Internet of things - nieustanny rozwój czy łatwy cel cyberprzestępców

Inteligentne urządzenia, inteligentne domy, inteligentne miasta jaka jest wizja technologicznej przyszłości? Czy nowo budowane aglomeracje, będą w rzeczywistości działały na podstawie milionów czujników? Tak zakłada poniekąd rozwój internet of things Internetu Rzeczy. Jednak czy prostym użytkownikom może wyjść to na dobre? O tym poniżej.

Wygodna technologia

Internet Rzeczy, to koncepcja, według której najróżniejsze przedmioty mogą zostać przyłączone do sieci komputerowej (tutaj właśnie internetu) i gromadzić, przetwarzać, przesyłać dane, a także działać na podstawie ich analizy. IoT zdobywa coraz większe poparcie i wykorzystywane jest przez coraz więcej producentów nowych technologii. Założenie to może dotyczyć wielu aspektów życia, od sprzętu domowego użytku (RTV i AGD), oświetlenia, systemów zarządzania budynkami, po inteligentne przedsiębiorstwa, miasta, naszpikowane elektronicznymi czujnikami. Internet of Things, nie ma już niemal ograniczeń, stosuje się go np. w służbie zdrowia, energetyce, działaniach środowiskowych.Internetowa lista pożyczek online dla każdego

Najważniejsze są dane, nie urządzenie

Właściwa koncepcja Internetu Rzeczy nie polega jednak na tym, że urządzenie podłączone jest do sieci. Najważniejsze jest to, co robi ono ze zgromadzonymi informacjami. W jaki sposób i w jakim celu są one przetwarzane przez smart urządzenia, sensory lub całe ich systemy. Internet of Things, według założenia ma działać pożytecznie dla ludzkości, na rzecz użytkowników. Dlatego właśnie przestrzenie publiczne, domy i biura przepełnione są inteligentnymi technologiami połączonymi z siecią. Według szacunków przeprowadzonych przez International Data Corporation liczba urządzeń należących do internetu rzeczy ma wynieść aż 30 mld. Jednak wartość ta znacznie waha się w zależności od firmy analitycznej przeprowadzającej badania.

Przede wszystkim praktyczne zastosowanie

Internet of things z całą pewnością daje wiele możliwości ułatwia życie wprowadzając pewnego rodzaju wygodę, związaną z łatwą obsługą inteligentnych urządzeń i ich praktycznym wykorzystaniem. Koncepcja może być także stosowana na znacznie większą skalę, np. w Los Angeles, umieszczone w mieście czujniki używane są do analizy ruchu, kontroli sygnalizacji świetlnej, a co za tym idzie rozładowywania ruchu drogowego.

Kiedy udostępniane dane mogą być zagrożeniem

Istotną cechą, a raczej właściwością Internetu Rzeczy jest to, że nie można odłączyć go od pojęcia danych, gdyż ma on rację bytu wyłącznie na ich podstawie. Tutaj jednak pojawia się największe zagrożenie. IoT, w którym przetwarzane są setki Zettabajtów informacji, przez nieodpowiednie wykorzystanie lub brak zabezpieczeń, może stać się jednym z największych technologicznych zagrożeń.

W erze wprowadzenia Internetu Rzeczy w niemal każdą dziedzinę życia, dane przetwarzane przez smart urządzenia mogą dotyczyć życia osobistego, działania firmy, urzędu, organizacji czy nawet całych społeczności miejskich. Autonomiczne urządzenia smart analizują ogromne ilości informacji, jednak ich działanie często zależy od użytkownika. Czy tak samo jest z zabezpieczeniami technologii IoT?

- Użytkownicy bardzo często nawet nie wiedzą, jakie za pośrednictwem urządzeń typu smart udostępniają o sobie informacje. Dotyczy to zarówno technologii wykorzystywanych w przestrzeni prywatnej, jak i publicznej. Przejęcie kontroli nad tego typu nowymi rozwiązaniami, dla cyberprzestępców

nie jest nawet wyzwaniem, gdyż w dużej mierze nie posiadają one odpowiednich zabezpieczeń, a pozyskiwane dane nie są chronione. - mówi Robert Dziemianko z G DATA, producenta oprogramowania antywirusowego.

Świadome użytkowanie, świadome zabezpieczanie

Ochrona sieciowa w przypadku Internet of Things powinna stać się priorytetem. Ostatecznie przecież są to urządzenia, które często posiadają dostęp do najbardziej prywatnych informacji, zapisów medycznych czy nawet odpowiedzialne za bezpieczeństwo na drogach, jak w Los Angeles. Przejęcie kontroli przez cyberprzestępców nad systemami IoT daje im wiele możliwości, w tym zdalne przejęcie kontroli nad urządzeniami.

Jak zatem chronić dane, przetwarzane przez technologię IoT? Najważniejsze jest stosowanie odpowiednich zabezpieczeń sieci, bez względu czy jest to połączenie prywatne, czy publiczne. Drugi krok to stosowanie wszystkich dostępnych na urządzeniu zabezpieczeń, takich jak hasła, kody dostępu, wymogi autoryzacji przez SMS lub mail itd. Ostatnie co użytkownik powinien zrobić to odpowiednio skonfigurować sprzęt, tak by tworzona przestrzeń IoT, nie stała się pułapką dla danych, a technologie służyły temu, czemu powinny.

Jak pokazują wyżej przytoczone statystyki, już niedługo Internet of Things opanuje w stopniu globalnym życie każdego z użytkowników sieci. Dlatego lepiej teraz zapoznać się ze sposobami korzystania nowych technologii przedmiotowych w odpowiedzialny i niezagrażający sposób. Bagatelizowanie ochrony przestrzeni IoT, to świadome zaniedbanie, zwłaszcza w czasach gdy technologia pochłania użytkowników i przedostaje się w najbardziej prywatne strefy życia.