Udostępnianie sieci bezprzewodowych

14 grudnia 2014

Otwarta, bezprzewodowa sieć to dziś norma. Kawiarnia, biblioteka, uczelnia, szkoła, przestrzeń publiczna w mieście… Coraz więcej instytucji udostępnia otwarte sieci, coraz więcej osób z nich korzysta. Każdy, kto tworzy taką sieć i nią administruje, ma bezpośredni wpływ na jej użytkowników – na to, w jaki sposób z niej korzystają, do czego mają dostęp oraz czy, używając jej, mogą chronić swoją prywatność. Jeśli odpowiadasz za działanie otwartej sieci, to tekst dla Ciebie. Znajdziesz w nim informacje, na co warto zwrócić uwagę, dzieląc się z innymi dostępem do Internetu.

W STRONĘ OTWARTEGO WI-FI

To, że sieć jest otwarta i dostępna dla szerokiego kręgu osób, nie powinno oznaczać, że jest niezabezpieczona. Podstawa to oczywiście hasło, które zapewnia nam szyfrowanie połączenia z publiczną siecią. Dość dobrze zabezpiecza ono przed podsłuchiwaniem użytkowników, które jest trywialnie proste w przypadku sieci bez hasła.

Jak wybrać dobre hasło? W przypadku otwartych sieci bezprzewodowych nie chodzi o stworzenie hasła „sekretnego”, takiego jak przy zabezpieczeniu osobistych danych lub kont do portali internetowych. Hasło będzie przecież rozpowszechniane. Nawet jego nieznajomość nie powstrzyma osób chcących uzyskać dostęp do naszej sieci za wszelką cenę – hasło może zostać złamane (nawet w ciągu minut – za pomocą dostępnych w Internecie narzędzi, również przez osoby z niewielką techniczną wiedzą) i puszczone w dalszy obieg bez wiedzy właściciela sieci. Dlatego lepiej postawić na hasło wygodne, które nie będzie trudne do zgadnięcia i zapamiętania.

Dobrym pomysłem jest umieszczenie hasła w nazwie sieci (np.

nazwanie sieci „NazwaSieci_haslo:NaszeHaslo” w przypadku hasła „NaszeHaslo”). Pozwoli to naszym gościom na łatwe i jednocześnie bezpieczne skorzystanie z dostępu do sieci. Niezależnie od tego, jakie będą nazwa i hasło do sieci, warto je umieścić w widocznym miejscu.

FILTROWANIE TREŚCI

Współczesne routery dają różne możliwości kontroli nad tym, do czego mają dostęp użytkownicy sieci. W przypadku sieci szkolnych i bibliotecznych często instaluje się specjalistyczne oprogramowanie (uruchamiane na oddzielnym komputerze), którego jedyną funkcją jest umożliwienie blokowania niepożądanych treści.

Jednym z takich mechanizmów kontroli jest automatyczne blokowanie dostępu do stron zawierających (w treści lub tylko w adresie) wybrane słowa lub frazy. Takie blokowanie na pierwszy rzut oka może wydawać się dobrym pomysłem, jednak to tylko pozory – technicznie odróżnienie treści pożądanej od zabronionej jest bardzo trudne i realizowane zwykle przy pomocy niedoskonałych algorytmów i list filtrujących. Efektem tego są częste pomyłki i blokowanie „na wyrost” treści nieszkodliwych (np. artykułów na Wikipedii dotyczących biologii czy stron organizacji pozarządowych) oraz pomijanie części treści, która powinna zostać zablokowana.

Ponadto, tego typu mechanizmy blokujące są zazwyczaj stosunkowo łatwe do obejścia – ich ominięcie jest możliwe przy pomocy dostępnych w Internecie narzędzi. Z pewnością nie powstrzymają one użytkownika zdeterminowanego je obejść, a z uwagi na nieprzewidywalne i wadliwe blokowanie są problemem dla wszystkich korzystających. Zachęcamy do porzucenia tego narzędzia i pozostawienia wyboru użytkownikom.

To, co wydaje się prostą radą w przypadku udostępniania sieci osobom dorosłym, komplikuje się w przypadku dzieci, które chcemy chronić przed treściami, które mogą być dla nich

krzywdzące. W tym kontekście szczególnym przypadkiem są sieci szkolne – Ustawa o systemie oświaty narzuca obowiązek zabezpieczenia uczniów przed treściami dla nich nieprzeznaczonymi. Warto jednak pamiętać, że i w tym przypadku blokowanie stron internetowych jest rozwiązaniem bardzo niedoskonałym. Uczniowie zawsze mogą ominąć zabezpieczenia lub skorzystać z innej sieci (np. komórkowej). Dlatego środki techniczne nie mogą zastąpić jasno wytyczonych zasad korzystania z Internetu w szkole, edukacji i indywidualnego wsparcia. Blokowanie stron to oczywiście dużo łatwiejsze rozwiązanie, ale – jak to z łatwymi rozwiązaniami zazwyczaj bywa – ogromnie zawodne.

W przypadku konieczności zastosowania rozwiązań filtrujących radzimy uważnie przyjrzeć się ich domyślnym ustawieniom – zdarza się, że filtry stworzone przez producenta blokują nieszkodliwe treści (np. całą zawartość pochodzącą z portalu ze zdjęciami Flickr), jednocześnie zezwalając na dostęp do treści, które teoretycznie mają być blokowane (np. „nagich" zdjęć umieszczonych poza dużymi portalami z pornografią, choćby na prywatnych blogach).

Popularność narzędzi filtrujących napędza nie tylko chęć dbania o bezpieczeństwo dzieci, ale również ochrona własnych interesów. Dość powszechna jest obawa, że jeśli użytkownik za pomocą otwartej sieci złamie prawo (np. dokona naruszenia praw autorskich), to odpowiedzialność za to poniesie właściciel sieci. Na szczęście dla otwartych sieci i ich właścicieli sytuacja nie jest wcale tak niekorzystna, jak mogłoby się wydawać. Za przestępstwa popełnione w Internecie (podobnie jak poza nim) odpowiada sprawca, a udostępnienie otwartej sieci trudno w takim przypadku uznać za pomocnictwo. Podobnie ma się sprawa z odpowiedzialnością cywilną, choć w tym przypadku trzeba pamiętać o kilku małych, choć ważnych, „ale". Jedno z nich wynika z faktu, że dzieci poniżej 13 roku życia same nie odpowiadają za wyrządzoną szkodę – odpowiedzialność za ich działanie może ponieść opiekun, wówczas gdy nienależycie

wywiązywał się ze swoich obowiązków.

Popularnych, choć pozornych, sposobów na zabezpieczenie sieci jest wiele. Jednym z nich jest ograniczenie możliwości korzystania z niektórych protokołów sieciowych, np. wyłączenie poczty elektronicznej lub ruchu szyfrowanego. Skrajnym przypadkiem takiego blokowania jest zezwolenie na korzystanie wyłącznie z nieszyfrowanych stron WWW. Uniemożliwia to korzystanie z klientów poczty (de facto niezbędnych do szyfrowania maili) oraz logowanie się do bezpiecznych stron używających HTTPS (w tym webmaili oraz banków internetowych). Takie działania wynikają najczęściej z chęci zablokowania „na wszelki wypadek" całego ruchu w sieci i pozostawienia tylko nielicznych usług, uważanych przez administratora za niezbędne (pojęcie niezbędności może być zupełnie inaczej rozumiane przez użytkowników sieci). Nie służą one jednak rzeczywistemu bezpieczeństwu: narażają użytkowników sieci na ataki służące pozyskaniu treści ich korespondencji i innych informacji, uniemożliwiają korzystanie z narzędzi zwiększających anonimowość, takich jak sieć Tor czy bezpieczna poczta elektroniczna.

UŻYTKOWNICY POD KONTROLĄ

Opiekunów sieci bezprzewodowych zachęcamy do zastanowienia się, czy wszystkie dane zbierane o ruchu i zwyczajach użytkowników są rzeczywiście niezbędne. W przypadku najprostszych sieci, opartych o pojedynczy router Wi-Fi i podłączonych do sieci dostawcy Internetu, nie jest to problemem – urządzenie domyślnie nie zapisuje żadnych istotnych informacji. W przypadku większych sieci (np. na uczelni lub w bibliotece publicznej) warto zwrócić uwagę na te jej elementy, które mogą zapisywać informacje o podłączających się urządzeniach i w miarę możliwości zrezygnować ze zbierania nieprzydatnych danych. Tu powinna działać zasada „im mniej, tym lepiej".

Oprogramowanie filtrujące jest typowym przykładem narzędzia,

które zbiera zbędne dane o użytkownikach. Zdarza się, że domyślnie zapisuje informacje o tym, z jakiego urządzenia wykonane zostało zapytanie o zablokowany zasób. Przechowywanie takiej informacji nie zwiększa w żaden sposób skuteczności narzędzia filtrującego, naraża natomiast użytkowników na problemy (np. szantaż) w razie uzyskania nieautoryzowanego dostępu do tych danych przez włamywacza. Mimo zagrożeń takie mechanizmy bywają domyślnie włączone.

REGULAMIN SIECI

Przydatną praktyką jest spisanie zasad korzystania z otwartej sieci. Warto pamiętać, że dobre zasady służą przede wszystkim edukacji użytkowników, a nie bieżącemu nadzorowi ich działań w sieci. Kluczowa jest dostępność regulaminu – w przypadku publicznej sieci dobrym pomysłem jest wywieszenie go w widocznym miejscu. Jeśli dochodzi do jawnego łamania ustalonych zasad, warto zastanowić się nad tym, co jest rzeczywistym źródłem problemów: być może użytkownicy nie znają regulaminu bądź nie rozumieją jego postanowień.

Ważnym elementem regulaminu powinna być informacja o tym, jak działa dana sieć. Jeśli zbierane są dane o ruchu i użytkownikach, ci powinni być o tym poinformowani. Podobnie wygląda sytuacja w przypadku sieci, które są „filtrowane” (np. w szkołach) – użytkownicy powinni mieć możliwość znalezienia informacji o tym w regulaminie, tak aby nie zostali zaskoczeni informacją o zablokowanej treści oraz mogli w razie potrzeby zapewnić sobie inny dostęp do Internetu.

Dobrą praktyką jest również zwrócenie w regulaminie uwagi na zagrożenia związane z korzystaniem z Internetu oraz umieszczenie w nim informacji o dodatkowych narzędziach zwiększających prywatność, takich jak Tor, szyfrowana poczta czy protokół HTTPS.

Autorstwo: Michał „Czesiek” Czyżewski, Małgorzata Szumańska
Współpraca: Kamil Śliwowski

Źródło: Fundacja Panoptykon