Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

- Sieć bezprzewodowa
- OpenDNS
- Urządzenia

Jak zabezpieczyć domową sieć

Wstęp

Jeszcze kilka lat temu sieci domowe były stosunkowo proste, zazwyczaj nic ponad bezprzewodowy punkt dostępu i komputer lub dwa służące do surfowania po Internecie lub gier online. Jednak sieci domowe stają się coraz bardziej złożone. Nie tylko podłączamy do naszych sieci domowych znacznie większą liczbę urządzeń, ale także robimy z nimi znacznie więcej. W tym wydaniu omówimy kilka podstawowych kroków w celu stworzenia bezpiecznej sieci domowej.

Redaktor gościnny

Redaktorem gościnnym tego wydania jest Kevin Johnson, CEO w Secure Ideas oraz prowadzący **MySecurityScanner.com**. Kevin jest także starszym instruktorem w SANS Institute. Więcej informacji można znaleźć na **www.secureideas.com**.

Sieć bezprzewodowa

Większość dzisiejszych sieci domowych opiera się na sieci bezprzewodowej (często nazywanej siecią Wi-Fi). To właśnie ona pozwala na podłączenie dowolnych urządzeń do Internetu, od laptopów i tabletów po konsole do gier i telewizory. Aby było to możliwe, sieć bezprzewodowa potrzebuje czegoś zwanego punktem dostępowym (ang. access point). Jest to urządzenie, które łączy się z routerem (może być też w niego wbudowane) i wysyła sygnał bezprzewodowy, z którym łączą się różne urządzenia. Kiedy twoje urządzenia połączą się z punktem dostępowym, mogą przez niego łączyć się z innymi urządzeniami z sieci domowej, jak również z Internetem. W efekcie bezprzewodowy punkt dostępu do sieci jest jednym z kluczowych elementów sieci domowej i bardzo zalecamy następujące kroki w celu jego zabezpieczenia:

- Dla większości bezprzewodowych punktów dostępu domyślny login i hasło administratora są ogólnie znane i często nawet umieszczone w Internecie. Dlatego przede wszystkim należy je zmienić na takie, które znasz tylko Ty. Upewnij się, że jest to unikalne hasło i nie wykorzystałeś go już do żadnego innego konta.
- Kolejną opcją którą należy skonfigurować to nazwa sieci bezprzewodowej (nazywana również SSID). Jest to nazwa, która wyświetli się na Twoich urządzeniach przy próbie połączenia się do lokalnej sieci bezprzewodowej. Nadaj swojej sieci niepowtarzalną nazwę, tak aby było łatwo ją zidentyfikować, ale pamiętaj, że nie powinna ona zawierać żadnych danych osobowych. Nie

Jak zabezpieczyć domową sieć

ma raczej większego sensu konfiguracja domowej sieci jako ukrytej (lub nie rozgłaszanej, ang. non-broadcast). Większość narzędzi do skanowania lub przeciętny atakujący może bardzo łatwo ją odkryć.

- Następnym krokiem jest upewnienie się, że tylko osoby, które znasz i którym ufasz mogą się połączyć i korzystać z twojej sieci bezprzewodowej oraz, że te połączenia są szyfrowane. Chcesz przecież mieć pewność, że sąsiedzi lub obcy nie będą mogli połączyć się albo monitorować twojej sieci. Można w prosty sposób zmniejszyć to ryzyko poprzez włączenie silnego zabezpieczenia w bezprzewodowym punkcie dostępu. Obecnie najlepszym rozwiązaniem jest korzystanie z mechanizmu zabezpieczeń WPA2. Włączając WPA2 sprawiasz, że aby ktoś mógł połączyć się z siecią musi podać hasło, a po uwierzytelnieniu wszystkie połączenia są szyfrowane. Upewnij się, że nie używasz starszych, przestarzałych metod zabezpieczeń, takich jak WEP lub że sieć nie ma żadnych zabezpieczeń, co jest nazywane inaczej siecią otwartą. Otwarta sieć pozwala każdemu połączyć się z nią bez uwierzytelniania.
- Hasło którego osoby w twoim domu będą używać do łączenia się z siecią bezprzewodową powinno być silne, trudne do odgadnięcia i różnić się od hasła administratora. Najprawdopodobniej będzie wymagane podać je tylko raz dla każdego urządzenia ponieważ później zostanie ono w nim zapamiętane.
- Wiele bezprzewodowych punktów dostępu obsługuje tzw. sieć dla gości (ang. guest network). Sieć dla gości pozwala odwiedzającym Cię połączyć się z bezprzewodowym punktem dostępu i uzyskać dostęp do Internetu, ale nie pozwala połączyć się z żadnym innym urządzeniem w sieci domowej. Jeśli dodasz sieć dla gości również należy włączyć dla niej WPA2 i ustanowić dla niej inne hasło.
- Jeśli masz problem z zapamiętaniem różnych haseł, użyj menedżera haseł aby je bezpiecznie przechowywać.

Aby chronić sieć domową upewnij się, że sieć bezprzewodowa jest zabezpieczona, że korzystasz z OpenDNS lub podobnej usługi, a wszystkie urządzenia w sieci domowej są zaktualizowane.

Jak zabezpieczyć domową sieć

OpenDNS

Po skonfigurowaniu sieci bezprzewodowej zalecamy skonfigurować sieć domową tak, aby używać usługi oferowanej przez OpenDNS jako serwerów DNS (lub innej podobnej, np. Norton ConnectSafe for Home). Po wpisaniu w przeglądarce nazwy, dzięki DNS Twoja przeglądarka wie, z którym serwerem w Internecie ma się połączyć. Usługi takie jak OpenDNS identyfikują znane, zainfekowane strony internetowe i powstrzymają wszelkie urządzenia podłączone do domowej sieci bezprzewodowej przed przypadkowym odwiedzeniem takich stron. Ponadto usługi te często dają możliwość filtrowania i blokowania witryn budzących zastrzeżenia. To co sprawia, że to rozwiązanie to jest tak skuteczne to że nie ma konieczności instalowania żadnego oprogramowania na twoich urządzeniach, wystarczy jedynie wprowadzić zmianę w bezprzewodowym punkcie dostępu.

Dowiedz się więcej

Zasubskrybuj comiesięczny biuletyn o bezpieczeństwie komputerowym SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące 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 reagowania 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

Źródła

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Network security scanner :
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Systemy zarządzania hasłami:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz