Te szczegóły zdają się umykać dystrybutorom, którzy zapominają, że w generalnym rozrachunku mało kto rozumie obszerny zasób słownictwa związanego z bezpieczną egzystencją IoT. Ataki DDoS, Jaming, exploit, botnets, man-in-the-middle, rogue HW, spearphishing, baiting – to nie są odosobnione, sporadyczne przypadki, które można zignorować i pominąć w trakcie promowania Internetu rzeczy. To nomenklatura, którą trzeba znać i na którą trzeba reagować. A przynajmniej powinniśmy spróbować, o ile dostatecznie mocno spopularyzujemy te pojęcia, by przestały brzmieć obco i złowieszczo.

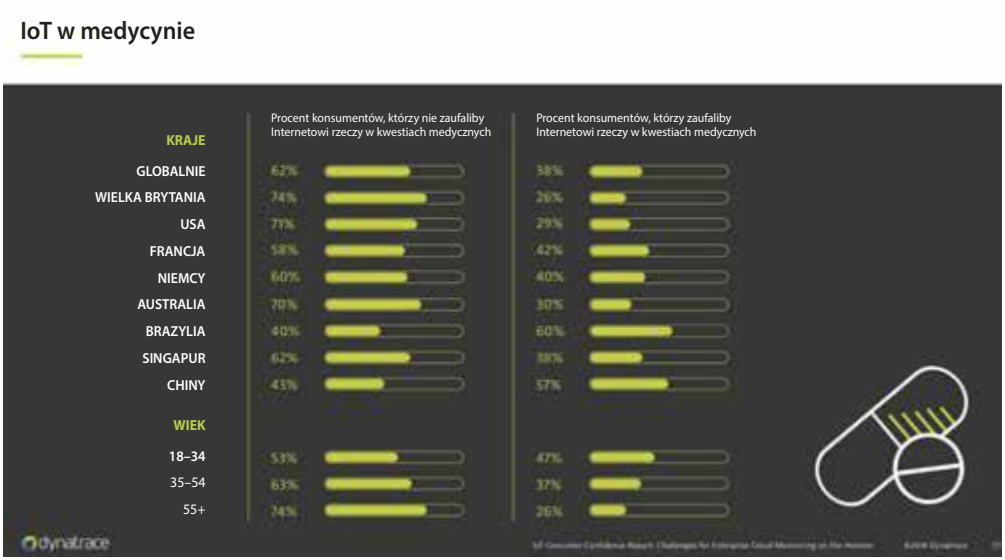
Brak zaufania

Jeśli mam być szczery – to jest moim zdaniem głównym powodem, dla którego IoT jest mylnie interpretowane, źle odbierane i nie rozumiane przez społeczeństwo (patrz rys. 8). W oczach profesjonalistów i pasjonatów, którzy znają poruszane technologie i podpatrują globalnych liderów, Internet rzeczy jest ogólnodostępnym środkiem prezentowanym z korzyścią dla wszystkich. Dla szarego obywatela jest to mało interesujące, wadliwe, niestabilne, drogie rozwiązanie, które na domiar złego jeszcze go podsłuchuje. Klient nie umie się nim posługiwać, ma problemy ze zwykłym korzystaniem, a w sytuacji krytycznej jest skazywany jest na tech banicję, bo albo kupi nowe i lepsze rozwiązanie, albo będzie miał bezużyteczną kupę plastiku w mieszkaniu. W praktyce prozaiczne i codzienne kwestie zabijają adaptację Internetu rzeczy. Masowego użytkownika nie interesuje bowiem wiele „bajerów", opcja zmieniania świata i bycia częścią rewolucji. Klient jest leniwy i najbardziej na świecie oczekuje, że rozwiązanie bezproblemowo wpisze się w jego życiową agendę.

Niestety, ale IoT nie cechuje się w stuprocentową niezawodnością. Nadal jest topornie i często nieintuicyjnie. Gama oferowanych urządzeń jest za duża i często są one projektowane bez sprawdzenia potrzeb rynku. Rozwiązania są za drogie w stosunku do rzeczywistej wartości, rynek zalewają produkty

wyglądające lub brzmiące podobnie lub, co gorsza, tajemniczo (czy klient wie, co oferuje firma oCO lub np. Zmodo?), a newsom, w których wspomniany jest akronim IoT zwykle towarzyszy słowo „kradzież", „błąd" lub „włamanie". Do tego dochodzi toporność instalacji, niska stabilność, niepełna kompatybilność i generalna niedojrzałość produktów połączona z brakiem holistycznej wizji technologicznego świata.

Sam byłem ostatnio świadkiem tego problemu, gdy „smart gimbal" do telefonów komórkowych (statyw kalibrujący obraz i reagujący na gesty dłoni) sprawił trudność moim rodzicom. Produkt ma fatalny interfejs i nie działa w pełni z Androidem (okrojone opcje), wymaga większej ilości zezwoleń w telefonie (naruszenie prywatności), nie działa stabilnie z Bluetoothem, zacinając aplikację (słabe środowisko użytkownika), a do tego dedykowana



RYSUNEK 8
Brak zaufania dla Internetu rzeczy w medycynie

Źródło: IoT Consumer Confidence Report: Challenges for Enterprise Cloud Monitoring on the Horizon, https://tinyurl.com/y2s7buya, s. 17