Biuletyn Bezpieczeństwa Komputerowego

Bezpieczna domowa sieć WI-Fi

Wstęp

Aby utworzyć bezpieczną sieć domową, musisz zacząć od zabezpieczenia i odpowiedniego skonfigurowania punktu dostępowego, czyli routera Wi-Fi. Router to urządzenie, które kontroluje, kto i co może połączyć się z Twoją siecią domową. Przedstawiamy pięć prostych kroków, aby stworzyć znacznie bezpieczniejszą sieć domową.

Skoncentruj się na podstawach

Często najłatwiejszym sposobem połączenia się i skonfigurowania routera jest połączenie z siecią domową. Połącz się za pomocą przeglądarki z konkretnym adresem IP udokumentowanym w instrukcji urządzenia (z reguły https://192.168.1.1) lub użyj narzędzia dostarczonego przez dostawcę urządzenia Wi-Fi.

1. **Zmień hasło administratora**: Najprawdopodobniej router został skonfigurowany z domyślnym hasłem konta administratora, które umożliwia zmianę konfiguracji urządzenia. Często domyślne hasła są powszechnie znane i są publikowane w Internecie. Pamiętaj, aby zmienić hasło administratora na unikalne i silne, na takie które jest znane tylko Tobie. Jeśli urządzenie na to pozwala, zmień również nazwę administratora.
2. **Utwórz hasło dostępu do sieci**: Skonfiguruj swoją sieć Wi-Fi tak, aby dostęp do niej również był chroniony unikalnym, silnym hasłem (upewnij się, że różni się ono od hasła konta administratora). W ten sposób tylko osoby i urządzenia, którym ufasz, mogą dołączyć do Twojej sieci domowej. Rozważ użycie menedżera haseł, aby utworzyć silne hasło. Może on również przechowywać wszystkie hasła, których używasz.
3. **Aktualizuj oprogramowanie** : Zadbaj o włączenie automatycznej aktualizacji oprogramowania w routerze. Dzięki aktualnemu oprogramowaniu, zapewnisz sobie maksymalne bezpieczeństwo urządzenia. Jeśli automatyczna aktualizacja nie jest dostępna w Twoim routerze, loguj się cyklicznie do urządzenia, aby sprawdzić, czy są dostępne aktualizacje. Jeśli urządzenie nie jest już wpierane, rozważ zakup nowego, które będziesz mógł zaktualizować, aby uzyskać najnowsze aktualizacje zabezpieczeń.

4. **Używaj sieci dla gości**: Sieć dla gości to oddzielna wirtualna sieć, którą może utworzyć router Wi-Fi. Oznacza to, że router ma w rzeczywistości dwie sieci. *Sieć podstawowa* to ta, z którą łączą się zaufane urządzenia, takie jak Twój komputer, smartfon lub tablet. *Sieć dla gości* jest używana do połączenia niezaufanych urządzeń, na przykład urządzenia gości odwiedzających Twój dom lub niektóre z Twoich osobistych urządzeń domowych. Urządzenia połączone z siecią dla gości, nie mogą widzieć, ani komunikować się z żadnym z zaufanych urządzeń podłączonych do sieci podstawowej.
5. **Używaj filtrowania DNS:** DNS to usługa internetowa, która konwertuje nazwy witryn internetowych na adresy IP. Dzięki temu komputer może łączyć się z odpowiednią stroną po wpisaniu jej nazwy. Routery zazwyczaj używają domyślnego serwera DNS dostarczonego przez dostawcę usług internetowych, ale bezpieczniejsze alternatywy są dostępne bezpłatnie w usługach takich jak OpenDNS , Cloudflare for Families lub Quad9. Mogą one zapewnić dodatkowe bezpieczeństwo, blokując złośliwe i niepożądane witryny. Zaloguj się do routera Wi-Fi i zmień adres serwera DNS na bezpieczniejszą alternatywę.

Zabezpieczenie routera Wi-Fi to pierwszy i jeden z najważniejszych etapów tworzenia bezpiecznej sieci domowej. Aby uzyskać więcej informacji na temat zabezpieczania routera Wi-Fi, zapoznaj się z instrukcją obsługi urządzenia lub, jeśli dostawca usług internetowych udostępnił urządzenie Wi-Fi, skontaktuj się z nim, aby uzyskać więcej informacji na ten temat.

Redaktor gościnny

Joshua Wright (Twitter @joswr1ght) jest dyrektorem w Counter Hack Challenges, LLC, kieruje koordynacją i rozwojem wyzwań cybernetycznych dla NetWars i Holiday Hack Challenge. Znajdź Josha na LinkedInie: https://linkedin.com/in/joswr1ght.

Źródła

Tworzenie haseł w prostszy sposób: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Menedżer haseł: https://www.sans.org/security-awareness-training/resources/password-managers-0
Aktualizacje: https://www.sans.org/security-awareness-training/resources/power-updating
OpenDNS Setup Guide: https://www.opendns.com/setupguide/#familyshield

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz