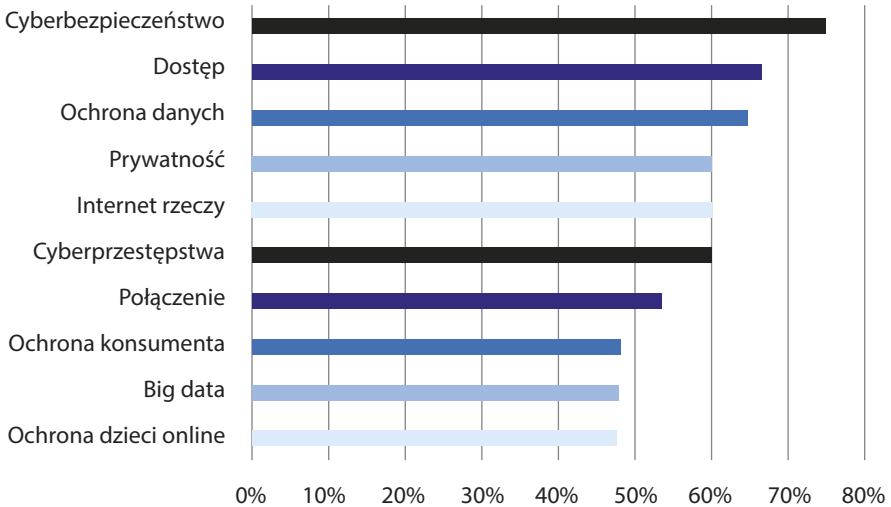
(Natural Language Understanding) – dzięki którym w jeszcze lepszy sposób dane nam będzie pracować z Internetem rzeczy. Skoro już teraz IBM Watson API umożliwia analizę zdań na podstawie zakresu emocji respondenta, a firmy pokroju Disneya wprowadzają rozwiązania stawiające na analizę emocji widzów, to kolejne rozwiązania będą jedynie kwestią czasu. Zwłaszcza że obecnie publicznie wystawione są API m.in. Microsoftu (Luis), Amazonu (Lex), czy Facebooka (wit.ai). Pozostaje jedynie zapytać – kto kolejny dołączy do tego grona?

Przyszłość IoT to… świadomość

Po piąte, aspektem, w którym pokładam gigantyczną wiarę, jest wzmocnienie świadomości i sposobów bezpieczeństwa IoT. Szczególnie będzie to istotne, gdy uzmysłowimy sobie, jak wiele włamań będzie miało miejsce na zapleczu (*backend*). Włamania i nadużycia, których jesteśmy obecnie świadkami, staną się przykrą codziennością, z którą będziemy musieli się borykać każdego niemal dnia. Scenariusze, w których potencjalny włamywacz gromadzi dane na nasz temat, identyfikuje cel, zbierając specyficzne informacje, montuje tylne drzwi (*backdoor*), aby następnie, podczas aktualizacji, zmodyfikowanym oprogramowaniem zdalnie przejąć kontrolę nad urządzeniem, będziemy traktować jak coś równie nieprzyjemnego jak wyskakujące w sieci reklamy. Najgorsze w tym wszystkim może okazać się bierne wciąż nastawienie konsumentów, którzy ulegną presji technologicznych zagrożeń – problemów będzie coraz więcej i będzie to miało większy niż dotychczas skutek. Ransomware, scareware, rootkity, malware, scareware wejdą do słownika codziennych pojęć, zastępując dotychczasową fascynację „smart" rozwiązaniami. Wycieki danych osobistych, przejęcia protokołów, porzucanie wsparcia urządzeń – każdy cios skierowany w użytkownika będzie powodować stopniową degradację zaufania. A w przypadku bezpośrednich ataków na strefę osobistą (nieautoryzowane przejęcia, phishing, spearphishing, reverse social engineering, baiting) doświadczy-

my wzrostu głosów sprzeciwu wobec istniejącego stanu rzeczy. Głosu, który oprócz dyskusji, w moim odczuciu, nie wywoła żadnej konkretnej reakcji.

Podczas gdy 80% użytkowników obecnie nie ufa rozwiązaniom IoT (dane ogłoszone podczas CES 2019), 81% jest zaniepokojonych wyciekiem ich osobistych danych, 73% obawia się ataku hakerów, a 71% wyraża troskę o bycie notorycznie monitorowanym (The Internet Society Survey on Policy Issuesin Asia-Pacific 2018), to czy możemy spodziewać się jakiejkolwiek poprawy tych wyników? (Patrz rys. 25). Jak możemy mówić, że będzie lepiej, wiedząc, że włamania staną się bardziej wyrachowane, bezpośrednie, dojrzałe i bezczelne (ukraiński VPNFilter był jednym z takich przykładów), ewoluując w swym kształcie i formie z roku na rok? Infekowane będą duże wolumeny urządzeń bezpośrednio podłączonych do sieci (IoT DDOS), a celem będzie zarówno przejęcie, jak i zastraszanie właścicieli, przejmowanie urządzeń i nadawanie



RYSUNEK 25
Obawy związane z IoT

Źródło: The Internet Society Survey on Policy Issues in Asia-Pacific 2018 , https://www.internetsociety.org/wp-content/uploads/2018/10/APAC-Internet-Policy-Survey-Report-2018.pdf, s. 7