**Czy urządzenia IoT mogą działać bez internetu?**

**Powszechnie uważa się, że urządzenia internetu rzeczy (IoT) nie mogą funkcjonować bez połączenia z siecią globalną www – w końcu sama nazwa („internet”) na to wskazuje. Nie ma jednak prostej odpowiedzi na postawione w tytule pytanie – wszystko zależy od komunikacyjnych wymagań konkretnego gadżetu.**

Systemy IoT określane są również jako „inteligentne” i „połączone”. Jak to wyjaśniono w innym artykule, ich głównym zadaniem jest obserwowanie świata fizycznego i zbieranie informacji o otoczeniu, w oparciu o którą podejmowane są następnie decyzje lub inicjowane działania. Aby mogło to funkcjonować, niezbędny jest kanał komunikacyjny.

- *Nie wszystkie urządzenia IoT, aby działać prawidłowo, muszą być podpięte do internetu. Wszystkie jednak wymagają połączenia z innymi gadżetami tworzącymi sieć – dzięki temu można zautomatyzować pewne zadania, umożliwić użytkownikowi interakcję z urządzeniami za pomocą bezpośrednich poleceń lub konfigurować system. Natomiast podłączenie urządzeń do internetu daje możliwość sterowania nimi spoza sieci lokalnej* - **tłumaczy Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe.**

Pracująca w sieci lokalnej kamera IP może doskonale wypełniać swoje zadania, bez konieczności podłączania jej do internetu. Jeżeli jednak wymagany jest do niej dostęp z odległej lokalizacji, do utworzenia kanału komunikacyjnego potrzebna jest sieć globalna. Także poszczególne inteligentne źródła światła, tworzące sieć o topologii kratowej (ang. mesh network), mogą korzystać z różnych standardów komunikowania się między sobą, a sterująca całością jednostka nadrzędna wcale nie musi być podłączona do internetu.

Bardzo często użytkownicy, pragnący zdalnie sterować lokalnym gadżetem, podejmują ryzykowną decyzję o eksponowaniu go w internecie. Jeśli zrobione jest to nieprofesjonalnie, cyberprzestępcy również zyskują bezpośredni dostęp do urządzenia. Wykrycie takiego gadżetu i rozpoczęcie wykorzystywania go w przestępczej działalności zajmuje hakerom niespełna pięć minut.

W przypadku niektórych produktów dostęp do lokalnego urządzenia może być realizowany za pośrednictwem infrastruktury chmurowej dostawcy. Rozwiązanie takie jest bezpieczniejsze, ponieważ daje większą szansę uzyskania solidnej ochrony.