Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu

- **Zarządzanie siecią WiFi**
- **Nazwa Twojej sieci**
- **Szyfrowanie I uwierzytelnianie**
- **OpenDNS**

Zabezpieczanie domowej sieci WiFi

REDAKTOR GOŚCINNY

Redaktorem gościnnym tego wydania biuletynu OUCH! jest Raul Siles (www.raulsiles.com). Raul jest założycielem firmy Taddong w której jest starszym analitykiem bezpieczeństwa teleinformatycznego. Ponadto jest autorem kilku szkoleń w ramach instytutu SANS. O jego pasji – bezpieczeństwie IT, pisze na swoim blogu (blog.taddong.com) oraz Twitterze (@taddong).

WSTĘP

Sieci bezprzewodowe (fachowo nazywane sieciami z grupy standardów 802.11) pozwalają na łatwe uzyskanie dostępu do Internetu z urządzeń takich jak smartfony, konsole do gier, tablety, laptopy itp. Uruchomienie takiej sieci stało się na tyle prostym zadaniem, że większość z nas ma zazwyczaj jakąś działającą w swoim domu (czasami nawet o tym nie wiedząc!). Niestety, często nasze domowe sieci WiFi nie są wystarczają dobrze zabezpieczone. Pozwala to nieautoryzowanym osobom podłączać się do naszej sieci, podsłuchiwać przesyłane dane oraz wykorzystywać nasze połączenie internetowe do własnych, często nie do końca legalnych celów. Upewnij się, że Twoja sieć bezprzewodowa jest bezpieczna. W kilku prostych krokach prezentujemy podstawowe zasady jakimi należy się kierować, aby poprawić bezpieczeństwo domowej sieci WiFi.

ZARZĄDZANIE SIECIĄ WIFI

Sieć bezprzewodowa jest kontrolowana przez tzw. punkt dostępowy (z ang. WiFi access point). Jest to urządzenie, które obecnie najczęściej występuje jako element w tzw. bezprzewodowym routerze. To on jest odpowiedzialny za podłączanie urządzeń do sieci domowej i umożliwianie im dostępu do Internetu. Jednym z pierwszych kroków w celu poprawienia bezpieczeństwa sieci WiFi jest ograniczenie liczby osób oraz sposobów pozwalających uzyskać dostęp do panelu administracyjnego, który pozwala na zmianę konfiguracji sieci. W czasie pierwszej konfiguracji swojego routera WiFi pamiętaj o następujących czynnościach:

- Koniecznie zmień hasło oraz, o ile to możliwe, domyślną nazwę użytkownika uprawnionego do zarządzania siecią WiFi. Wiele z dostępnych urządzeń (zwłaszcza pochodzących od tego samego producenta) używa standardowych loginów i haseł, które są powszechnie znane i mogą pozwolić obcym na uzyskanie dostępu do Twojego urządzenia i zmianę jego ustawień.
- O ile to możliwe wyłącz dostęp bezprzewodowy do interfejsu zarządzania ustawieniami routera WiFi. Zalecamy, aby umożliwić **jedynie** dostęp poprzez interfejs przewodowy (Ethernet).

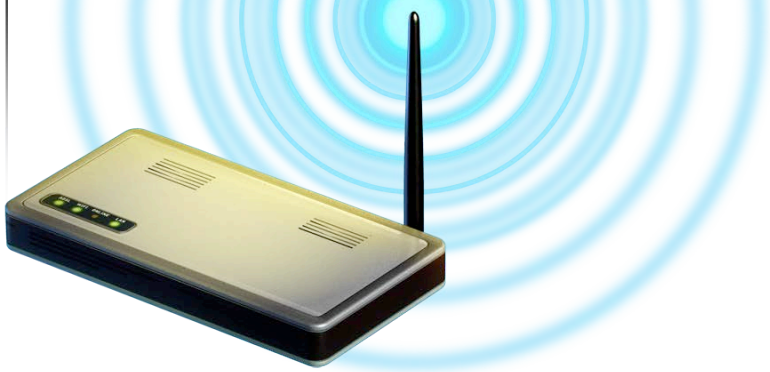
Zabezpieczanie domowej sieci WiFi

W przypadku, gdy dostęp bezprzewodowy w celu zarządzania ustawieniami jest niezbędny, należy uaktywnić bezpieczne (szyfrowane) połączenie HTTPS oraz wyłączyć standardową metodę dostępu (z reguły HTTP).

NAZWA SIECI BEZPRZEWODOWEJ

Nazwa sieci (inaczej określana jako SSID) jest niezbędna, aby możliwe było jej wyszukanie i podłączenie się. Zalecamy, aby zmienić ją na unikalną, która w łatwy sposób pozwoli zidentyfikować ją wśród innych. Pamiętaj jednak, aby przy tworzeniu nazwy sieci nie umieszczać w niej żadnych informacji osobistych, takich jak nazwisko, czy adres. Niektóre z poradników rekomendują, aby uaktywnić opcję, która ukrywa nazwę sieci. W naszej opinii jest to krok zbyteczny, gdyż obecnie dostępne narzędzia w łatwy sposób pozwalają na wykrycie takiej sieci. Zastosowanie się do kroków opisanych w dalszej części artykułu w znacznie lepszym stopniu przyczyni się do poprawy bezpieczeństwa niż proste ukrywanie nazw.

Bezpieczne domowe WiFi wymaga uwierzytelnienia, zapewnia szyfrowaną komunikację oraz ma świadomego administratora.



SZYFROWANIE I UWIERZYTELNIANIE

Kolejnym krokiem jest zapewnienie dostępu do sieci bezprzewodowej użytkownikom, których znasz i ufasz oraz, że dostęp będzie bezpieczny i szyfrowany. Bezprzewodowy router należy skonfigurować w taki sposób, aby inne nieuprawnione osoby, które będą odbierały sygnał radiowy naszej sieci, nie były w stanie się podłączyć ani podsłuchiwać ruchu. Na szczęście można te cele łatwo osiągnąć poprzez włączenie mechanizmów zabezpieczeń, które standardowo są dostępne w większości routerów WiFi. Mowa tu o obecnie jednym z najpowszechniej zalecanych – WPA2 (często określane jako WPA2 Personal). Uruchomienie go wiąże się z zabezpieczeniem dostępu do sieci hasłem, co dodatkowo zapewnia, że ruch między urządzeniami a routerem będzie szyfrowany. Upewnij się, że **nie używasz** starszych metod zabezpieczania dostępu do sieci takich jak WEP lub nie pozostawiasz sieci niezabezpieczonej (tzw. open network), co umożliwia każdemu na połączenie oraz podsłuch danych. WPA2 ma kilka opcji związanych z konfiguracją zabezpieczeń. Zalecamy, aby do szyfrowania ruchu wybrać opcję AES zamiast innych, takich jak TKIP oraz TKIP+AES.

Konfigurując zabezpieczenia dostępu do sieci WiFi pamiętaj, aby hasło, które będzie wykorzystywane do podłączania się, było inne niż hasło do panelu administracyjnego. Tworzenie silnego i jednocześnie łatwego do zapamiętania hasła zostało opisane w biuletynie OUCH! z maja 2011 roku. Długie hasło (ok. 20 znaków) oraz zawierające symbole (trudne do odgadnięcia) jest traktowane jako bezpieczne. W przypadku haseł dla sieci WiFi, długość nie powinna stanowić problemu w używaniu hasła, gdyż nie musimy go zapamiętywać i podawać za każdym razem, gdy chcemy się połączyć.

Zabezpieczanie domowej sieci WiFi

Urządzenia, które podłączamy do sieci zapamiętają je same. Jeżeli punkt dostępowy znajduje się w miejscu, do którego dostęp mają jedynie zaufane osoby, hasło może zostać nawet umieszczone bezpośrednio na nim (np. podklejone od spodu). Jednak, co jakiś czas (np. co 3-6 miesięcy) powinniśmy je zmieniać, szczególnie, gdy udostępnialiśmy swoją sieć gościom.

Dodatkowym zaleceniem jest wyłączenie tzw. metody dostępu WPS (WiFi Protected Setup). Standard WPS określa sposób w jaki urządzenia mają łatwo oraz bezpiecznie podłączać się do punktu dostępowego sieci bezprzewodowej. Niestety w momencie publikowania tego wydania biuletynu, WPS jest podatny na ataki, umożliwiając tym samym uzyskanie nieautoryzowanego dostępu do sieci WiFi.

OPENDNS

W momencie, gdy zabezpieczenia punktu dostępowego są już w pełni skonfigurowane, jednym z ostatnich kroków jest ustawienie serwerów DNS, które mają być używane w sieci domowej. DNS to usługa, która jest niezbędna do prawidłowego funkcjonowania sieci Internet. Zalecamy, aby ustawić serwery usługi OpenDNS jako podstawowe (primary DNS) w konfiguracji punktu dostępowego. OpenDNS to darmowa usługa, która zapewnia, że witryny do których się łączymy są bezpieczne (nie dokonują ataków na użytkownika). Dodatkowo OpenDNS umożliwia administratorowi domowej sieci łatwe zarządzanie listą stron, do których domownicy mają mieć zapewniony dostęp, oraz tych do których dostęp powinien zostać ograniczony (np. filtrowanie treści dostępnych dla najmłodszych użytkowników Internetu). Samouczki na stronie serwisu OpenDNS pokazują jak w łatwy sposób skonfigurować bezprzewodowy router, tak aby używał jego serwerów.

ŹRÓDŁA

W celu poprawy czytelności tekstu niektóre odnośniki w biuletynie zostały skrócone przy użyciu usługi TinyURL. Dla zachowania bezpieczeństwa OUCH! używa opcji podglądu TinyURL, która pozwala sprawdzić treść odnośnika przed wejściem na stronę o docelowym adresie.

OnGuard Online Wi-Fi Security:
http://preview.tinyurl.com/7sylsul

Encyklopedia bezpieczeństwa:
http://preview.tinyurl.com/bpc2h23

WPS Vulnerability: http://preview.tinyurl.com/cjs4l4w

OpenDNS: http://www.opendns.org

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

DOWIEDZ SIĘ WIĘCEJ

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS z zakresu bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

POLSKI PRZEKŁAD

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagownia na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet.
Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redakcja: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Polski przekład (NASK/CERT Polska): Tomasz Grudziecki and Paweł Jacewicz