aut. Sylwia Gliwa 07.05.2021

BRYTYJSKIE WYTYCZNE OCHRONY MIAST PRZED CYBERINGERENCJĄ

Jak bezpiecznie projektować, zarządzać i budować inteligentne miasta? Brytyjskie National Cyber Security Centre opublikowało listę rekomendacji skierowanych do włodarzy miast, określających zbiór zasad bezpieczeństwa. Działania mają na celu ograniczenie potencjalnej ingerencji wrogich podmiotów.

Brytyjskie National Cyber Security Centre, mając na uwadze stały wzrost zastosowania rozwiązań z zakresu IoT, zwraca uwagę na konieczność zadbania o bezpieczeństwo miejsc publicznych. „Chociaż inteligentne miasta oferują obywatelom znaczne korzyści, są również potencjalnymi celami cyberataków" – stwierdzono w oficjalnym komunikacie do sprawy. Jeśli sieć zostanie źle zaprojektowana „naruszenie pojedynczego systemu w inteligentnym mieście może potencjalnie mieć negatywny wpływ na całą sieć". Dlatego też brytyjska służba postanowiła wydać zasady bezpieczeństwa dla władz lokalnych, mających zminimalizować ryzyko potencjalnego ataku na infrastrukturę.

Systemy miejskie mogą być atrakcyjnym celem dla szeregu podmiotów – czytamy w wytycznych sporządzonych przez Brytyjczyków. Miejsca określone jako „connected place" - wykorzystujące integrację technologii informacyjnych i komunikacyjnych oraz urządzenia IoT do gromadzenia i analizowania danych w celu budowy nowych usług i poprawy jakości obywateli. Jak wskazuje NCSC, konsekwencje naruszeń tego typu systemów mogą mieć wpływ na lokalnych mieszkańców a skutki będą różne - od naruszenia prywatności po zakłócenie lub awarię kluczowych funkcji. Pośród istotnych następstw brytyjska służba wymienia zarówno te związane z utratą reputacji jak i konsekwencjami finansowymi.

Na 16 stronach brytyjska służba wyjaśnia najważniejsze zagadnienia związane z budową i ochroną inteligentnego miasta. Autorzy raportu zwracają szczególną uwagę na systemy zarządzania sygnalizacją świetlną, CCTV (systemy monitoringów), gospodarowania odpadami, oświetleniem miejskim, parkingami i usługami transportowymi oraz usługami publicznymi.

„Chociaż korzyści te powinny zostać uwzględnione, ważne jest, aby już teraz podjąć kroki w celu zmniejszenia ryzyka cyberataków i ich potencjalnie poważnego wpływu na te wzajemnie połączone sieci. Wzywam każdą osobę i organizację tworzącą połączone miejsca w Wielkiej Brytanii do zapoznania się z naszymi nowo opublikowanymi zasadami cyberbezpieczeństwo" – stwierdził Dr Ian Levy, dyrektor techniczny NCSC. „Naszym wspólnym obowiązkiem jest zapewnienie, aby nasze miasta przyszłości były bezpieczne i odporne" – dodał w komentarzu do oficjalnego komunikatu NCBC.

Brytyjska służba jest bardzo aktywna jeśli chodzi o wydawanie wszelkiego rodzaju rekomendacji i wskazówek odnośnie budowania cyberbezpieczeństwa kraju, w tym wymiarze rządowym jak i władz lokalnych oraz obywateli. W lutym br. National Cyber Security Center opracowało i upubliczniło narzędzie do samooceny dla przedsiębiorców indywidualnych i mikroprzedsiębiorstw - „Cyber Action

Plan”. „Cyber Action Plan” został stworzony aby pomóc małym firmom chronić się przed rosnącymi zagrożeniami pochodzącymi z cyberprzestrzeni. Narzędzie ma służyć do samooceny bezpieczeństwa cybernetycznego i jest skierowane głównie do osób prowadzących jednoosobową działalność gospodarczą oraz mikroprzedsiębiorców. Bezpłatna usługa online ma zapewnić porady dotyczące oprogramowania Cyber Aware dostosowane do indywidualnych potrzeb. „Chcemy, aby Wielka Brytania była najlepszym miejscem na świecie do prowadzenia interesów online” – wskazała wtedy służba w komunikacie do sprawy.

Czytaj też: Brytyjska platforma do walki z cyberoszustami odnotowała sukces

Czy działalność brytyjskiej National Cyber Security Center sprzyja budowaniu cyberbezpieczeństwa kraju i to zaczynając od jego podstaw? Warto wspomnieć chociażby o platformie „The Suspicious Email Reporting Service” za pomocą, której Brytyjczycy w zaledwie dwa tygodnie od jej uruchomienia przesłali ponad 160 000 podejrzanych wiadomości e-mail, umożliwiając tym samym zamknięcie prawie 400 stron, za pomocą których działali cyberoszuści. Dużą promocję usługi zrobił popularny program telewizyjny. Jednak wykorzystywanie narzędzia przez obywateli w takiej skali świadczy o dużym zaufaniu do administracji oraz o silnym zaangażowaniu obywateli w budowanie bezpieczeństwa. Czy na podobne rozwiązanie możemy liczyć w Polsce? Z pewnością brakuje nam zarówno służby na miarę NCBC w takim stopniu zajmującej się cyberbezpieczeństwiem, jak i zaufania obywateli do rozwiązań proponowanych przez państwo.