Nawet jeśli nie pracujesz w sektorze IT, to najpewniej nie raz słyszałeś o IoT (ang. „Internet of Things”), czyli internecie rzeczy. Pojęcie to dotyczy wszelkich urządzeń, których podstawowa funkcja jest inna niż korzystanie z internetu, jednak są one do niego podłączone, np. okulary, zegarek. Mogą być to również samochody, narzędzia kuchenne, a nawet sprzęt medyczny. Z każdym rokiem popularyzacji internetu rzeczy tych narzędzi przybywa. Dziś zegarek odbierający wiadomości SMS stał się rzeczą powszednią, jednak kolejne pomysły inżynierów są coraz bardziej niestandardowe.

Trendy rynkowe i zwrot z inwestycji

Według badań Business Insider BI Intelligence do 2020 roku na Ziemi będą już 24 miliardy urządzeń IoT.
Wtedy na jednego człowieka przypadną aż 4 urządzenia. Z kolei inwestycje w rynek IoT do 2025 roku wygenerują przychód w wysokości aż 13 trylionów $. Kto weźmie w tym udział? Takie branże jak Produkcja, Transport, Obrona, Rolnictwo, Infrastruktura, Sprzedaż, Logistyka, Bankowość, Energetyka, Ubezpieczenia, Gastronomia, Opieka zdrowotna, Nieruchomości, czyli prawie my wszyscy. Ekosystemy internet of things stworzą trzy podstawowe grupy: konsumenci, rządy oraz podmioty biznesowe.

Pionierzy internetu rzeczy

Większość międzynarodowych firm miała już styczność z internetem rzeczy, ale tylko niektóre mogą pochwalić się już sukcesami w tym temacie. Jedni z najaktywniejszych graczy na rynku to Hitachi, Cisco, Fitbit, IBM, Garmin, Google, Microsoft, z czego aż 4 z nich są dziś partnerami EIP. Oprócz hardware’u w grę wchodzi też rozwój platform przeznaczonych dla IoT. Urządzenia porozumiewają się ze sobą, używając internetu. Platformy działają jak most między ich sensorami i sieciami danych. Obecnie topowymi platformami internetu rzeczy są Microsoft Azure, IBM Watson, Cisco IoT Cloud Connect.

Bezpieczeństwo i jeszcze raz bezpieczeństwo

Wątpliwości wśród konsumentów, ale również przedsiębiorstw, budzą szczególnie takie aspekty jak bezpieczeństwo i prywatność. Utrata wrażliwych danych jest główną obawą aż 36% zainteresowanych, jak wynika z Vormetric Data Threat Report 2016.
Cyber ataki budzą obawy tym bardziej, że przybywa urządzeń podłączonych do międzynarodowej sieci.
Hakerzy mogliby zacząć penetrować krytyczną infrastrukturę, kontrolować samochody, a nawet domy prywatnych osób. Dlatego naczelnym wyzwaniem, przed jakim staną firmy

technologiczne, będzie stworzenie bezpiecznego środowiska oraz odpowiednich procedur. Artykuł powstał na podstawie materiałów anglojęzycznych autorstwa Business Insider.