Z tym bywa jednak różnie. Szczególnie gdy co ambitniejszy prezentujący zapragnie poruszyć aspekt bezpieczeństwa i konceptu przetwarzania danych. To dwa fundamentalne i elementarne filary, bez których nie powinno się nawet rozpoczynać dyskusji. Coś, co powinno być długo i dobitnie wyjaśniane w pierwszej kolejności, zanim poruszone zostaną biznesowe hasła dotyczące skali, ustanawiania nowych norm, poprawiania jakości życia, rozwiązywania istniejących problemów społeczeństwa, optymalizacji procesów, wnoszonej innowacji i poprawionej produkcji.

Ale właśnie… bezpieczeństwo – pięta Achillesowa IoT. Czy czasem nie jest tak, że to właśnie ignorancja rodzi ignorancję? Dostrzegam pewną powtarzającą się prawidłowość w tym, że biznes i technologia nie mogą się ze sobą porozumieć, rozmawiając dwoma odmiennymi językami, a rykoszetem tego sporu dostaje końcowy konsument. Konsument, który potencjalnie ma zerową wiedzę na temat proponowanej mu technologii i rozwiązań. Klient, który żyje w utartych schematach w myśl słów wydmuszek zasłyszanych lub przeczytanych w sieci i mediach społecznościowych. Klient, który opiera decyzje o schematy, w których smart produkty stanowią błahy zakup, formę zabawki, kolejnego produktu, który można nabyć do domu bez większej rozwagi lub zastanowienia. A wszystko w imię przekonania, że są to niegroźne, interesujące drobiazgi, które nie niosą zagrożeń.

Ale czy na pewno tak jest? Czy rzeczywiście konsument powinien wykazywać tak statyczną postawę? Czy rzeczywiście nie musi się on dwukrotnie zastanowić, nim nabędzie takie cacuszko? Przeanalizujmy na przykład smart żarówkę – zdaje się najprostszy i najtańszy produkt, którym mógłby zainteresować się konsument po raz pierwszy stykający się z IoT. Szczególnie, że towar ten popularyzuje się w marketach na całym świecie sloganem „nowych doznań i oszczędności pieniędzy". A wszystko zamknięte w niewielkim i „niezbędnym" do wygodnego życia produkcie.

Bezpieczeństwo IoT – przypadek smart żarówki

Niby jest to prosta żarówka, ale jak na ironię ten prosty produkt do swego powstania może wymagać zaangażowania co najmniej czterech firm[4] – kogoś kto wyprodukuje fizyczne urządzenie, kogoś kto dostarczy firmware, firmę, która zrealizuje i utrzyma działające środowisko oraz podwykonawcę, który napisze dedykowaną aplikację mobilną. Z własnego doświadczenia wiem, że za taki kontrakt z reguły odpowiedzialne są Chiny, które wytwarzają produkt po ekstremalnie niskich cenach za jednostkę, Europa, która przygotowuje i kompiluje aplikację, ze względu na sprawdzonych specjalistów, oraz Stany Zjednoczone, które zajmują się pozostałymi tematami, o ile stosunek kosztu do zysku jest relatywnie sensowny. Samo to, że na starcie mamy już do czynienia z kilkoma firmami, które w odmienny sposób traktują koncept „prywatności" oraz „bezpieczeństwa", a które zazwyczaj spaja zewnętrzny klient, powinno wzbudzać już pewien niepokój i dyskomfort. Pozostawię jedynie do domysłu sytuacje, które generuje takie podejście, a w którym zazwyczaj wyznacznikiem jakości nie jest bezpieczeństwo w fazie projektowania (*security by design*), lecz czas wprowadzania na rynek (*time to market*). Mentalności bogatych klientów co prawda nie zmienimy, jednak warto pamiętać o tym, bądź co bądź „osobliwym" podejściu, które generuje kolejne problemy.

[4] Źródło: The State Of IoT Security, http://pepper.me/static/media/TheStateofIoTSecurity.171becc4.pdf, s. 6.