Cezary Lasocki
Wydział MIM UW

Internet Rzeczy – szansa czy koszmar?

Ach, te wszystkie połączone w sieć żarówki, mierniki, inteligentne części ubioru, urządzenia gospodarstwa domowego, inteligentne miasta… Ostatnimi czasy wiele osób dostało bzika na ich punkcie, nie tylko z kręgu analityków Big Data. Widocznie jednak amerykańska agencja rządowa FBI nie podchodzi z równym entuzjazmem do tej kwestii. 10 września 2015r. Federalne Biuro Śledcze opublikowało dokument (Alert I-091015-PSA), w którym podjęto się analizy zupełnie nowych zagrożeń wynikających z upowszechniania się rozwiązań typu Internet Rzeczy.

Agencja FBI wyraża wyraźne zaniepokojenie faktem, że owe nowe technologie, na swoim obecnym etapie rozwoju, mają wyraźne braki w kwestiach bezpieczeństwa i skupia się na opisie kilku podstawowych scenariuszy ataku. Wspomina o możliwości przejęcia kontroli nad systemem monitorującym dom lub przedsiębiorstwo, doprowadzając potencjalnych atakujących do wykradnięcia poufnych informacji, które mogą być transmitowane między urządzeniami w lokalnej sieci.

Przechwycenie przez hakerów niedostatecznie zabezpieczonych konfiguracji chroniących połączenia Wi-Fi może skutkować uzyskaniem dostępu do garażu, uruchomieniem samochodu oraz swobodnym wyjechaniem nim na zewnątrz – a wszystko to dokonane zdalnie przed ekranem komputera cyberprzestępcy. Głośno było już o przypadkach Jeepa czy Corvetty, w przypadku których hakerzy byli w stanie zdalnie kontrolować pracę hamulców pojazdu. Nieprzemyślane wdrożenie nowatorskiego produktu zmusiło koncern Chrysler do zorganizowania na szeroką skalę akcji poprawy zabezpieczeń w 1,4 mln pojazdów.

Przy skrupulatnym podejściu do kwestii bezpieczeństwa, nie wolno wykluczać czarnych scenariuszy cyberataków związanych nawet z zagrożeniem życia - amerykańska Administracja Żywności i Leków zdecydowała się wycofać z rynku model pompy insulinowej, który ze względu na zdolność komunikowania się przez sieć i niedostateczne zabezpieczenia podatny był na ataki.

Odnośnie ryzyka w sieciach korporacyjnych, FBI przytacza przykład uzyskania kontroli nad systemem monitorującym pompę paliwa na stacji benzynowej. W tym przypadku przestępca mógłby albo spowodować przepełnienie zbiornika i wywołać w ten sposób zagrożenie pożarowe, albo przerwać połączenie z punktem sprzedaży, stwarzając możliwość pobrania paliwa bez zarejestrowania transakcji finansowej.

Szczelna ochrona rozwiązań z dziedziny Internetu Rzeczy jest niezwykle istotna w obliczu mnogości potencjalnych zagrożeń oraz rodzaju obsługiwanych danych. Ale czy w dobie coraz większej liczby produktów i ich zróżnicowania będziemy w stanie poradzić sobie z problemem standaryzacji? Należałoby podejmować działania w celu opracowania spójnego ekosystemu, w którym urządzenia o różnych funkcjonalnościach oraz pochodzące od różnych producentów będą w stanie ze sobą płynnie współpracować. Brak pewnego globalnego

zespołu standardów mógłby doprowadzić do sytuacji niemal z koszmaru, kiedy to przeciętny użytkownik musiałby poświęcić kilka dni, aby skonfigurować na nowo wszystkie inteligentne urządzenia w swoim domu po zmianie lub odłączeniu od sieci jednego z nich. A co w przypadku, gdyby zawiódł sam Internet? Czy oznaczałoby to, że nie możemy korzystać w pełni z żadnego z naszych urządzeń?

Wygląda jednak na to, że upowszechnianie się Internetu Rzeczy jest nieuchronne i będzie kształtowało biznes już w ciągu najbliższych lat. Według przedsiębiorstwa analityczno-doradczego Gartner, do 2020 roku na świecie liczba urządzeń podłączonych do sieci sięgnie 21 miliardów. Wszystkie będą stale generowały i konsumowały dane. Interesującym przykładem są samoloty brytyjskich linii lotniczych Virgin, które w ciągu jednego lotu są w stanie wyprodukować ponad 500 GB informacji. Przy 21 tysiącach lotów wykonywanych rocznie przez flotę Virgin powstanie ponad 10 mln GB danych.

Według analiz, 90 procent globalnych danych zostało zarejestrowanych w ciągu zaledwie dwóch ostatnich lat. Ważne, abyśmy przy coraz szybciej wzrastających wolumenach informacji oraz zwiększającej się liczby ich źródeł potrafili wyciągać z nich nową wartość. Z pewnością giga-dane pochodzące od wszystkich urządzeń spiętych w sieć potrafią wskazać coś, czego na pierwszy rzut oka nie widać na podstawie materiałów pozyskiwanych tradycyjnymi metodami. Są w stanie stanowić bazę do innowacyjnych metod określania nowych trendów w społeczeństwie, odkrywania sposobu postępowania klientów albo opisywania zjawisk gospodarczych.

Po wypracowaniu odpowiednich poziomów bezpieczeństwa oraz spójnych standardów systemów będziemy mogli w przyszłości w pełni czerpać z potencjału oferowanego przez Internet Rzeczy i Big Data. Niewątpliwie, szanse, które leżą w dialogu przedmiot-przedmiot oraz człowiek-przedmiot są ogromne, nie tylko z perspektywy komfortu życia prywatnych użytkowników, ale także potrzeb wielkich przedsiębiorstw i organizacji.