najlepszy wybór dla domowej sieci bezprzewodowej.

Zdarzają się przypadki, że użycie WPA nie jest możliwe – zazwyczaj wtedy, gdy infrastruktura sieci opiera się na starszym sprzęcie zakupionym przed wprowadzeniem tego standardu. Jeśli twoje urządzenie nie wspiera protokołu WPA, sprawdź na stronie producenta czy nie jest dostępna aktualizacja firmware'u dodająca taką funkcjonalność.

Nawet jeśli nowy firmware nie jest dostępny, lepiej wybrać szyfrowanie WEP niż pozostawić połączenie nieszyfrowane, chociaż należy wówczas mieć świadomość, że dane są nieosłonięte przed potencjalnym napastnikiem, więc mądrzej byłoby jednak wydać około 100 złotych i kupić nowy router bezprzewodowy, który wspiera protokoły WPA / WPA2.

Ustawienia reguł dostępu MAC (Media Access Control)

Kolejnym sposobem odfiltrowania intruzów jest zdefiniowanie reguł weryfikujących tożsamość komputera, który próbuje podłączyć się do sieci bezprzewodowej. Większość routerów i access pointów dla domu i małych firm umożliwia kontrolę w oparciu o filtrowanie MAC, co oznacza, że router zaakceptuje wyłącznie połączenia pochodzące od klientów znajdujących się na predefiniowanej liście, zidentyfikowanych na podstawie adresów MAC ich kart bezprzewodowych.



Rozgłaszanie SSID mówi użytkownikom, że w pobliżu znajduje się sieć bezprzewodowa. Napastnicy mogą wykorzystać to do swoich celów.

Niektóre karty sieciowe umożliwiają użytkownikom dowolną zmianę adresu MAC, co znaczy, że samo filtrowanie MAC nie jest wystarczającym rozwiązaniem do zabezpieczenia się przed intruzami. Jednakże, jako dodatkowy środek ochrony, wraz z silnym szyfrowaniem WPA, znacznie zwiększy bezpieczeństwo sieci bezprzewodowej.

Trzy wymienione wyżej kroki to najbardziej powszechne środki służące ochronie sieci i zapobieganiu podłączania się do niej nieupoważnionych osób (takich jak sąsiedzi albo włamywacze sieciowi). W następnej sekcji omówimy sposoby ukrycia sieci przed napastnikami, którzy chcieliby sforsować zastosowane zabezpieczenia.

Wyłączenie rozgłaszania SSID

Aby użytkownik mógł odróżnić jedną sieć bezprzewodową od drugiej, routery i access pointy automatycznie rozgłaszają swoją nazwę (określaną także jako ESSID / SSID lub Service Set ID). Chociaż jest to wygodne dla właściciela sieci, z metody tej korzystają również atakujący, ponieważ router przez cały czas “hałasuje” zwracając uwagę na swoją obecność. Wyłączenie rozgłaszania SSID uczyni router (wraz z wszystkimi połączonymi do niego klientami) niewidocznym dla każdego, kto nie orientuje się, że w pobliżu znajduje się aktywny nadajnik sieci bezprzewodowej.

Rozgłaszanie SSID mówi użytkownikom, że w pobliżu znajduje się sieć bezprzewodowa. Napastnicy mogą wykorzystać to do swoich celów.

Zmniejszenie mocy transmisji

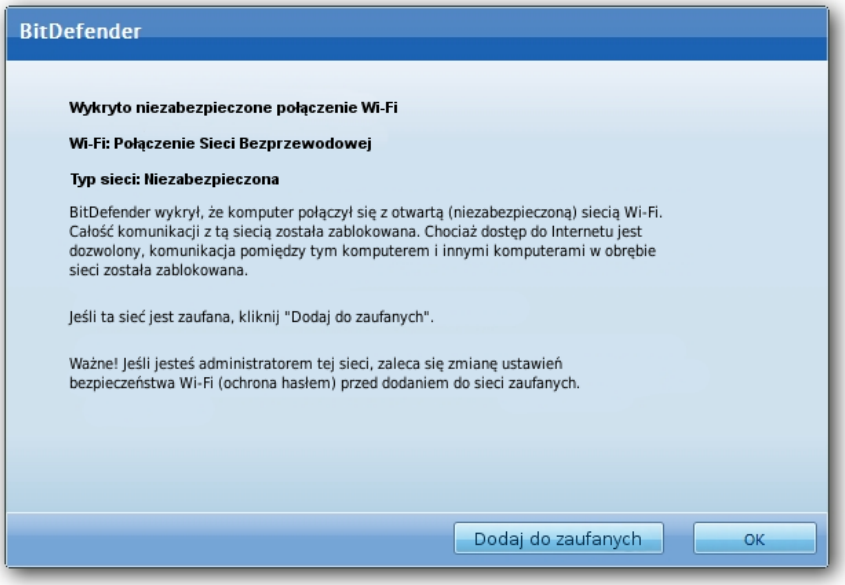
Jak każdy sprzęt radiowy, router / access point pokrywa zasięgiem obszar, którego wielkość jest wprost proporcjonalna do mocy wbudowanego nadajnika. Ustawienia fabryczne w zupełności wystarczają do objęcia zasięgiem całego mieszkania a nawet części przestrzeni publicznej wokół niego, jak klatka schodowa czy chodnik przed domem, co wiąże się z ryzykiem, że każda osoba wyposażona w netbook albo laptop może próbować włamać się do twojej sieci. Dzięki zmniejszeniu siły transmisji, sygnał routera nie będzie przedostawał się poza lokal uniemożliwiając podsłuchiwanie sieci.

Niektóre routery i access pointy z wyższej półki posiadają możliwość programowej redukcji siły sygnału karty WLAN. Nie istnieje jednak magiczna wartość oferująca najlepsze proporcje bezpieczeństwa i wydajności.

Podkręcając moc wyjściową WLAN miej na uwadze, że zwiększenie siły transmisji może zachęcić niechcianych gości do udziału w zabawie, natomiast zbytnie jej zmniejszenie spowoduje drastyczne obniżenie wydajności sieci w sensie jej przepustowości.

Siłę transmisji można kontrolować także w przypadku urządzeń, które nie posiadają takiej opcji wbudowanej w firmware. Proste zdjęcie anteny (albo jednej z anten, jeśli urządzenie posiada ich więcej) poskutkuje pogorszeniem jakości sygnału utrudniającym jego przechwycenie, ale będzie to wystarczające do zachowania wysokiej wydajności wewnątrz mieszkania.

Fizyczne umiejscowienie routera również ma wpływ na zasięg. W zasadzie nigdy nie powinno się umieszczać routera bezprzewodowego blisko okna wychodzącego na miejsca publiczne, ponieważ fale radiowe dużo łatwiej przedostają się przez szkło niż przez beton.



Zapora sieciowa BitDefendera automatycznie wykrywa niezabezpieczoną sieć i doradza użytkownikowi podjęcie odpowiednich kroków.

Ryzyka dotyczące uruchamiania oraz łączenia się z niezabezpieczoną siecią

Generalnie, niezabezpieczona sieć oznacza kłopoty. Pomijając kilka wyjątków, gdzie brak ochrony w rzeczywistości zwraca się przeciwko „napastnikowi", sieci bez zabezpieczeń stanowią poważne źródło utraty danych przez ich właścicieli.

Sieci domowe bazują na zaufaniu: nie posiadają drogich mechanizmów uwierzytelniania minimalizujących dostęp do takich czy innych zasobów. Przeciwnie, użytkownicy domowi skłaniają się do upubliczniania wszystkiego, aby mieć dostęp do informacji zgromadzonych na jednym komputerze z innych maszyn w gospodarstwie domowym.

Udziały sieciowe z uprawnieniami do odczytu i zapisu lub zawierające prywatne informacje (choćby dokumenty czy zdjęcia) to najczęściej spotykane słabe punkty sieci domowych. Nieupoważniony użytkownik, który podłączy się do niechronionej sieci, uzyskuje dostęp również do współdzielonych zasobów, co oznacza, że może skopiować zdjęcia rodzinne, dokumenty lub pliki multimedialne, takie jak gry i filmy. Jeśli te udziały dają także prawo do zapisu, intruz może skasować zawartość folderu albo pozostawić malware ukryty w czystych plikach i czekać na jego uruchomienie.

Podsłuchiwanie pakietów (sniffing) i przechwytywanie ruchu sieciowego to kolejne powody do niepokoju, jeśli chodzi o włamania do sieci. Z założenia, ruch sieciowy swobodnie przepływa pomiędzy komputerami. To komputer decyduje, który ruch przetworzyć, a który odrzucić, ponieważ określona informacja nie była przeznaczona dla niego. Fałszywy „członek sieci" może podsłuchiwać całość ruchu sieciowego używając specjalnych narzędzi i wyszukiwać treści rozmów z komunikatorów, szczegóły logowania, które nie zostały przesłane przez połączenie SSL, itd.

Sidejacking to także forma podsłuchiwania pakietów, ale dużo bardziej efektywna niż bezowocne czyhanie na przesyłane zwykłym tekstem loginy i hasła. Ten rodzaj ataku polega na przechwytywaniu ciasteczek, jakie wymieniane są między uwierzytelnionymi użytkownikami i poszczególnymi stronami www. Atak jest skuteczny nawet przeciwko serwisom webowym, które korzystają z SSL do szyfrowania nazwy użytkownika i hasła jeszcze przed ich przesłaniem do serwera. Kiedy ciasteczka wpadną w niewłaściwe ręce, mogą zostać wykorzystane do uwierzytelnienia w serwisie tak samo, jak autentyczny użytkownik, który nawet nie będzie wiedział, że jeszcze ktoś inny używa jego konta.

Niezabezpieczone sieci są idealne także do **różnych nielegalnych celów**. Zazwyczaj cyberprzestępcy kierują się do otwartych sieci, żeby zamawiać produkty wykorzystując kradzione karty kredytowe, włamywać się do prywatnych przestrzeni lub nielegalnie ściągać muzykę, filmy i oprogramowanie przez P2P, gdyż w ten sposób ukrywają swoją własną tożsamość za adresem IP niezabezpieczonej sieci. Jeśli policja postanowi ścigać przestępcę, w rzeczywistości sprawa zakończy się na oskarżeniu nieostrożnego właściciela otwartej sieci. Czasami cyberoszuści używają niezabezpieczonych sieci bezprzewodowych do rozsyłania masowego spamu w imieniu właściciela sieci, co w konsekwencji może prowadzić do rozpoczęcia śledztwa, a nawet do zerwania umowy na dostawę Internetu.

Łączenie się z niechronionymi sieciami jest równie niebezpieczne, ponieważ ruch przepływający między twoim komputerem a routerem lub access pointem, bez szyfrowania, bardzo łatwo może być podsłuchany przez osoby o złych intencjach podłączone do tej samej sieci. Możesz także niechcący **wyeksponować udziały sieciowe** skonfigurowane dla własnej sieci domowej lub nawet zostać zainfekowanym przez różnego rodzaju robaki pochodzące z innych systemów w sieci.

Wskazówki bezpieczeństwa przy łączeniu się z hotspotami

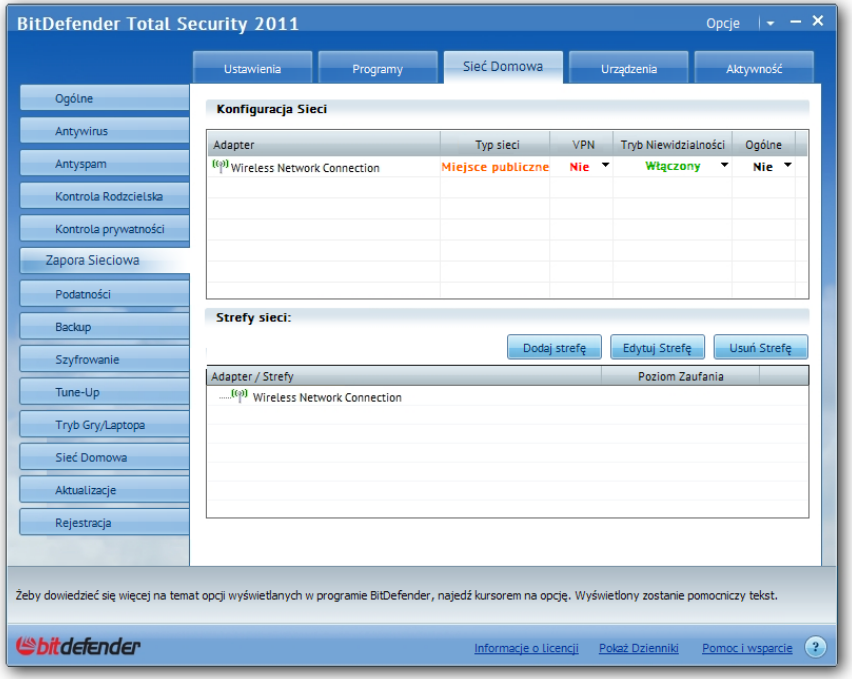
Hotspoty są całkiem powszechne w dzisiejszych czasach - tak powszechne, że prawie każdy park, kawiarnia lub lotnisko zapewniają bezpłatny dostęp do Internetu tym, którzy chcą być w nieustannym kontakcie ze swoją online'ową rzeczywistością.

Pomimo tego, podłączanie się do niezabezpieczonego hotspota może przynieść więcej problemów niż satysfakcji, jeśli nie zostanie zachowany minimalny poziom ostrożności. Poniżej przedstawiamy kilka wskazówek, dzięki którym pozostaniesz bezpieczny w czasie surfowania incognito.

Zawsze gdy korzystasz z niezabezpieczonej sieci pamiętaj, że nie wiesz kogo masz w swoim sąsiedztwie. Napastnik może próbować skanowania portów, aby wykryć **luki systemowe** i przez nie przeniknąć przez zabezpieczenia. W celu zminimalizowania ryzyka należy używać zapory sieciowej, która potrafi odfiltrować próby połączeń z sieci zewnętrznej.

Sieci publiczne nie są przystosowane do wymiany wrażliwych informacji. Są duże szanse, że jeden lub więcej użytkowników dzielących ten sam hotspot spróbuje grzebać w ruchu sieciowym pochodzącym z innych komputerów w poszukiwaniu wartościowych informacji, takich jak nazwy użytkowników i hasła, interesujące konwersacje prowadzone przez komunikatory IM, albo jeszcze lepiej, dane dostępu do kont bankowych. Wskazane jest przykładanie wielkiej uwagi do usług, z jakich korzystamy podczas połączenia przez hot spot, oraz **unikanie logowania jeśli tylko jest to możliwe**.

Współdzielone zasoby to kolejny krytyczny aspekt, który należy brać pod uwagę łącząc się z obcą siecią, ponieważ istnieje ryzyko niezamierzonego **ujawnienia prywatnych danych nieupoważnionym osobom**. Pamiętaj, by zawsze wyłączać udostępnianie przed połączeniem się z hotspotem.



BitDefender automatycznie ukrywa komputer przed innymi klientami w sieci jeśli jej profil ustawiony jest na „Miejsce publiczne”

Jak BitDefender może ci pomóc?

BitDefender wprowadził moduł zapory sieciowej w 2001 roku stając się tym samym pierwszym programem antywirusowym z wbudowanym firewallem. Seria produktów 2011 z rodziny BitDefender Internet Security i BitDefender Total Security posiada udoskonaloną zaporę, która jest w stanie sprostać wymogom bezpieczeństwa w środowisku niezabezpieczonych sieci bezprzewodowych.

W celu ułatwienia konfiguracji, firewall BitDefendera rozróżnia cztery predefiniowane typy sieci: Zaufana, Dom / Biuro, Publiczna oraz Niezaufana.

Co więcej, w czasie połączenia z siecią publiczną firewall automatycznie uruchamia **Tryb Niewidzialności**, który ukrywa komputer przed innymi systemami, dzięki czemu zmniejsza się szansa, że zostanie przejęty przez malware lub hakerów.

Nawet podczas korzystania z własnej sieci zapora może okazać się przydatna, gdyż posiada funkcję wyświetlania powiadomień za każdym razem, kiedy do sieci podłącza się inny komputer.

Jest to szczególnie pomocne do określenia czy system podłączający się do sieci należy faktycznie do legalnego użytkownika, czy też nastąpił udany atak hakerski.

bitdefender