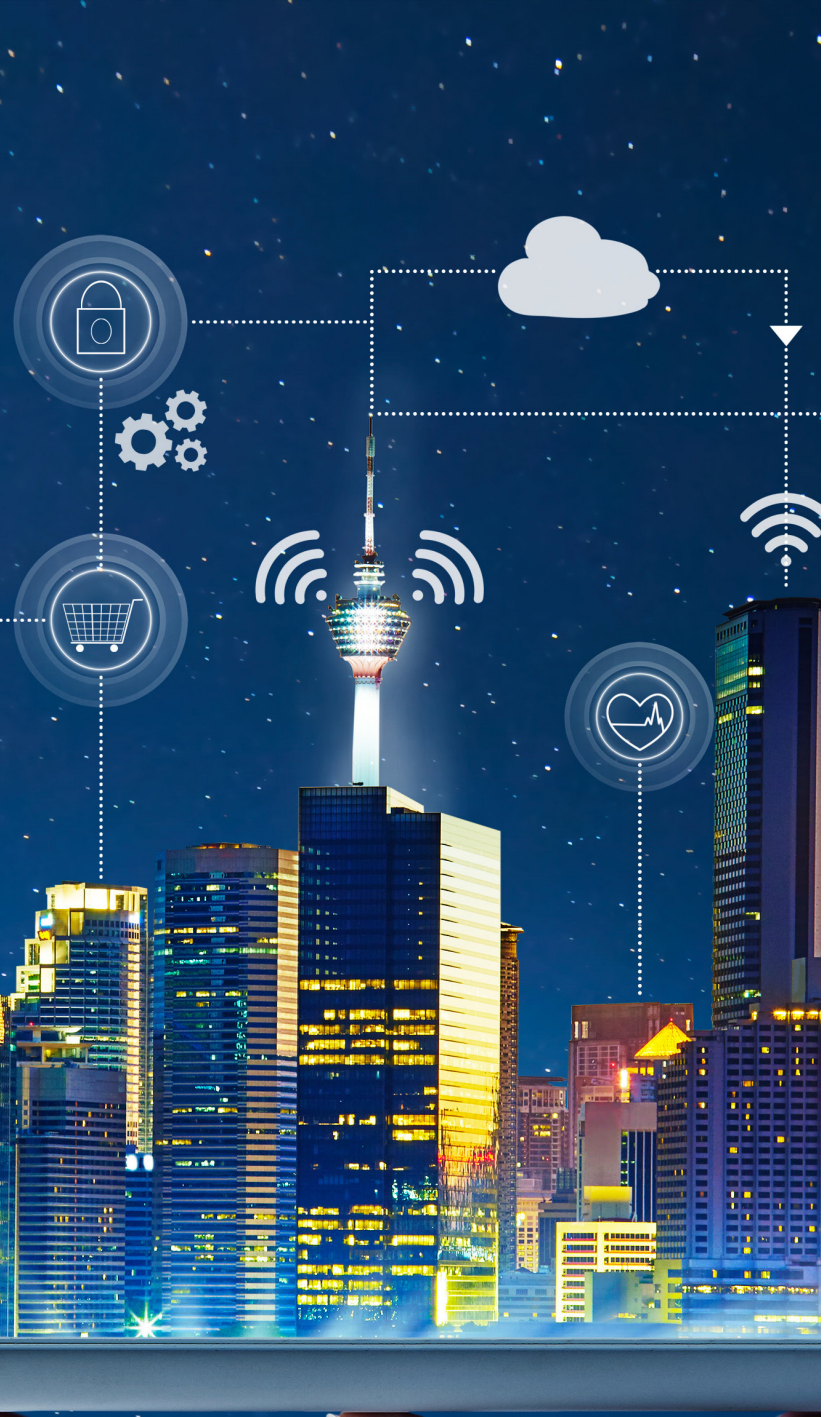

fot. © jamesteohart / Adobe Stock

Ochrona urządzeń i danych w Internecie Rzeczy

Natalie Mouyal

Włącz radio, ustaw timer na kolację, zmniejsz temperaturę, wyłącz światła. Dzięki Internetowi Rzeczy (IoT) to wszystko jest możliwe. Czynności te można wykonać siedząc wygodnie na kanapie albo jadąc autobusem.
IoT sprawia, że domy, biura i pojazdy są „inteligentniejsze, bardziej wymierne i nieformalne”.

Firma IoT Analytics szacuje, że w 2018 roku całkowita liczba urządzeń połączonych pozostających w użyciu na całym świecie przekroczy 17 miliardów; 7 miliardów urządzeń określa się jako urządzenia IoT (wyłączając smartfony, tablety, laptopy oraz telefony stacjonarne). Zakłada się, że do 2025 roku liczba urządzeń IoT osiągnie poziom 21,5 miliarda. Z kolei Business Insider szacuje, że do roku 2025 liczba urządzeń IoT w użyciu może przekroczyć nawet 55 milionów.

Definiowanie IoT

Internet Rzeczy (IoT) obejmuje każde urządzenie, które może się połączyć oraz zebrać i udostępnić dane w sieci. Generalnie, przez to pojęcie rozumie się obiekty fizyczne kontrolowane przez Internet i w jego ramach połączone. Według IEC Electropedia Internet Rzeczy to „łącznik pomiędzy łatwymi do zidentyfikowania obiektami fizycznymi (rzeczami) i usługami a wirtualnym odwzorowaniem w podobnej do Internetu strukturze". Do urządzenia fizycznego dodawana jest cyfrowa inteligencja, co pozwala na połączenie świata fizycznego z cyfrowym.

Określenie Internet Rzeczy zostało wymyślone przez managera firmy Proctor and Gamble, Kevina Ashtona, który chciał użyć znaczników RFID, aby lepiej zrozumieć łańcuch dostaw swojej firmy, a konkretniej, dlaczego pewien kolor szminki był bardzo rzadko dostępny w jego lokalnym supermarkecie. Ashton zauważa, że termin Internet Rzeczy celowo opisuje coś głębiej: „połączenie wszystkich naszych narzędzi i materiałów eksploatacyjnych".

Wszystkie rodzaje urządzeń zostały podłączone do sfery IoT, od kamer wideo i żarówek po telewizory, termostaty i opaski fitness. Urządzenia IoT mają zastosowanie nie tylko do przedmiotów codziennego użytku, lecz także do budynków, sieci transportowych i sieci energetycznych. Połączenie tych urządzeń z analizą danych może ostatecznie doprowadzić do powstania inteligentnych budynków, inteligentnych fabryk i inteligentnych miast.

Słabości urządzeń IoT

Młoda matka w Nowym Jorku przeżyła rodzicielski koszmar, gdy odkryła, że ktoś obcy rozmawiał z jej synkiem przez kamerę wideo zainstalowaną w jego sypialni. Mimo tego, że natychmiast odłączyła kamerę, to nie wiadomo, jak długo ten obcy obserwował rodzinę. To mógł być tylko żartowniś, ale równie dobrze ten człowiek mógł mieć złe zamiary.

Urządzenia połączone takie jak kamery monitoringu to pierwszy cel dla hakerów. Tak jak wiele urządzeń połączonych mają wbudowane słabe zabezpieczenia. W jednym z badań wykazano, że istnieją dwa typy kamer internetowych (obecnie około 100 000 sztuk w użyciu), do których można się z łatwością włamać.

Te słabości zabezpieczeń mogą być także wykorzystywane do włamania się do szerszej sieci. Tak było w przypadku inteligentnego termostatu w akwarium dla ryb, który cyberprzestępcy wykorzystali do włamania się do sieci kasyna i kradzieży danych, w tym danych kont bankowych klientów.

Zagrożenie stwarzane przez urządzenia IoT zostało uznane przez rządy krajowe, ponieważ konsekwencje włamania się do sieci za pośrednictwem urządzenia IoT mogą być katastrofalne. Wyobraźmy sobie szpital zmuszony do zamknięcia lub samochody, które zostały zepchnięte z drogi.

Słabe zabezpieczenia związane z urządzeniami IoT wynikają z wielu przyczyn. Obejmują one użycie domyślnych haseł, które można łatwo wykorzystać, brak mechanizmu aktualizacji oprogramowania i ograniczone zabezpieczenie systemu, takie jak możliwość zainstalowania zapór sieciowych (*firewall*) lub wyłączenia obsługi plików cookie.

Z uwagi na znaczny spadek kosztów i uproszczenie procedur tworzenia inteligentnych urządzeń, producenci mogą z łatwością oferować klientom takie urządzenia. Jednak producenci urządzeń o niskiej marży, mają niewielką motywację do utrzymania pewnego poziomu bezpieczeństwa. A jeszcze mniej będzie mieć niezbędną wiedzę w tym zakresie.

Ochrona prywatności

Urządzenia IoT gromadzą znaczną ilość danych o swoich użytkownikach. W domu dane te mogą obejmować czas pobudek i snu, filmy, które są oglądane, zakupy oraz czas, kiedy ktoś jest w domu, a kiedy nie. Asystenci uruchamiani głosowo nieustannie monitorują rozmowy i mogą rejestrować każde słowo wypowiadane w domu. Dane te mogą zostać przesłane do producenta urządzenia.

Nie jest jasne, co stanie się z tymi danymi i jak mogą zostać wykorzystane. Jednak wiele zebranych danych może stworzyć dokładny profil użytkownika, który może zostać wykorzystany w celach marketingowych lub innych. W ostatnim wystąpieniu w Parlamencie Europejskim Tim Cook (CEO firmy Apple) zauważył, że „te skrawki danych... pojedynczo niegroźne...

są ostrożnie łączone, syntetyzowane i sprzedawane. Proces ten, doprowadzony do skrajności, tworzy trwały profil cyfrowy i pozwala firmom poznać cię lepiej, niż Ty siebie".

Cook pochwalił również Unię Europejską za przyjęcie ogólnego rozporządzenia w sprawie ochrony danych (RODO), które nakłada surowe wymagania dotyczące gromadzenia, przechowywania i udostępniania danych osobowych zbieranych online. RODO obejmuje takie pojęcia, jak indywidualne „prawo do bycia zapomnianym", jak również prawo do „przenoszenia danych", które pozwala użytkownikowi na łatwe przesyłanie danych osobowych między usługodawcami.

W innych krajach działania regulacyjne mające na celu ochronę prywatności były ograniczone. Według jednego z naukowców, Bruce'a Schneiera, ekonomiczne i techniczne zachęty branży IoT nie są dostosowane do potrzeb społeczeństwa w zakresie bezpieczeństwa i prywatności. Z tego powodu uważa, że regulacje państwowe i normy są niezbędne, aby pomóc chronić obywateli.

Zapotrzebowanie na normy

Normy Międzynarodowe zapewniają solidne i niezawodne ramy, oparte na najlepszych praktykach gromadzenia, przechowywania i przetwarzania poufnych danych. W ramach Wspólnego Komitetu Technicznego ISO I IEC (ISO/IEC JTC) 1 ds. technologii informacyjnej, Podkomitet (SC) 27 (*IT security techniques*) opracował normy ISO/IEC 27000. To kompletny zestaw narzędzi i metodologii zarządzania bezpieczeństwem danych, a także najlepsze praktyki w dziedzinie bezpieczeństwa danych, wymiany informacji, ochrony i przetwarzania pamięci masowej.

JTC 1/SC 41, zajmujący się Internetem Rzeczy, opublikował niedawno swoją architekturę referencyjną.

ISO/IEC 30141 zapewnia ramy dla IoT służące za podstawę do opracowania konkretnych architektur i systemów IoT. Jednym z celów tej normy jest ochrona prywatności i gwarancja, że dane nie zostaną zhakowane. François Coallier (przewodniczący JTC 1/SC 41) uważa, że „kluczowe dla użytkowników jest poczucie, że mogą zaufać systemom Internetu Rzeczy. Wiarygodność była jednym z kluczowych pojęć, które kierowały naszą pracą w tym dokumencie". SC 41 pracuje obecnie nad dwoma innymi projektami, w których wiarygodność jest najważniejszą zasadą: podstawą wiarygodności i metodologią wdrażania i utrzymywania wiarygodności systemów Internetu Rzeczy.

Ponieważ nie wszystkie ryzyka są oparte na technologii, personel techniczny odpowiedzialny za zarządzanie danymi wymaga szkolenia oraz zwiększania wiedzy i umiejętności. Praca Komitetu ds. Oceny Zgodności (Committee on Conformity Assessment - CASCO) – wspólny wysiłek ISO i IEC – ma zasadnicze znaczenie dla procesu określania, czy organizacja spełnia wymagania związane z jej kompetencjami technicznymi w tym obszarze.

Co więcej, cyberbezpieczeństwo znajduje się w kręgu zainteresowań Grupy Roboczej (WG) 17 Rady ds. Oceny Zgodności IEC (IEC CAB) oraz Certification Management Committee Task Force w IECEE, the IEC Conformity Assessment for Electrotechnical Equipment and Components (system IEC zgodności badań i certyfikacji sprzętu elektrotechnicznego).

Źródło: IEC e-tech Magazine, Issue 6/2018
Tłum. I. P.