OUCH! | Czerwiec

SANS SECURITY AWARENESS

Biuletyn Bezpieczeństwa Komputerowego

Projektowanie bezpieczeństwa

Wstęp

W przeszłości budowanie domowej sieci sprowadzało się jedynie do instalacji bezprzewodowego routera i kilku komputerów należących do sieci. Dziś z racji tego, że coraz częściej pracujemy, uczymy i łączymy się z domu, musimy więcej uwagi poświęcić bezpieczeństwu sieci domowych. Oto cztery kroki aby poprawnie to zrobić.

Twoja bezprzewodowa sieć

Prawie każda domowa sieć zaczyna się od sieci bezprzewodowej. Pozwala ona na podłączenie urządzeń do internetu. Większość domowych sieci bezprzewodowych kontrolowana jest przez router lub dedykowany punkt dostępu. Oba działają w ten sam sposób: emitują bezprzewodowy sygnał, który pozwala na łączenie się domowych urządzeń z internetem. Oznacza to, że zabezpieczenie sieci bezprzewodowej jest kluczowe dla ochrony twojego domu. Rekomendujemy następujące kroki dla prawidłowego zabezpieczenia:

- W pierwszej kolejności należy zmienić domyślne hasło administracyjne dla routera lub bezprzewodowego punktu dostępu, w zależności od tego który kontroluje sieć bezprzewodową. Konto administratora pozwala na konfigurowanie ustawień sieci.
- Upewnij się czy jedynie zaufane urządzenia są połączone z siecią bezprzewodową. Powinno się to zrobić przez włączenie silnych ustawień bezpieczeństwa. Wymaga to ustawienia hasła do łączenia się z siecią domową oraz szyfrowania aktywności po połączeniu się z nią.
- Musimy się upewnić, że hasło dostępowe jest silne i inne niż hasło administratora. Urządzenia przechowują hasła, więc nie będzie potrzeby wpisywania go za każdym razem kiedy będziemy chcieli się połączyć z siecią.

Jeśli nie jesteśmy pewni jak poprawnie i bezpiecznie zainstalować router, powinniśmy skorzystać z instrukcji obsługi i montażu danego urządzenia dostępowego. Informacje te przeważanie są dostępne na stronie producenta routera lub punktu dostępowego.

Hasła

Używajmy silnych, unikalnych haseł dla każdego z naszych urządzeń i kont internetowych. Ze szczególnym naciskiem na *silne* i *unikalne*. Im dłuższe jest hasło tym silniejsze. Warto używać kombinacji kilku słów jak np. ***słodkie-pączki-szczęścia***..

Unikalne hasło oznacza stosowanie różnych haseł dla każdego urządzenia i konta. Używanie menedżera haseł, który przechowuje w bezpieczny szyfrowany sposób hasła usprawni ich stosowanie i uwolni nas od ich zapamiętywania.

Warto również gdy tylko to możliwe stosować uwierzytelnianie dwuskładnikowe, w szczególności w stosunku do kont internetowych. Taki rodzaj uwierzytelniania oprócz hasła wymaga potwierdzenia poprzez kod przesłany wiadomością tekstową SMS lub wygenerowany przez specjalną aplikację. To jeden z najskuteczniejszych kroków, który można podjąć, a zarazem jeden z prostszych.

Urządzenia

Kolejnym krokiem jest świadomość tego jakie urządzenia są podłączone
do naszej sieci bezprzewodowej i upewnienie się, że wszystkie te urządzenia są zaufane i bezpieczne. Dawniej gdy w sieci mieliśmy do czynienia jedynie z komputerami było to o wiele prostsze. Dziś mamy do czynienia z wieloma urządzeniami, które mogą zostać podłączone
do sieci od smartfonów przez telewizory, konsole do gier, drukarki na samochodach skończywszy. Gdy już zidentyfikujemy wszystkie urządzenia w naszej sieci, upewnijmy się że każde z nich jest bezpieczne. Najlepszym sposobem jest zmiana domyślnych haseł oraz włączenie automatycznych aktualizacji, jeśli to tylko możliwe.

Kopie zapasowe

Czasami niezależnie od poziomu naszej ostrożności i tak możemy zostać ofiarą ataku hackerskiego. Gdy to się wydarzy zazwyczaj jedynym wyjściem do odzyskania danych jest przywrócenie ich z użyciem kopii zapasowych. Starajmy się regularnie tworzyć kopie zapasowe wszystkich ważnych informacji i weryfikować czy można je przywrócić. Większość przenośnych urządzeń ma możliwość tworzenia kopi zapasowych z zastosowaniem chmury. Można również zastanowić się nad zakupem oprogramowania do tworzenia kopii zapasowych dla komputerów osobistych, które to są relatywnie tanie i łatwe do korzystania.

Redaktor gościnny

Randy Marchany jest Głównym Inspektorem bezpieczeństwa teleinformatycznego w Virginia Tech. Jest również starszym instruktorem SANS i wykłada SEC566, SEC440 oraz prowadzi kurs Implementing & Auditing the Critical Security Controls. Śledź Randy @randymarchany.

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
Czy robisz kopie zapasowe?: https://www.sans.org/security-awareness-training/resources/got-backups
Domyślne hasła urządzeń: https://www.routerpasswords.com/

Polski przekład CERT Polska: Bartłomiej Wnuk, Konrad Purzycki.