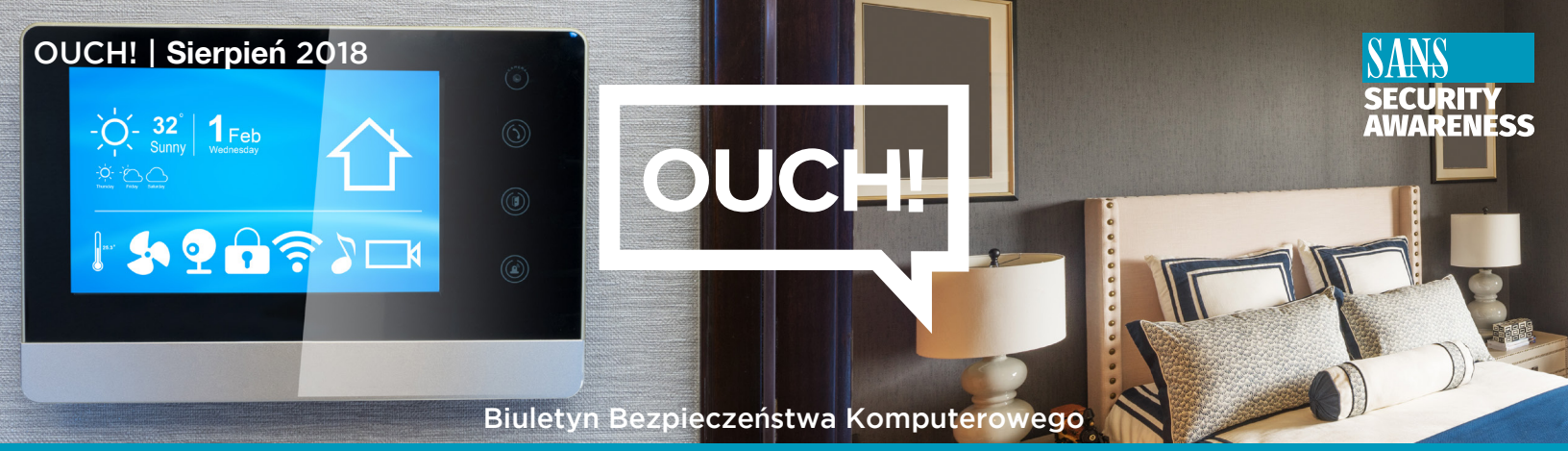
OUCH! | Sierpień 2018



OUCH!

SANS SECURITY AWARENESS

Biuletyn Bezpieczeństwa Komputerowego

Inteligentne urządzenia w Twoim domu

Czym są inteligentne urządzenia domowe?

Do niedawna tylko niewielka część domowych urządzeń mogła łączyć się z Internetem. Na tej liście był laptop, smartfon, być może konsola do gier. Obecnie jednak coraz więcej urządzeń, od żarówek i głośników, poprzez telewizory, aż po zamki w drzwiach wejściowych do domu, czy samochodu łączy się z globalną siecią. Już niedługo prawie każdy sprzęt w Twoim domu będzie posiadał taką możliwość. Urządzenia tego typu nazywamy Internetem Rzeczy (ang. IoT – Internet of Things). Korzystanie z nich jest bardzo wygodne, ale pociąga za sobą także specyficzne zagrożenia.

Gdzie leży problem?

Im więcej urządzeń jest podłączonych do Twojej sieci domowej, tym więcej rzeczy może pójść nie tak. Cyberprzestępcy mogą zaprogramować je w celu przeprowadzenia ataku na inne osoby, producenci mogą gromadzić dane o Twojej aktywności, zaś same urządzenia mogą zostać zainfekowane przez złośliwe oprogramowanie, a dostęp do nich zablokowany. Wielu producentów wspomnianych urządzeń nie posiada doświadczenia w zakresie cyberbezpieczeństwa i postrzega zabezpieczenia jako koszt. W rezultacie większość inteligentnych urządzeń domowych jest słabo zabezpieczona, albo w ogóle nie posiada zabezpieczeń. Dla przykładu, niektóre urządzenia zabezpieczone są standardowymi hasłami które są powszechnie znane, często brakuje im też możliwości aktualizacji oprogramowania albo zmiany domyślnego hasła.

Jak mogę się chronić?

Co można zrobić? Zdecydowanie chcemy, żeby korzystanie z urządzeń podłączonych do sieci ułatwiało życie i jednocześnie było bezpieczne. Urządzenia te posiadają fantastyczne możliwości i pomagają w codziennym życiu. Co więcej, w miarę rozwoju Internetu Rzeczy rezygnacja z korzystania z inteligentnych sprzętów może stać się niemożliwa. Poniżej podajemy kilka kluczowych zasad, dzięki którym zadbasz o swoje bezpieczeństwo.

Podłączaj do sieci tylko te urządzenia, których naprawdę potrzebujesz: Najprostszym sposobem zabezpieczenia inteligentnego urządzenia, jest nie podłączanie go do Internetu. Jeżeli nie ma potrzeby, aby Twój domowy sprzęt łączył się z całym światem, nie podłączaj go do domowej sieci Wi-Fi. Czy naprawdę powiadomienia wysyłane przez toster na Twój telefon są Ci niezbędne?

Stwórz listę podłączonych urządzeń: Które sprzęty korzystają z Twojej sieci domowej? Nie jesteś pewien lub nie pamiętasz? Wyłącz router odpowiedzialny za domowe Wi-Fi i sprawdź, które z nich przestaną działać. W ten sposób może nie wychwycisz wszystkich urządzeń, ale będziesz zaskoczony o jak wielu z nich nie pamiętałeś.

Aktualizuj na bieżąco: To bardzo ważne, aby aktualizować urządzenia, podobnie jak komputery czy urządzenia mobilne. Jeżeli urządzenie posiada opcję aktualizacji automatycznych, pamiętaj aby ją aktywować.

Hasła: Zmień domyślne hasło dostępu do urządzenia. Wybierz takie, które jest niepowtarzalne, znane tylko Tobie i trudne do złamania. Prawdopodobnie nie będziesz musiał wpisywać go zbyt często, lub będzie to jednorazowe działanie. Masz problem z zapamiętaniem haseł? Nie martw się, my też mamy z tym problem. Rozważ możliwość skorzystania z rozwiązania zwanego menadżerem haseł.

Ustawienia prywatności: Jeżeli Twoje urządzenie umożliwia konfigurację opcji prywatności, wykorzystaj to. Ogranicz liczbę informacji, które są przez nie zbierane, czy udostępniane. Jedną z możliwości jest po prostu wyłączenie wszelkiego przekazywania danych dalej.

Producent: Kupuj urządzenia od firm, które dobrze znasz i do których masz zaufanie. Wybieraj produkty wspierające bezpieczeństwo, na przykład takie które umożliwiają automatyzację pobieranych aktualizacji, zmianę domyślnego hasła i dostosowanie opcji prywatności.

Urządzenia też słuchają: Jeżeli urządzeniu można wydawać polecenia głosowe, będzie ono nieustannie nasłuchiwać. Przykładowo, rozwiązania takie jak Alexa czy Google Home mogą rejestrować rozmowy o charakterze wrażliwym. Weź to pod uwagę ustalając miejsce, w którym umieścisz urządzenie w swoim domu. Zrób także przegląd ustawień prywatności.

Sieć dla gości: Rozważ podłączenie urządzeń, składających się na tzw. „inteligentny dom" do specjalnie wydzielonej sieci WiFi w odróżnieniu od urządzeń takich jak komputer i inne urządzenia mobilne, które korzystają z podstawowej sieci WiFi w Twoim mieszkaniu. W ten sposób, w przypadku infekcji któregokolwiek z urządzeń IoT, komputer i urządzenia mobilne pozostaną bezpieczne.

Nie ma powodu, aby obawiać się nowych technologii, należy jednak rozumieć zagrożenia, jakie mogą stanowić. Podejmując kilka prostych kroków możesz uczynić swój inteligenty dom bardziej bezpiecznym.

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

Redaktor Gościnny

Robert M. Lee (@RobertMLee) - certyfikowany instruktor SANS, autor kursu FOR578 (Cyber Threat Intelligence) oraz ICS515 (ICS Active Defense and Incident Response). Założyciel i dyrektor generalny firmy Dragos, specjalizującej się w cyberbezpieczeństwie infrastruktury przemysłowej.

Przydatne linki

Silne hasła:	https://www.sans.org/u/GEB
Menedżery haseł:	https://www.sans.org/u/GEG
Jak zabezpieczyć domową sieć:	https://www.sans.org/u/GEL