**Jak zabezpieczyć swoją sieć Wi-Fi przed intruzami**

**W dzisiejszych czasach skonfigurowanie sieci bezprzewodowej jest niezwykle proste. Wystarczy kupić ruter WiFi i podłączyć go do modemu kablowego lub sieci DSL. Jednak zanim zaczniesz korzystać z bankowości elektronicznej, zakupów online i przeglądać strony internetowe, warto upewnić się, że Twoja sieć jest zabezpieczona przed intruzami.**

Być może uważasz, że sąsiad podłączający się do twojej sieci aby sprawdzić pocztę to nic szkodliwego. Tak naprawdę istnieją o wiele poważniejsze problemy niż to, że nieuprawiona osoba po podłączeniu zajmuje całą przepustowość łącza oglądając filmy w formacie HD. Taka osoba będąc wewnątrz twojej sieci może podsłuchiwać wszystkie dane, które wysyłasz, nakłonić cię do odwiedzenia złośliwej strony i włamać się do komputerów lub urządzeń podłączonych do WiFi. Pozwolić nieznajomemu na korzystanie z twojej sieci to tak, jakby mu pozwolić oglądać wszelkie przesyłane przez nią dane.

Jeżeli posiadasz własną sieć WiFi, to bardzo ważną rzeczą jest zabezpieczenie jej przed nieautoryzowanymi użytkownikami i urządzeniami za pomocą odpowiedniej konfiguracji rutera. Chociaż niektóre metody konfiguracji w oprogramowaniu mogą się różnić w zależności od dostawcy i modelu sprzętu, to ustawienia te są dosyć uniwersalne i znalezienie ich nie powinno stanowić problemu.

Poniżej znajduje się kilka wskazówek, które pomogą poprawić bezpieczeństwo sieci bezprzewodowej.

**1. Szyfruj za pomocą WPA2**

Po skonfigurowaniu sieci bezprzewodowej pojawia się opcja włączenia szyfrowania. W przypadku użytkowników sieci domowej, szyfrowanie należy włączyć (w przeciwieństwie do tzw. otwartej sieci), a jako metodę szyfrowania wybrać WPA2. Protokół WEP nie jest bezpieczny, a niektóre z zaawansowanych metod są na ogół poza zasięgiem większości użytkowników domowych. Nawet jeżeli szyfrowanie za pomocą WPA2 nie zostało włączone przy pierwszej konfiguracji, oprogramowanie do zarządzania ruterem powinno pozwolić na włączenie tej opcji w każdej chwili.

Po wybraniu WPA2, powinna pojawić się prośba o utworzenie klucza dla użytkowników chcących podłączyć się do sieci. Ważną sprawą – chociaż nie najważniejszą – jest zadbanie o to, by hasło było unikalne i złożone tak, by osoby spoza sieci nie mogły go złamać atakiem brute-force lub po prostu je zgadując w celu uzyskania dostępu do sieci. Hasło powinno być dosyć długie oraz zawierać kombinację liter i cyfr. W przypadku słabego hasła, atakujący i tak będzie w stanie włamać się do sieci.

Nie włączaj WPS (WiFi Protected Setup). Mechanizm ten nie zawsze działa w spójny sposób, a dziewięciocyfrowy kod PIN jest podatny na próby zgadywania. Gdy atakujący zdobędzie kod PIN do WPS, nie ma nic, co by go powstrzymało przed dostępem do wszystkich współdzielonych zasobów znajdujących się w sieci bezprzewodowej.

**2. Zmień standardowe hasła**

Wiele z ruterów jest dostarczanych z domyślnym hasłem do oprogramowania udostępniającego panel administracyjny. Może to być np. „admin”, lub nawet brak hasła. Często zdarza się, że hasło jest zapisane gdzieś w dokumentacji i udostępniane online. Użytkownicy podczas konfiguracji sieci powinni natychmiast zmienić hasło do panelu administracyjnego, aby zabezpieczyć się przed nieautoryzowanym dostępem do zmiany konfiguracji rutera. Włamywacz po dostaniu się do panelu administracyjnego posiada pełną kontrolę nad ruterem – właściciel sprzętu ma wtedy poważny problem.

Poza zmianą hasła, warto sprawdzić, czy ruter ma prekonfigurowane identyfikatory SSID. SSID to nazwy sieci bezprzewodowych ustawionych dla danego rutera. Należy zmienić hasła dla domyślnych SSID nawet w przypadku, gdy nie korzystamy z tych sieci. Na wszelki wypadek.

**3. Wyczyść listę SSID**

Skoro mowa o SSID – dostawcy często korzystają z bardzo ogólnych identyfikatorów, takich jak “linksys” lub „netgear-wireless”. Należy je zmienić z domyślnych na coś bardziej unikalnego. Atakujący często wykonują ataki man-in-the-middle wykorzystując najczęściej używane SSID ustawione na ich złośliwych ruterach, co sprawia, że urządzenia łączą się do sieci hakera. Posiadanie unikalnego identyfikatora SSID i hasła sprawia, że potencjalnemu włamywaczowi jest trudniej się włamać.

Najlepiej jest po prostu usunąć wszystkie identyfikatory SSID, z których się nie korzysta (znajdują się najczęściej w zakładce „wireless”). Po co zwiększać potencjalną przestrzeń możliwość ataku? Po wyczyszczeniu listy, warto ukryć nazwę. Niektórzy z dostawców nazywają to „cloaking” . Założenie jest takie, by nie rozpowszechniać nazwy sieci do wszystkich urządzeń. Do sieci można się podłączyć tylko poprzez ręczne wpisanie nazwy SSID. Osoby niepowołane nie będą nawet wiedziały, że w okolicy znajduje się jakaś sieć WiFi.

**4. Sprawdzaj, kto jest podłączony do sieci**

Panel administracyjny na ogół posiada sekcję o nazwie “Device List” („Lista urządzeń”), na której wyświetlane są identyfikatory wszystkich urządzeń podłączonych do bezprzewodowej sieci. Dobrym zwyczajem jest okresowe przeglądanie tej listy w celu upewnienia się, że wszystkie urządzenia są nam znane. Aby uniemożliwić podłączanie się nieznanych urządzeń, można zastosować Mac Address Filtering (filtrację adresów MAC). Wymaga to poznania i wpisania adresów sprzętowych (MAC Address) urządzeń do panelu administracyjnego. Być może jest to nieco uciążliwe i czasochłonne, ale za to gwarantuje, że nikt nie będzie mógł niepostrzeżenie dostać się do sieci.

Rutery posiadają też pewne zaawansowane opcje, takie jak „guest networking” („dostęp dla gości”), który należy wyłączyć, czy też firewall, który warto uruchomić. Jeżeli nie korzystasz z żadnego oprogramowania typu firewall, włączenie tej funkcji na ruterze jest koniecznością, jednak dobrym pomysłem jest posiadanie równolegle tych dwóch zabezpieczeń. Dodatkowo warto aktualizować oprogramowanie rutera przy każdej możliwej okazji – w ten sposób można cieszyć się całkiem nieźle zabezpieczoną siecią bezprzewodową. Z pewnością warto poświęcić nieco czasu na poprawną konfigurację zamkniętej sieci. Pozwoli to uniknąć wielu problemów w przyszłości.

O Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), światowy lider w dziedzinie bezpieczeństwa Internetu, dostarcza klientom bezkompromisową ochronę przeciwko zagrożeniom każdego rodzaju, zmniejsza złożoność systemów bezpieczeństwa i obniża całkowity koszt użytkowania. Firma Check Point była pionierem na rynku wprowadzając swój produkt FireWall-1 wykorzystujący opatentowaną technologię stanowej inspekcji pakietów. Obecnie Check Point wciąż tworzy innowacyjne technologie oparte o architekturę Software Blade Architecture, dzięki której klienci otrzymują elastyczne i proste rozwiązania, z możliwością pełnej konfiguracji w celu najlepszego dopasowania do potrzeb przedsiębiorstwa. Check Point jest jedynym dostawcą, który wykracza poza technologię i definiuje bezpieczeństwo jako proces biznesowy. 3D Security firmy Check Point w unikalny sposób łączy politykę bezpieczeństwa, zaangażowanie ludzi i wsparcie technologiczne w celu jeszcze lepszej ochrony danych i umożliwienia przedsiębiorstwom zaprojektowania dokładnego planu bezpieczeństwa odpowiadającego wszelkim wymogom. Klienci firmy to dziesiątki tysięcy przedsiębiorstw każdego rodzaju, włączając w to wszystkie firmy z list Fortune 100 i Global 100. Wielokrotnie nagradzane rozwiązanie Zone Alarm firmy Check Point chroni komputery milionów konsumentów przed atakami hakerów, oprogramowaniem szpiegującym i kradzieżą tożsamości w sieci.

W Polsce dystrybutorami produktów Check Point są firmy Clico Sp. z o.o. (www.clico.pl), RRC Poland Sp. z o.o. (www.rrc.pl) oraz Computerlinks Sp. z o.o. (www.computerlinks.pl).

©2014 Check Point Software Technologies Ltd. Wszelkie prawa zastrzeżone