„Inteligentne miasta” to zagrożenie dla bezpieczeństwa

11 marca 2023

Kanadyjskie służby wywiadowcze ostrzegają, że innowacje technologiczne tzw. smart cities wprowadzane przez władze municypalne mogą zostać wykorzystane przez przeciwników, takich jak chiński rząd, do zbierania wrażliwych danych, atakowania diaspory i ingerowania w wybory.

Niedawno opublikowany raport Canadian Security Intelligence Service wzywa decydentów i branżę technologiczną do rozważenia kroków, które można podjąć w celu zaradzenia i złagodzenia pojawiających się zagrożeń, zanim platformy „inteligentnych miast” zostaną powszechnie przyjęte.

Takie systemy obejmują elektronicznie połączone urządzenia, które gromadzą, analizują, przechowują i przesyłają informacje za pośrednictwem scentralizowanych platform. Z kolei władze municypalne mogą wykorzystywać sztuczną inteligencję do sprawnego kontrolowania operacji i usług, umożliwiając im zmianę sygnalizacji świetlnej w optymalnym czasie, zarządzanie zużyciem energii czy śledzenie lokalizacji rowerów wypożyczonych publicznie. „Jednym z głównych problemów bezpieczeństwa związanych z inteligentnymi miastami jest fakt, że wymagają one selekcji i przechowywania ogromnych, stale przetwarzanych pul danych, które można wykorzystać do ujawnienia wzorców zachowań indywidualnych i społecznych” – czytamy w raporcie. „Obawy te potęguje brak kontroli i wglądu w to, gdzie przechowywane są te dane i kto ma do nich dostęp”.

Raport CSIS, przygotowany w 2021 r., został dopiero niedawno udostępniony „The Canadian Press” w odpowiedzi na prośbę o dostęp do informacji złożoną w październiku tego roku.

Chociaż integracja innowacji technologicznych i danych może usprawnić procesy, może również wprowadzić zagrożenia

bezpieczeństwa, ostrzega CSIS. „Inteligentne urządzenia miejskie gromadzą ogromne ilości danych osobowych, w tym dane biometryczne i inne informacje podkreślające wybory i wzorce życia osobistego. Wrogie podmioty państwowe badają obecnie różne sposoby uzyskania dostępu do przyszłych platform inteligentnych miast, w tym poprzez dostęp oferowany przez państwowe lub powiązane z państwem firmy technologiczne".

Kanadyjskie miasta mogą podejmować partnerstwa technologiczne z zagranicznymi firmami, które umożliwiają wrogim lub niedemokratycznym państwom dostęp do gromadzenia danych, ostrzega CSIS.

Projekty inteligentnych miast w krajach zachodnich spotkały się z mieszanym przyjęciem ze względu na obawy dotyczące prywatności, ale Chiny „całym sercem przyjęły tę koncepcję", zapewniając ich firmom technologicznym przewagę konkurencyjną, czytamy w raporcie. Przewaga sztucznej inteligencji Made in China polega na dostępie do dużych zbiorów danych, braku ochrony prywatności i taniej sile roboczej do kategoryzowania danych i tworzenia algorytmów AI.

Chiny używają nowych technologii do wspierania „cyfrowego autorytaryzmu", wykorzystania zaawansowanej technologii do monitorowania, represjonowania i manipulowania populacjami krajowymi i zagranicznymi, twierdzi CSIS.

Tymczasem w nadchodzącej dekadzie sieci nowej generacji prawdopodobnie zostaną głęboko osadzone w miejskiej infrastrukturze krytycznej, zwiększając możliwość dostępu „tylnymi drzwiami", czytamy w raporcie, narażając wszystkie urządzenia na zakłócenia pracy lub ataki. „Innymi słowy, dane zebrane za pośrednictwem aplikacji do udostępniania rowerów mogą teoretycznie zwiększyć dostęp do innych podłączonych urządzeń, takich jak miejska sieć energetyczna, zaopatrzenie w wodę lub baza danych zarządzania sygnalizacją świetlną" – czytamy. „Tego rodzaju narażenie będzie miało poważne konsekwencje finansowe, społeczne oraz zdrowotne dla

bezpieczeństwa kraju. Wyobraźmy sobie scenariusz, w którym skoordynowany cyberatak usuwa blokady bezpieczeństwa, które zapobiegają katastrofalnym eksplozjom w zakładzie petrochemicznym, jednocześnie kontrolując sygnalizację świetlną w celu zahamowania reakcji kryzysowej".

Według raportu legalny dostęp do danych może odbywać się na podstawie umów między miastami i firmami, podczas gdy nielegalny dostęp może mieć miejsce wewnętrznie za pośrednictwem wbudowanej funkcji obcego sprzętu lub oprogramowania, lub na zewnątrz w wyniku cyberataku. Dane mogą być następnie wykorzystane do ukierunkowania na określone elementy społeczeństwa kanadyjskiego, takie jak społeczności chińskiej diaspory, infrastruktura, taka jak elektrownie gazowe, stacje uzdatniania wody i bazy danych rządu centralnego, demokratyczne procesy polityczne, takie jak wybory, lub grupy społeczeństwa obywatelskiego w celu ograniczenia debaty publicznej i wolność słowa, dodaje.

Wykorzystywanie technik zbierania danych przez kraje takie jak Chiny, Iran i Rosja do śledzenia populacji diaspory, a mianowicie osób uważanych za przeciwników, jest prawdziwym problemem, ostrzega David Murakami Wood, profesor Uniwersytetu w Ottawie, który specjalizuje się w inwigilacji, bezpieczeństwie i technologii. „Nie ma neutralnych danych" – powiedział w wywiadzie.

Murakami Wood ostrzegł przed przekonaniem, że dane są w jakiś sposób bezpieczniejsze, jeśli są w kanadyjskich rękach „Możesz być pewien, że jeśli zostanie zbudowana na przykład ogólnokrajowa baza danych o bardzo dużej skali, policja prędzej czy później będzie chciała uzyskać do niej dostęp. I wymyślą argument, dlaczego powinni go otrzymać".

Chociaż połączenie niektórych usług miejskich ze światem online ma sens, inne, takie jak szpitale, mogą być po prostu zbyt wrażliwe, aby ryzykować połączenie ich z cyberprzestrzenią, uważa Murakami Wood. „Jeśli naprawdę chcemy

mieć bardzo inteligentne miasta, powinniśmy przede wszystkim pomyśleć o tym, czego nie chcemy w nich łączyć”.

Autorstwo: Andrzej Kumor
Źródło: Goniec.net