**Okiem ekspertów: 5G „znacząco rozszerzy” pole ataku na IoT**

**Sieci 5G są coraz bliżej. Zapowiadana prędkość (do 10 Gb/s) wyznaczy dla branży nowy standard, który zastąpi powszechny obecnie LTE 4G, oferując szybszy bezprzewodowy internet dla najróżniejszych zastosowań, od autonomicznych pojazdów, poprzez inteligentne domy, aż po inteligentne miasta. Jednak 5G ma też stworzyć zupełnie nową jakość w zakresie internetu rzaczy (IoT). Według ekspertów znacznie powiększy to pole potencjalnych ataków cybernetycznych.**

- *Korea Południowa zakończyła podobno w ubiegłym miesiącu pierwsze udane wdrożenia 5G, a trzej główni dostawcy infrastruktury twierdzą, że dysponują dziesiątkami tysięcy stacji bazowych. W sektorze telekomunikacyjnym dominuje obecnie pięć firm skupiających się na technologii 5G, są to Huawei, ZTE, Nokia, Samsung i Ericson. Poza wykorzystaniem przez operatorów telefonii komórkowej, nowa technologia jest również przygotowana do zastosowania w sieciach prywatnych IoT, sieciach korporacyjnych i systemach komunikacyjnych o znaczeniu krytycznym* - **wyjaśnia Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe** (www.bitdefender.pl). - *Także w Polsce temat sieci 5G jest żywo dyskutowany. To również jeden z głównych tematów, którymi ma zająć się obecny rząd na najbliższych posiedzeniach. Chodzi mianowicie o nowelizację ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych, nazywanej potocznie “megaustawą”*.

Według przeprowadzonych w globalnej skali, przez Business Performance Innovation Network, we współpracy z A10 Networks, nowych badań ankietowych wśród specjalistów IT i kadry zarządzającej firm oferujących usługi telekomunikacyjne, łączność 5G zapewni wiele nowych rozwiązań w obszarze IoT, obejmujących zarówno potrzeby ludności jak i środowisk przemysłowych oraz korporacyjnych.

Celem raportu jest wykazanie, że w sytuacji agresywnego marketingu promującego technologię 5G, najważniejszym do rozwiązania problemem staje się bezpieczeństwo. 67% respondentów planuje wdrożenie pierwszych komercyjnych sieci 5G w ciągu najbliższych 18 miesięcy, a kolejne 20% zrobi to w ciągu dwóch lat.

94% spodziewa się, że wprowadzane urządzenia IoT, wraz aplikacjami o znaczeniu krytycznym, będą miały istotny wpływ na bezpieczeństwo i niezawodność sieci 5G, ze względu na znaczący wzrost generowanego ruchu sieciowego. Natomiast 79% twierdzi, że 5G brane jest pod uwagę w bieżących inwestycjach w bezpieczeństwo.

„Nowe aplikacje o znaczeniu krytycznym, takie jak pojazdy autonomiczne, inteligentne miasta i monitoring stanu zdrowia pacjenta sprawią, że niezawodność sieci będzie miała podstawowe znaczenie dla ochrony ludzi i gospodarki. Tymczasem gwałtowny wzrost natężenia ruchu i liczby podłączonych urządzeń znacznie zwiększy pole potencjalnych ataków i ich skalę” – powiedział Gunter Reiss, wiceprezes A10 Networks.

Jednym z podstawowych kroków w kierunku zabezpieczenia ruchu 5G będzie aktualizacja zapór sieciowych Gi/SGi. Jak dotąd zrobił to zaledwie jeden na dziesięciu operatorów.

Najważniejszymi czynnikami napędzającymi rozwój 5G są – według raportu – inteligentne miasta (60%), automatyka przemysłowa i „inteligentna produkcja” (43%), szybka łączność (39%), stała sieć bezprzewodowa (37%) i pojazdy autonomiczne (35%).

Jednocześnie największe znaczenie dla bezpieczeństwa ma zabezpieczenie warstwy rdzenia sieci oraz ochrona przed atakami DDoS. 63% respondentów uznało zaawansowaną ochronę DDoS za najważniejszą sferę bezpieczeństwa w sieciach 5G, podczas gdy prawie wszyscy (98%) respondenci stwierdzili, że zabezpieczenie warstwy rdzenia sieci jest – w przypadku wdrażania technologii 5G – bardzo ważne (72%) lub ważne (26%).