SANS SECURITY AWARENESS
CERT.PL
OUCH! | Styczeń 2018
Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Domowa sieć Wi-Fi**
- **Twoje urządzenia**
- **Hasła**
- **Kopie zapasowe**

Cyberbezpieczny Dom

Wprowadzenie

Jeszcze kilka lat temu stworzenie cyberbezpiecznego domu nie było niczym skomplikowanym; większość gospodarstw domowych składała się głównie z sieci bezprzewodowej oraz kilku komputerów. Dzisiejsza technologia stała się daleko bardziej rozwinięta i zintegrowana z niemal każdą dziedziną naszego życia – od urządzeń mobilnych i konsol do gier po domowe termostaty czy lodówki. Poniżej podajemy cztery proste kroki opisujące jak zadbać o cyberbezpieczeństwo swojego domu.

Redaktor gościnny
Matt Bromiley na codzień zajmuje się reagowaniem na incydenty, pomagając swoim klientom w sprawach związanych z naruszeniem bezpieczeństwa danych. Jest także wykładowcą SANS i prowadzącym kurs FOR508 obejmujący swoim zakresem zaawansowaną informatykę śledczą oraz obsługę incydentów. Dostępny na Twitterze jako **@mbromileyDFIR**.

Domowa sieć Wi-Fi

Bezprzewodową sieć (Wi-Fi) znajdziemy dziś praktycznie w każdym domu. To dzięki niej możesz podłączyć do Internetu urządzenia, które posiadasz. Zarządzanie większością domowych sieci bezprzewodowych odbywa się za pośrednictwem routera lub dedykowanego punktu dostępowego. Oba rozwiązania działają w zbliżony sposób, propagując fale radiowe za pośrednictwem których urządzenia w Twoim domu mogą prowadzić komunikację. Oznacza to, że zabezpieczenie sieci bezprzewodowej stanowi kluczowy element dla bezpieczeństwa Twojego domu. Mając to na uwadze, zalecamy podjęcie następujących kroków:

- Zmień domyślne hasło administratora do wszystkich routerów i punktów dostępowych posiadających dostęp do Twojej sieci domowej. Konto administratora umożliwia zarządzanie konfiguracją takiej sieci.
- Upewnij się, że tylko osoby którym ufasz mogą łączyć się z Twoją siecią bezprzewodową. Korzystaj z rozwiązań oferujących wysoki poziom bezpieczeństwa. Aktualnie najlepszym wyborem będzie wykorzystanie WPA2. Aktywując ten mechanizm, osoby próbujące zalogować się do Twojej sieci domowej zostaną poproszone o podanie hasła, a ich połączenie będzie objęte szyfrowaniem.
- Upewnij się, że hasło używane do łączenia się z Twoją siecią bezprzewodową jest odpowiednio silne i różne od tego, które przypisałeś do konta administratora. Pamiętaj, że hasło to będziesz musiał wprowadzić tylko raz na każdym z posiadanych urządzeń, urządzenia zapamiętają hasło.
- Wiele sieci bezprzewodowych oferuje rozwiązanie pod nazwą “sieć dla gości”. Umożliwia ono połączenie z Internetem, przy jednoczesnej ochronie sieci domowej. Korzystając z tego rozwiązania goście nie będą mogli łączyć się z innymi urządzeniami wewnątrz Twojej domowej sieci. Jeżeli zdecydujesz się na skorzystanie z tej funkcjonalności, upewnij się że aktywowałeś mechanizm WPA2 oraz nadałeś unikalne hasło dla sieci.

Cyberbezpieczny Dom

Nie wiesz, jak podjąć powyższe kroki? Zapytaj swojego dostawcę Internetu, odwiedź jego stronę internetową, zajrzyj do dokumentacji dołączonej do routera / punktu dostępowego, lub poszukaj odpowiedzi na dedykowanej stronie producenta sprzętu.

Podejmij cztery proste kroki, aby zadbać o cyberbezpieczeństwo Twojego domu; zabezpiecz swoją sieć Wi-Fi, aktywuj aktualizacje automatyczne, korzystaj z unikatowych haseł, wykonuj kopie zapasowe.

Twoje urządzenia

Następnym krokiem będzie weryfikacja, jakie urządzenia podłączone są do Twojej domowej sieci Wi-Fi oraz upewnienie się, że są one odpowiednio zabezpieczone. Wydawało się to proste kiedy posiadałeś jeden lub dwa komputery. Dzisiaj jednak niemal wszystko może łączyć się z Twoją siecią domową, włączając w to smartfony, telewizory, konsole do gier, elektroniczne nianie, głośniki, a być może nawet Twój samochód. Po rozpoznaniu wszystkich urządzeń w sieci upewnij się, że każde z nich jest odpowiednio zabezpieczone. Najlepszą drogą aby to uczynić, będzie upewnienie się o uruchomionym automatycznym pobieraniu aktualizacji wszędzie tam, gdzie jest to możliwe. Cyberprzestępcy nieustannie wyszukują nowe podatności w urządzeniach i systemach operacyjnych. Aktywując aktualizacje automatyczne, Twój komputer oraz posiadane urządzenia będą korzystały z możliwie najnowszych wersji oprogramowana, dzięki czemu trudniej będzie przełamać ich zabezpieczenia.

Hasła

Kolejny krok to korzystanie z silnych i niepowtarzalnych haseł dla każdego urządzenia oraz konta w sieci. Kluczowa jest tutaj *siła* i *unikalność*. Być może jesteś zmęczony korzystaniem z zawiłych haseł, trudnych do zapamiętania i wpisywania. My również. Zamiast tego skorzystaj z odpowiedniej frazy lub wyrażenia. Jest to rodzaj hasła, który wykorzystuje ciąg łatwych do zapamiętania słów, jak np. “Gdzie jest moja kawa?” lub “słoneczne-pączki-szczęśliwie-zaginęły”. Im dłuższy ciąg znaków, tym trudniej go złamać. Unikalność hasła polega na rezygnacji z posiadania tego samego hasła dla dwóch różnych urządzeń, czy kont w Internecie. Dzięki temu, jeżeli jedno hasło dostanie się w niepowołane ręce, pozostałe konta i urządzenia nadal pozostaną bezpieczne. Masz problem z ich zapamiętaniem? Nie martw się, nas też to dotyczy. Zachęcamy Cię do korzystania z menedżera haseł. Jest to specjalny program, który w bezpieczny sposób przechowa wszystkie Twoje hasła w zaszyfrowanym, wirtualnym sejfie.

Na koniec, wszędzie tam gdzie jest to możliwe (szczególnie w przypadku kont internetowych) aktywuj dwuskładnikowe uwierzytelnianie. Rozwiązanie to znacząco podnosi poziom bezpieczeństwa. Opiera się na logowaniu za pomocą hasła, rozszerzając jednocześnie proces uwierzytelniania o dodatkowy warunek, który należy wypełnić w celu potwierdzenia swojej tożsamości. Dla przykładu, może to być jednorazowy kod przesyłany sms’em lub generowany w specjalnej aplikacji mobilnej na Twoim smartfonie. Uwierzytelnianie dwuskładnikowe jest prawdopodobnie jednym z najistotniejszych kroków, które warto podjąć w celu zadbania o swoje bezpieczeństwo w sieci, jest także dużo prostsze niż myślisz.

Cyberbezpieczny Dom

Kopie zapasowe

Czasami niezależnie od tego jak bardzo jesteś ostrożny, może się zdarzyć, że padniesz ofiarą ataku hakerów. W takiej sytuacji często jedyną możliwością odzyskania Twoich danych jest odtworzenie ich z kopii zapasowej. Upewnij się, że tworzysz je regularnie, że obejmują wszystkie dane na których Ci zależy, oraz weryfikuj czy zostały wykonane prawidłowo poprzez próbę odtworzenia ich zawartości. Większość urządzeń mobilnych wspiera wykonywanie automatycznych kopii zapasowych w chmurze. W przypadku komputerów może być konieczny zakup dedykowanego oprogramowania lub usługi, są one stosunkowo niedrogie i proste w użyciu.

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 securingthehuman.sans.org/ouch/archives 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

Silne hasła:	https://securingthehuman.sans.org/ouch/2017#april2017
Menedżery haseł:	https://securingthehuman.sans.org/ouch/2017#september2017
Uwierzytelnianie dwuskładnikowe:	https://securingthehuman.sans.org/ouch/2017#december2017
Kopie zapasowe:	https://securingthehuman.sans.org/ouch/2017#august2017

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski

