OUCH! | Maj 2016

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W tym wydaniu..

- **Czym jest Internet Rzeczy**
- **Problemy z IoT**
- **Jak chronić urządzenia IoT**

Internet Rzeczy (IoT)

Czym jest Internet Rzeczy

W przeszłości technologia była względnie prosta w użyciu: po prostu podłączałeś komputer do Internetu i wykorzystywałeś go do codziennej pracy. Później pojawiły się urządzenia przenośne, takie jak smartfony i tablety, a technologia stała się bardziej zaawansowana. Obecnie urządzenia, które możesz zmieścić w kieszeni mają moc obliczeniową komputerów stacjonarnych. Ich mobilność i możliwości powodują, że stajemy przed nowymi wyzwaniami jeśli chodzi o zapewnienie im bezpieczeństwa. Kolejnym dużym skokiem technologicznym jest tzw. Internet Rzeczy (z ang. Internet of Things, IoT), którego głównym zadaniem jest podłączenie dowolnego urządzenia do Internetu, np. żarówek, dzwonków do drzwi, zabawek czy termostatów. Urządzenia potrafiące komunikować się przez Internet mogą spowodować, że nasze życie stanie się łatwiejsze. Dzięki temu możesz tak skonfigurować włączniki prądu, aby światło w domu zapalało się gdy do niego wracasz, a gasło w momencie kiedy wychodzisz. Rynek urządzeń IoT rozwija się w niesamowitym tempie - nowinki pojawiają się praktycznie każdego tygodnia. Podobnie jak w przypadku urządzeń mobilnych, wprowadzenie IoT do naszych domów niesie ze sobą pewne zagrożenia, z którymi nie musieliśmy mierzyć się wcześniej. W tym wydaniu OUCH! pokażemy jakie ryzyka niesie ze sobą używanie urządzeń IoT, jak zabezpieczyć je, swój dom, a tym samym własną rodzinę.

Redaktor gościnny

James Lyne (**@jameslyne**) jest globalnym szefem działu odpowiedzialnego za badania związane z bezpieczeństwem IT w firmie Sophos. Jest certyfikowanym instruktorem szkoleń Instytutu SANS oraz często prezentuje na branżowych konferencjach.

Problemy z IoT

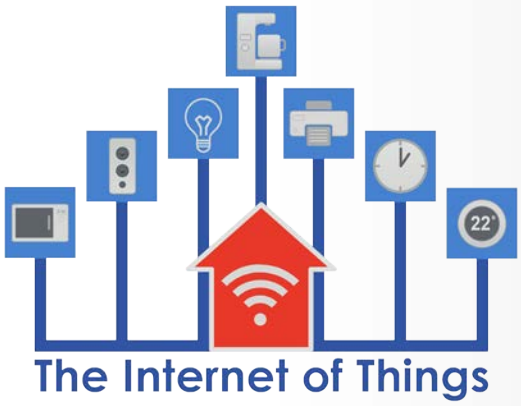
Główną zaletą urządzeń IoT jest to, że są bardzo proste w użyciu. Np. ekspres do kawy z możliwościami komunikacji poprzez Internet prosi jedynie o podanie nazwy i hasła dostępu do Twojej domowej sieci WiFi i już można go używać. Niestety, ta prostota nie jest za darmo. Największym problemem tego typu rozwiązań jest brak zabezpieczeń wynikający z tego, że firmy, które najczęściej wprowadzają nowe urządzenia IoT do tej pory produkowały zwykły sprzęt domowy. Zdarza się też, że są to młode firmy, chcące wprowadzić na rynek nowatorskie produkty minimalnym kosztem i kwestie bezpieczeństwa odkładają na później. Często dla takich przedsiębiorstw najważniejszy niestety jest zysk, a nie bezpieczeństwo użytkowników. Rezultatem takich działań jest to, że większość z urządzeń IoT ma bardzo nikłe lub praktycznie nieistniejące zabezpieczenia. Często zdarza się, że niektóre z nich posiadają ustawione domyślne hasło (często już wszystkim znane), którego w większości przypadków nie można zmienić. Nierzadko dostarczane są z predefiniowaną konfiguracją, której także w żaden sposób nie można

Internet Rzeczy (IoT)

zmodyfikować, ani też zaktualizować samego urządzenia. W rezultacie, tego typu urządzenia, szybko się deaktualizują i pozostają podatne na ataki, ponieważ nie można załatać odkrytych w nich podatności.

Jak chronić urządzenia IoT

Zatem… Co można zrobić? Z pewnością chcesz wykorzystywać urządzenia IoT bezpiecznie i efektywnie. Jak już wspomnieliśmy wcześniej, mają one niesamowite możliwości i mogą sprawić, że Twoje życie będzie znacznie prostsze, oszczędzisz pieniądze i może nawet podniesiesz poziom zabezpieczenia swojego domu przed np. włamywaczami. W przyszłości ta technologia może stać się tak powszechna, że każdy będzie posiadał je w swoim domu. Poniżej zamieszczamy kilka porad jak chronić swoje urządzenia IoT i siebie.



Zawsze sprawdzaj jakie urządzenia IoT łączą się z Twoją siecią, izoluj je jeśli to możliwe, często aktualizuj i chroń używając silnych haseł.

- **Tylko niezbędne urządzenia w sieci**. Najprostszym sposobem na zabezpieczenie urządzenia IoT jest niepodłączanie go do Internetu. Jeżeli nie potrzebujesz, aby urządzenie było cały czas dostępne z Internetu, nie podłączaj go do swojej domowej sieci WiFi.
- **Oddzielna sieć WiFi**. Jeśli Twoje urządzenia IoT muszą być podłączone do Internetu cały czas, zastanów się nad utworzeniem dedykowanej sieci WiFi tylko dla takiego sprzętu - wiele z ruterków domowych wspiera funkcję tworzenia kilku sieci WiFi, jak np. sieci dla gości. Innym wyjściem jest zakup ruterka domowego przeznaczonego specjalnie na potrzeby urządzeń IoT. Taka konfiguracja sprawi, że urządzenia IoT będą odseparowane od innych, znajdujących się w Twojej głównej sieci domowej. Separacja zapewni, że nie będą mogły być wykorzystane do ataku na Twój komputer lub smartfon, które są głównym celem przestępców.
- **Aktualizacje**. Podobnie jak w przypadku komputerów czy urządzeń przenośnych, powinieneś często aktualizować urządzenia IoT. Jeżeli w konfiguracji urządzenia jest opcja, aby aktualizowało się automatycznie, to koniecznie ją wykorzystaj.
- **Silne hasła**. Zmień standardowe hasła w urządzeniach IoT na silne, takie które tylko Ty znasz. Jeżeli obawiasz się, że nie będziesz w stanie ich zapamiętać, użyj menedżera haseł, który w bezpieczny sposób je wszystkie przechowa.
- **Opcje prywatności**. Jeżeli Twoje urządzenia IoT mają możliwość konfiguracji opcji prywatności, postaraj się zminimalizować ilość informacji jakimi dzielą się z resztą sieci. Jeżeli istnieje możliwość całkowitego wyłączenia udostępniania jakichkolwiek danych, zrób to.

Internet Rzeczy (IoT)

- **Wymiana**. Jeżeli Twoje urządzenia IoT mają znane i wykorzystywane luki, a producent nie ma zamiaru udostępnić łatki, pomyśl o wymianie urządzenia na nowe, które nie będzie stanowić zagrożenia dla Ciebie i Twoich bliskich.

Nie ma jednego uniwersalnego rozwiązania jeśli chodzi o zabezpieczanie urządzeń IoT, dlatego warto zapoznać się z literaturą, która dotyczy tego tematu. Niestety, większość z urządzeń IoT nie była tworzona z myślą o bezpieczeństwie użytkowników, więc informacje z tej dziedziny nie są proste do znalezienia. Na szczęście, świadomość użytkowników w dziedzinie bezpieczeństwa z roku na rok poprawia się i mamy nadzieję, że coraz więcej twórców urządzeń IoT będzie je projektować uwzględniając dobre praktyki i udostępniając informacje w jaki sposób aktualizować takie urządzenia.

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

Nowe oblicze hasła:	https://securingthehuman.sans.org/ouch/2015#april2015
Menedżery haseł:	https://securingthehuman.sans.org/ouch/2015#october2015
Zabezpiecz swój nowy tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Jak zabezpieczyć domową sieć:	https://securingthehuman.sans.org/ouch/2016#february2016

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Polski przekład (NASK/CERT Polska): Paweł Jacewicz, Małgorzata Dębska, Przemysław Zielony