Problemy Zarządzania, vol. 15, nr 4 (71): 41–53
ISSN 1644-9584, © Wydział Zarządzania UW
DOI 10.7172/1644-9584.71.3

Zastosowania koncepcji Internetu rzeczy w kontekście inteligentnego miasta. Wybrane zagadnienia bezpieczeństwa

Nadesłany: 07.09.17 | Zaakceptowany do druku: 24.11.17

Artur Rot*

Miasta, chcąc być coraz bardziej przyjazne dla mieszkańców oraz coraz sprawniej zarządzane, wykorzystują na te potrzeby różne nowoczesne rozwiązania teleinformatyczne. W ten sposób wdrażana jest w życie idea inteligentnego miasta (ang. *smart city*), wykorzystująca m.in. systemy Internetu rzeczy (ang. *Internet of Things*, IoT), które będą stawać się kluczowym narzędziem usprawniającym funkcjonowanie aglomeracji miejskich. Koncepcja Internetu rzeczy rozwija się bardzo dynamicznie i stwarza ogromne możliwości dla inteligentnych miast. Oprócz korzyści, jakie przynosi, przynosi jednak też poważne zagrożenia, przede wszystkim dla prywatności i ochrony danych osobowych. Jej zastosowania usprawniają nasze życie, ale stwarzają nowe formy ryzyka i stanowią wyzwanie dla architektów systemów bezpieczeństwa. Celem artykułu jest przegląd wybranych przypadków użycia Internetu rzeczy w kontekście koncepcji inteligentnego miasta oraz opis zagrożeń dla cyberbezpieczeństwa, wynikających z poszerzania dostępu do sieci nowych urządzeń w tym obszarze.

Słowa kluczowe: Internet rzeczy, inteligentne miasta, cyberbezpieczeństwo, zagrożenia, podatności.

The Applications of the Internet of Things in the Context of the Smart City. Selected Security Issues

Submitted: 07.09.17 | Accepted: 24.11.17

Wishing to be more friendly to their citizens and to be managed more efficiently, cities are using a variety of modern ICT solutions for their needs. In this way, the smart city concept is being implemented, using, among others, the Internet of Things (IoT), which will become a key tool to improve the functioning of urban agglomerations. This idea develops very dynamically and creates tremendous opportunities for smart cities. But in addition to the benefits it brings, it also creates serious threats, primarily for privacy and personal data protection. Its applications improve our lives but also create new forms of risk and become the challenge for security architects. The purpose of this paper is to review selected applications of the Internet of Things in the context of the smart city and to describe the cybersecurity threats resulting from widening access of new devices to the network in this area.

Keywords: Internet of things, smart city, cybersecurity, threats, vulnerabilities.

JEL: O32, O33, O18

* **Artur Rot** – dr, Katedra Systemów Informacyjnych, Wydział Zarządzania, Informatyki i Finansów, Uniwersytet Ekonomiczny we Wrocławiu.

Adres do korespondencji: Katedra Systemów Informacyjnych, Wydział Zarządzania, Informatyki i Finansów, Uniwersytet Ekonomiczny we Wrocławiu, ul. Komandorska 118/120, 53-345 Wrocław; e-mail: artur.rot@ue.wroc.pl.

1. Wprowadzenie

Inteligentne miasta są efektem postępującej rewolucji informacyjnej, która wiąże się z wykorzystaniem innowacyjnych rozwiązań teleinformatycznych. Z danych Schneider Electric wynika, że obecnie miasta zajmują jedynie 2% powierzchni Ziemi, ale mieszka w nich ok. 54% światowej populacji. Szacuje się, że do 2045 roku w miastach będzie mieszkać aż 70% wszystkich ludzi (Gazeta Prawna, 2016).

Systemy nawigacji samochodowej analizujące natężenie ruchu, kamery wykrywające śmieci w miejscach publicznych czy samoregulujące się systemy lamp ulicznych to tylko kilka rozwiązań implementowanych w inteligentnych miastach, wykorzystujących technologię Internetu rzeczy (ang. *Internet of Things*, IoT), który jest połączeniem urządzeń w sieć, tak aby umożliwić ich zdecentralizowaną komunikację między sobą. Koncepcja ta opiera się na stałym postępie technologicznym i związana jest z istnieniem globalnej sieci łączącej wiele urządzeń i czujników, które potrafią samodzielnie wymieniać się informacjami (Rot, 2016). Oczekuje się, że IoT znajdzie wiele zastosowań w różnych dziedzinach, m.in. właśnie w inteligentnych miastach, energetyce, transporcie, przemyśle, budownictwie, logistyce, opiece zdrowotnej i wielu innych. Według prognoz firmy Gartner, w 2020 r. do Internetu podłączonych będzie 26 mld urządzeń, co oznacza ogromny przyrost ilości danych, które trzeba będzie odpowiednio przechowywać i przetwarzać w chmurze (Middleton, Kjeldsen i Tully, 2013; Rot, 2017). Przewiduje się, że szczególnie dynamiczny postęp będzie miał miejsce w przypadku zastosowań tej koncepcji w aglomeracjach miejskich. Według danych firmy Navigant Research do 2023 roku rynek inteligentnych miast może być warty nawet 27,5 miliarda dolarów rocznie.

Zastosowania koncepcji Internetu rzeczy w miastach usprawniają nasze życie, ale stwarzają zupełnie nowe zagrożenia i stanowią jednocześnie znaczące wyzwanie dla architektów systemów bezpieczeństwa. Pewne jest, iż w rozwoju koncepcji inteligentnych miast będziemy mieli do czynienia z coraz większą ilością generowanych, przetwarzanych i przechowywanych danych. Niestety tego typu dane będą również atrakcyjnym celem dla cyberprzestępców. Eksperci uważają, że nowe urządzenia dają hakerom mnóstwo nowych możliwości i furtek dla ewentualnych cyberataków. Cyberprzestępcy z łatwością wykorzystają luki w urządzeniach IoT, a to niesie poważne ryzyko dla organizacji i samorządów planujących wdrożenie tych technologii. Wśród najczęstszych zagrożeń i podatności IoT wymieniane są problemy z prywatnością danych, słabe punkty w systemach autoryzacji i uwierzytelnienia, niezabezpieczone interfejsy, luki i błędy w oprogramowaniu.

Celem artykułu jest wprowadzenie do koncepcji Internetu rzeczy, przedstawienie potencjału jej zastosowań w kontekście inteligentnego miasta, ale przede wszystkim identyfikacja i analiza zagrożeń dla cyberbezpieczeństwa

 DOI 10.7172/1644-9584.71.3

wynikających z dostępu do Internetu nowych urządzeń i procesów w ramach IoT, które pierwotnie nie były do tego przystosowane.

2. Idea inteligentnych miast

Badania nad strukturą przestrzenną oraz gospodarczą miast coraz częściej wskazują na nowe czynniki rozwoju, do których należą między innymi zaawansowane technologie, niezmiernie ważne w rozwoju miast, dające nowe możliwości, a także pozwalające m.in. na oszczędności czasu i energii. Współczesne miasto to już nie tylko jego struktura fizyczna, ale także ogromna sieć nowoczesnych technologii, dążących do zoptymalizowania zużycia zasobów miasta oraz procesów zapobiegania negatywnym efektom, wynikającym z jego funkcjonowania. W ostatnich latach pojawiły się koncepcje zmierzające do oszczędności zasobów, planowania przestrzennego oraz sieci transportowych, aby uniknąć wzrostu kosztów wynikających z powiększania się miast. Coraz częściej miasta zaawansowane technologicznie określa się jako miasta inteligentne (ang. *smart cities*), w których dąży się do oszczędności wszelakich zasobów, w tym finansowych, czasu czy energii (Stawasz, Sikora-Fernandez i Turała, 2012).

Koncepcja *smart city* jest jednym z najważniejszych i najsilniej rozwijanych kierunków zmierzających do poprawy jakości życia mieszkańców, a tym samym konkurencyjności miast (Nowicka, 2014). Idea ta to inteligentne zarządzanie wspólną przestrzenią miejską przez władze miasta, obywateli oraz przedstawicieli przemysłu nowych technologii. S*mart cities* to miasta, które, wykorzystując technologie informacyjne i komunikacyjne, są bardziej inteligentne i efektywne w wykorzystaniu zasobów, a w wyniku oszczędności kosztów i energii poprawiają się warunki realizacji usług i jakości życia mieszkańców. Zmniejsza się także negatywne oddziaływanie na środowisko naturalne poprzez wykorzystanie innowacji (Cohen, 2012). W literaturze przedmiotu coraz częściej obecne są również inne określenia takich miast, takie jak: *intelligent city*, *innovative city*, *e-city*, *the creative city*, *digital city* czy *resilient city* (Wiśniewski, 2013).

W tworzeniu inteligentnych miast dużą rolę odgrywa koncepcja Internetu rzeczy. Systemy inteligentnego oświetlenia, redukcji emisji CO_2 czy inteligentna gospodarka odpadami, to tylko kilka przykładów systemów, w których stosuje się tę technologię. Idea ta rozwija się dynamicznie i stwarza ogromne możliwości dla inteligentnych miast.

Internet rzeczy może też wpłynąć na poprawę jakości życia ludzi, którzy będą mogli wykonywać zdalne płatności, sprawdzać dostępność miejsc parkingowych, a inteligentne systemy zarządzania odpadami, energią, transportem czy ruchem ulicznym staną się powoli codzienną rzeczywistością współczesnych miast (EY, 2015).

3. Koncepcja Internetu rzeczy

Zachodzące obecnie zmiany w sferze technologii i transmisji danych, wpływające m.in. na rozwój Internetu rzeczy, przez wielu określane są często jako czwarta rewolucja przemysłowa. O Internecie rzeczy można mówić od momentu, w którym liczba rzeczy i obiektów podłączonych do Internetu przekroczyła liczbę ludności (Evans, 2011). W 2000 r. na świecie było 500 mln urządzeń podłączonych do sieci, na początku 2009 r. liczba ta przekroczyła już liczbę mieszkańców Ziemi. W 2011 roku, dzięki popularyzacji smartfonów, tabletów i innych urządzeń mobilnych, liczba urządzeń podłączonych do Internetu wyniosła ponad 13 mld (liczba ludności osiągnęła 7 mld) (Raymond, 2014). Firma Gartner szacuje, iż w 2020 roku IoT będzie dotyczył ponad 26 mld. urządzeń (Middleton i in., 2013). Oczekuje się, że IoT znajdzie wiele zastosowań w różnych dziedzinach, m.in. w inteligentnych miastach, energetyce, transporcie, przemyśle, budownictwie, logistyce, opiece zdrowotnej, sektorze IT.

Lp.	Kontekst	Opis i przykłady wykorzystania
1.	Miasto	Środowisko miejskie z publiczną infrastrukturą, np. inteligentne parkometry, kontrola jakości wody czy świateł ulicznych.
2.	Człowiek	Przedmioty do połknięcia i noszenia powiązane z monitorowaniem i polepszaniem zdrowia, samopoczucia i produktywności, np. inteligentne tabletki, monitory pracy serca, opaski fitness.
3.	Środowisko pracy	Zorganizowane miejsca pracy, takie jak plac budowy, górnictwo, wydobycie minerałów, np. systemy monitorowania warunków pracy.
4.	Dom	Domy i rezydencje, np. inteligentny dom, systemy zabezpieczeń.
5.	Handel i usługi	Miejsca sprzedaży i oferowania usług, takie jak hotele, restauracje, banki, sklepy itp. Przykładem są promocje oparte na lokalizacji.
6.	Środowisko produkcyjne	Środowisko produkcji, takie jak fabryki, farmy, np. samojeżdżące wózki widłowe.
7.	Transport	Osobiste środki lokomocji, takie jak samochody, motory, rowery, np. nawigacja, unikanie kolizji, samojeżdżące samochody itp.
8.	Biuro	Budynki komercyjne i biurowe, np. inteligentne termostaty i klimatyzatory.
9.	Świat zewnętrzny	Wszystkie inne środowiska zewnętrzne poza wymienionymi powyżej, zdefiniowane jako przestrzeń powietrzna i kosmiczna, logistyka itp., np.: zarządzanie lokalizacją floty.

Tab. 1. Przegląd najważniejszych obszarów występowania Internetu rzeczy. Źródło: opracowanie własne na podstawie Rot i Blaicke (2016).

 DOI 10.7172/1644-9584.71.3

Internet rzeczy może być zdefiniowany jako ogół inteligentnych przedmiotów, mogących reagować na środowisko oraz przetwarzać informacje, a także przesyłać je do innych obiektów (i użytkowników) za pośrednictwem protokołów internetowych (Nowakowski, 2015). Obszarów jego zastosowania może być wiele (zob. tabela 1) oraz mogą one przenikać wiele aspektów życia. Nie jest to koncepcja przyszłości, gdyż jest już w pewnym zakresie aktualnie realizowana.

Oczekiwania na szybki rozwój Internetu rzeczy są powiązane także z zastosowaniami tej technologii w inteligentnych miastach, inteligentnym budownictwie i samochodach oraz w automatyce przemysłowej określanej mianem przemysłu 4.0. W dalszej części artykułu syntetycznie scharakteryzowane zostaną wybrane obszary zastosowań Internetu rzeczy na tle koncepcji inteligentnego miasta. Podane zostaną przykłady realizacji omawianej koncepcji w praktyce, przykłady ataków oraz najważniejszych zagrożeń.

4. Zastosowania Internetu rzeczy w kontekście inteligentnego miasta

Systemy IoT będą się stawać kluczowym narzędziem komunikacji między firmami i ich klientami, a także w znacznym stopniu pomogą usprawnić funkcjonowanie aglomeracji miejskich. Znaczenie tego kontekstu podnosi fakt, że coraz większa część populacji ulega urbanizacji i jak wspomniano na początku artykułu, do roku 2045 prawie 70% ludzkości będzie mieszkać w miastach, więc liczba osób obcujących z tą technologią będzie ogromna.

IoT już przynosi wymierne korzyści wielu miastom na świecie, a metropolie takie jak Los Angeles odnotowują znaczące oszczędności. W mieście tym, po zastosowaniu inteligentnego oświetlenia ulicznego, odnotowano oszczędność energii na poziomie powyżej 60%. Inne miasta osiągnęły znaczne oszczędności, wdrażając np. inteligentne rozwiązania w zakresie gospodarki odpadami, redukując emisję dwutlenku węgla czy zwiększając satysfakcję obywateli dzięki inteligentnemu parkowaniu i zarządzaniu ruchem (Polski, 2017).

Przykłady na zastosowanie omawianej koncepcji IoT w miastach można mnożyć. Jedno z praktycznych wdrożeń IoT to czujniki instalowane na kontenerach ze śmieciami, co pozwala na zdalne monitorowanie stanu ich wypełnienia. Dzięki temu przedsiębiorstwa zajmujące się gospodarką odpadami komunalnymi mogą optymalizować trasy przejazdów śmieciarek, oszczędzając czas i paliwo. Przykładem takiego systemu jest BigBelly. Jest to zasilany energią słoneczną zbiornik na śmieci z ich zagęszczarką, wyposażony w system czujników, który ostrzega ekipy sanitarne, gdy zbiornik jest pełny. Instytucje zarządzania odpadami wykorzystują historyczne dane zbierane z każdego pojemnika do planowania działalności związanej z odbiorem śmieci oraz do wprowadzania usprawnień, takich jak dostosowanie rozmiaru pojemników w konkretnych lokalizacjach (Castro i Mistra, 2012).

Inny przykład to wykorzystanie przez aglomeracje systemów przeciwpowodziowych, opartych na specjalnych czujnikach i kontrolerach podłączonych bezprzewodowo do sieci, do monitorowania stanu rzek i zbiorników wodnych, a także pomiarów czystości wody. Sensory i mikrokontrolery montowane na rurach miejskich wodociągów i sieci kanalizacyjnych pomagają w kontrolowaniu jakości wody i wykrywaniu nieszczelności (Intel, 2016).

Kolejny system – Air Quality Egg – to zespół urządzeń, który wykorzystuje czujniki to zbierania i udostępniania danych o jakości powietrza w różnych punktach miasta. Podczas gdy urządzenia instytucji zajmujących się tym problemem monitorują poziom zanieczyszczenia w centralnych punktach metropolii, Egg zbiera dane w czasie rzeczywistym z najbliższego otoczenia użytkowników (przy ich mieszkaniach, biurach itp.). Stacja bazowa przesyła dane o jakości powietrza przez Internet, gdzie strona internetowa agreguje i wyświetla dane z każdego czujnika. Dane te mogą być wykorzystane do projektowania i pomiaru efektów polityki walki z zanieczyszczeniem powietrza w różnych częściach miasta. Systemy te można spotkać w krajach Ameryki Północnej, Europy Zachodniej i Azji Wschodniej (Castro i Misra, 2013; Metcalfe, 2012).

Jak pokazują analizy i badania, znacząca część spowolnienia ruchu miejskiego na ulicach miast jest generowana przez kierowców poszukujących miejsc parkingowych (Shoup, 2007). Inteligentnym rozwiązaniem tego problemu jest system ParkSight. Jest to sieć bezprzewodowych czujników parkowania, informujących w czasie rzeczywistym o dostępności indywidualnych miejsc parkingowych. Czujniki parkowania są montowane w chodniku lub nad nim. Zebrane dane udostępnia się kierowcom oraz operatorom obiektów parkingowych. Parkingi lub garaże miejskie mogą używać cyfrowych wyświetlaczy, informujących, ile miejsc jest wolnych i na którym poziomie. Kierowcy mogą również przy użyciu aplikacji mobilnej zlokalizować dostępny parking. Funkcjonalność ta może być zintegrowana w systemach nawigacyjnych. Dzięki temu kierowcy mogą zobaczyć, ile będzie kosztować parking, jak długo będą mogli tam pozostawić auto, oraz dokonać zdalnej płatności. Urzędnicy miejscy mogą również używać systemu do egzekwowania naruszeń parkowania oraz do planowania potrzeb parkingowych w przyszłości (Castro i Misra, 2013).

Z ruchem miejskim związane są również czujniki drogi HiKoB, będące kompaktowymi, energooszczędnymi, bezprzewodowymi czujnikami, które mogą być osadzone w jezdni, w celu pomiarów parametrów takich jak temperatura, wilgotność i natężenie ruchu. Dane czujnika są przesyłane przez sieć bezprzewodową do serwera w celu przetwarzania i analizy. Następnie system dostarcza w czasie rzeczywistym informacje o warunkach drogowych. Te informacje pozwalają służbom drogowym na np. odpowiednie działania w trudnych warunkach pogodowych. System może również ostrzegać kierowców o potencjalnych zagrożeniach drogowych lub korkach (Castro i Misra, 2013). W Holandii została oddana do użytku droga pokryta powłoką czułą

 DOI 10.7172/1644-9584.71.3

na temperaturę. W razie spadku temperatury poniżej zera na drodze pojawiają się interaktywne znaki w kształcie płatków śniegu, co ma ostrzegać kierowców przed śliską nawierzchnią. Pojawiają się one w trudnych warunkach atmosferycznych, znacznie lepiej przyciągając uwagę kierowców niż tradycyjne znaki drogowe, przez co mają znaczny wpływ na bezpieczniejszą jazdę (Brachman, 2013).

Przedsiębiorstwo publicznych usług autobusowych w St. Louis (stan Missouri) wykorzystuje elektroniczne czujniki na autobusach w celu zbierania danych dotyczących parametrów takich jak prędkość, temperatura silnika i ciśnienie oleju. Komputery analizują dane i generują rekomendacje dla serwisantów, pomagając poprawić niezawodność miejskiego systemu transportowego i obniżyć koszty operacyjne. Korzystając z analityki predykcyjnej, zmniejszona została ilość potencjalnych awarii i przestojów, wydłużono czas eksploatacji pojazdów, dzięki czemu poczyniono duże oszczędności (Courtney, 2011).

W 2012 roku miasto Amsterdam we współpracy z firmami Cisco oraz Philips zainstalowało inteligentny system oświetlenia ulicznego. Każda z lamp została wyposażona w sensory i jest w stanie automatycznie raportować problemy związane z prawidłowym działaniem, automatycznie planuje okresowe przeglądy w taki sposób, aby jak najmniej zakłócać ruch, przeprowadza automatycznie ściemnianie, gdy nie ma dużego natężenia ruchu itp. Obecnie mówi się już o wykorzystaniu sieci, która powstała dzięki połączeniu oświetlenia ulicznego do innych usług publicznych (Mitchell, Villa, Stewart-Weeks i Lange, 2013), a sam Amsterdam jest jednym z liderów w drodze do inteligentnego miasta, charakteryzującego się zrównoważonym modelem przestrzeni publicznej z udziałem nowoczesnych technologii.

Jak widać, przykładów zastosowań omawianej koncepcji w kontekście miasta jest wiele. Z ideą *smart city* wiąże się też pojęcie *smart grid*, tj. systemów elektroenergetycznych, gdzie zasada działania jest analogiczna jak w przypadku interakcji między miastami. Chodzi o dostarczanie usług energetycznych przy jednoczesnym obniżaniu kosztów i zwiększeniu efektywności (Nylec, 2012). Prowadzone są prace zmierzające do wdrożenia nie tylko systemów zasilania, ale również inteligentnych systemów logistycznych, inteligentnych systemów racjonalizacji zużycia zasobów poszczególnych miast. Jedno z pierwszych wdrożeń stanowi *SmartGridCity*, w Boulder, w stanie Colorado. Koncepcja ta obejmuje cztery główne elementy: infrastrukturę inteligentnej sieci zasilania, inteligentne liczniki energii (ang. *smart metres*), inteligentne urządzenia domowe i witrynę sieci Web. W Polsce przykładem może być Bielsko-Biała, gdzie od kilkunastu lat stawia się na unowocześnianie sieci energetycznej. W drodze realizacji projektu efektywności energetycznej wdrożono np. energetyczny monitoring szkół i budynków użyteczności publicznej (Nylec, 2012; Wiśniewski, 2013).

5. Przykłady potencjalnych zagrożeń w kontekście miasta

Ataki na Internet rzeczy, który jest elementem koncepcji *smart city*, czy na większą skalę całych państw, może przynieść bardzo dotkliwe konsekwencje. Dzieje się tak dlatego, że poprzez atak na taki system atakujący są w stanie spowodować znaczące utrudnienia lub straty na dużym obszarze geograficznym. Przykładowo: w przypadku ataków na inteligentne liczniki możemy wyróżnić następujące ataki i zagrożenia (Rot i Blaicke, 2016):

- nielegalna modyfikacja, która – jeśli jest udana – pozwala na włamanie do urządzenia i zmianę wskazania lub poprzez atak *Man-in-the-middle* na zmianę przesyłanego wskazania licznika do dostawcy usługi,
- wykorzystanie aktualnego poziomu poboru prądu przez grupy przestępcze do określenia, czy i kiedy domownicy przebywają w domu, co w przypadku włamania do systemu pozwala w krótkim czasie sprawdzić setki, a nawet tysiące mieszkań na danym obszarze,
- sam fakt wykorzystania sposobu łączności i uwzględniania inteligentnych liczników w sieci domowej również stanowi zagrożenie. Włamanie do takiego licznika oznacza włamanie do wnętrza domowej sieci, więc byłoby równoznaczne z pozwoleniem na przyłączenie się takiej osoby do sieci domowej.

Jeśli weźmiemy pod uwagę scenariusze, gdzie atakowany jest cały system, a nie poszczególne liczniki, mamy do czynienia z atakiem na dużo większą skalę i z dużo bardziej znaczącymi konsekwencjami. Przykładowe scenariusze uwzględniają (TradeArabia, 2014):

- włamania i przejęcia kontroli nad systemem np. dostaw prądu w celu wymuszenia okupu bądź określonego działania danej organizacji,
- wywołanie chaosu lub obniżenie sprawności/obronności danego miasta lub regionu w celach politycznych lub militarnych.

Można wyliczać przykłady włamań do tego typu systemów. Haker znany jako „pr0f" włamał się do systemu zarządzania wodą i kanalizacją (ang. *SCADA*) w mieście Springfield (Illinois, USA), a nie musiał wykorzystywać do tego żadnych skomplikowanych aplikacji, gdyż 3-literowe hasło administracyjne było bardzo proste do złamania (Townsend, 2013).

Jedna z firm zajmujących się zabezpieczeniem inteligentnych miast w grudniu 2014 r. wprowadziła na rynek system CEWPS (ang. *Cognitive Early Warning Predictive Systems*), który działa podobnie jak ludzki system immunologiczny, tzn. konstruuje działania reaktywne, które atakują „wrogi kod", aby obronić system. W tym przypadku bazuje on na trzech silnikach analitycznych, które obserwują różne elementy i ich zachowania w systemie, a w przypadku wykrycia anomalii natychmiastowo reagują (Corpuz, 2014).

 DOI 10.7172/1644-9584.71.3

6. Bezpieczeństwo Internetu rzeczy

Podstawowe wyzwania jakie stoją przed IoT, także w kontekście *smart city*, to m.in. standaryzacja oprogramowania, jego personalizacja i aktualizacja oraz bezpieczeństwo, a w szczególności ochrona danych dotyczących użytkownika. Możliwość podłączenia dosłownie każdego elementu codziennego życia do globalnej sieci tworzy ogromne możliwości i znaczne oszczędności zasobów dla miast. Szerokie zastosowanie Internetu rzeczy usprawnia nasze życie, ale otwiera także drzwi dla zagrożeń bezpieczeństwa, począwszy od luk w oprogramowaniu do ataków *Denial of Service* (DoS), ataków na słabe hasła i ataków *cross-site scripting* (ataki polegające na osadzeniu w treści strony kodu, który wyświetlony użytkownikom może doprowadzić do wykonania przez nich niepożądanych akcji).

Eksperci są zdania, że urządzenia wchodzące w skład IoT są często bezradne na cyberataki ze względu na zbyt małe moce obliczeniowe. Internet rzeczy, opierający się na chmurze obliczeniowej i urządzeniach połączonych milionami obsługujących ich aplikacji, nie tworzy jednolitego środowiska i w związku z tym narażony jest na liczne zagrożenia (Rot i Sobińska, 2013). Niekontrolowana inwigilacja ludzi, zagrożenia wynikające z działalności hakerów oraz przejęcie kontroli nad urządzeniami to istotne niebezpieczeństwa, które wraz z rozpowszechnieniem IoT staną się realnymi zagrożeniami dla bezpieczeństwa użytkowników i całych miast. Luki znajdują się w wielu urządzeniach, a hakerzy mogą bez problemu uzyskać hasła umożliwiające dostęp do nich z przywilejami administratora, a następnie modyfikować ich oprogramowanie systemowe, by dostosować je do przestępczych celów.

Zastosowanie opisywanych rozwiązań, szczególnie w kontekście inteligentnych miast, wiąże się często z gromadzeniem informacji, w tym danych osobowych, na temat mieszkańców i innych osób znajdujących się na terenie miasta. Informacje te są potrzebne np. do zarządzania siecią transportu miejskiego, zaopatrzeniem w media, sterowaniem ruchem ulicznym czy dostosowaniem oferowanych usług publicznych do potrzeb. Ta nowa fala nowoczesnych technologii i usług spowoduje powstanie nieznanych wcześniej luk w zabezpieczeniach. Te działania prowadzą do (*Dziennik internautów*, 2015):

- zbierania danych osobowych o osobach korzystających z publicznych usług lub infrastruktury (np. miejskie rowery, dostęp do Internetu, strefy parkowania),
- instalowania inteligentnych liczników mediów (energii, wody itp.),
- wymiany danych osobowych między różnymi bazami danych w ramach infrastruktury miejskiej i ich analizy w modelu Big Data.

Powyższe działania stanowią potencjalne zagrożenie, dlatego konieczne staje się wyważenie wartości – zapewnienie mieszkańcom jak najlepszej jakości życia przy zachowaniu maksimum bezpieczeństwa, a zwłaszcza prywatności.

W wyniku badań przeprowadzonych przez Instytut SANS zidentyfikowano największe ryzyka związane z Internetem rzeczy, do których zaliczono (Pescatore, 2014):

- problemy z aktualizacją oprogramowania obiektów (zależną od producentów sprzętu),
- wykorzystanie obiektów, jako najsłabiej zabezpieczonych punktów wejścia do sieci, w celu kolejnych infekcji czy ataków,
- ataki typu DoS, które w przypadku np. infrastruktury sieci energetycznej w miastach mogą prowadzić do bardzo poważnych konsekwencji,
- nieuprawnione modyfikacje parametrów działania urządzeń,
- błędy użytkowników i przypadkowe modyfikacje, które z sieci bardzo silnie połączonych ze sobą systemów mogą prowadzić do trudnych do przewidzenia konsekwencji w skali całego miejskiego systemu połączonych urządzeń.

Jak pokazują badania przeprowadzone przez specjalistów firmy HP (HP, 2015), wiele urządzeń IoT jest podatnych na atak, a każde z nich posiada słabe punkty, dotyczące bezpieczeństwa haseł, kryptografii, braku odpowiedniego zarządzania kontrolą dostępu, które rozszerzają możliwości nadużyć przez intruzów. Firma HP przetestowała 10 popularnych urządzeń Internetu rzeczy, odkrywając średnio 25 luk w urządzeniu. Urządzenia te testowane wraz z ich aplikacjami mobilnymi pochodziły od producentów kamer, termostatów, kontrolerów energii, urządzeń do sterowania alarmami, otwieraniem bram itp. Najczęstsze problemy bezpieczeństwa obejmowały następujące zagadnienia:

- Problemy z prywatnością danych – w 8 na 10 urządzeniach zanotowano podatności dotyczące prywatności związanej z gromadzeniem danych osobowych, takich jak imię i nazwisko, adres e-mail, adres zamieszkania, data urodzenia, numery karty kredytowej oraz informacje na temat zdrowia.
- Słabe punkty w systemie autoryzacji i uwierzytelnienia – systemy bezpieczeństwa w 80% badanych urządzeń nie wymagały haseł o odpowiedniej długości i złożoności, a większość urządzeń pozwalała na używanie trywialnych haseł. Przykładowo, ekspertom Kaspersky Lab udało się bez większego problemu włamać do systemu sterującego latarniami ulicznymi w jednym z miast, ponieważ nie użyto tam żadnych technologii uwierzytelniających.
- Brak szyfrowania transmisji danych – 70% badanych urządzeń nie szyfrowało komunikacji z Internetem i sieciami lokalnymi, a połowa aplikacji mobilnych stosowanych do obsługi tych urządzeń przesyłała niezaszyfrowane komunikaty w chmurze obliczeniowej, Internecie lub sieci lokalnej. Szyfrowanie transmisji danych ma zasadnicze znaczenie, zważywszy że wiele z testowanych urządzeń (szczególnie w przypadku inteligentnych miast) gromadzi i przesyła poprzez różne kanały komunikacji dane wrażliwe, dotyczące m.in. mieszkańców.

 DOI 10.7172/1644-9584.71.3

- Niebezpieczne interfejsy WWW – w sześciu z dziesięciu testowanych urządzeniach zanotowano obawy związane z bezpieczeństwem interfejsów użytkownika, takie jak: narażenie na wspomniane już ataki *cross-site scripting*, złe zarządzanie sesjami, słaby system uwierzytelnienia.
- Niewystarczający poziom bezpieczeństwa oprogramowania – 60% urządzeń nie stosowało szyfrowania podczas pobierania aktualizacji oprogramowania. Niektóre pobrania mogły być przechwycone, przejrzane i modyfikowane.

Eksperci zaznaczają, że wraz z dynamicznym rozwojem IoT jest konieczne, aby samorządy i organizacje tworzące rozwiązania w ramach Internetu rzeczy identyfikowały podatności systemu, zanim zostaną one wykorzystane w praktyce i wdrożone w miastach. Odbywać się to powinno poprzez m.in. dokładne testy oprogramowania i proaktywne eliminowanie podatności w rozwijanych aplikacjach (HP, 2015). Producenci urządzeń i oprogramowania powinni zadbać o bezpieczeństwo na każdym etapie rozwoju swojego produktu, zająć się opracowaniem możliwie najlepszego oprogramowania oraz zapewnieniem bezpiecznego standardu współpracy między urządzeniami. Wyzwaniem dla instytucji standaryzacyjnych jest wprowadzenie standardów w tym zakresie, a dla różnych organizacji wprowadzanie certyfikatów branżowych. Należy jednak pamiętać o konieczności zwiększania świadomości użytkowników w zakresie bezpiecznego korzystania z urządzeń oraz ich oprogramowania.

7. Zakończenie

W artykule przeanalizowane zostały kwestie bezpieczeństwa związane z implementacją koncepcji Internetu rzeczy, która będzie zyskiwać na znaczeniu i w ciągu najbliższych lat na stałe wejdzie do kanonu rozwiązań wykorzystywanych nie tylko w firmach i gospodarstwach domowych, ale przede wszystkim w inteligentnych miastach. Zgodnie z prognozami analityków może się to przyczynić do znaczącego wzrostu wartości gospodarki, o ile nie nastąpi gwałtowny odwrót od tego typu rozwiązań, np. poprzez nieadekwatne potraktowanie kwestii bezpieczeństwa. IoT pozwala łączyć i wykorzystywać obiekty w celu osiągania licznych korzyści, przez co adopcja tych rozwiązań będzie wzrastać, poszerzając równocześnie ilość potencjalnych punktów ataku (Rot i Blaicke, 2016).

Obecnie istnieje niewiele wyspecjalizowanych rozwiązań, które są w stanie zapobiegać lub częściowo adresować znane oraz nowe podatności i metody ataku. Systemy IoT pozwalają na przeprowadzanie niespotykanych dotąd ataków na części samego Internetu rzeczy, a także często stanowią punkt wejścia do sieci i pozwalają atakującym na pominięcie tradycyjnych warstw zabezpieczeń.

Jednorazowe uwierzytelnianie oraz fakt, że większość urządzeń IoT jest zawsze uruchomiona i podłączona powodują, że Internet rzeczy jest atrakcyjnym celem dla hakerów. Wzmocnienie bezpieczeństwa bram, które

łączą elementy systemu Internetu rzeczy, w szczególności w inteligentnych miastach, jest zatem koniecznością. Kluczowe jest więc dobieranie takich rozwiązań, które oferują m.in. szyfrowanie komunikacji pomiędzy urządzeniami. Należy również rozważyć wdrożenie lub wzmocnienie systemów szyfrowania do ochrony danych w sieciach, usługach w chmurze i na urządzeniach końcowych (Gazeta Prawna, 2016).

Bibliografia

Brachman, A. (2013). *Internet przedmiotów. Raport Obserwatorium ICT*. Park Naukowo-Technologiczny „Technopark Gliwice", Gliwice. Pozyskano z: http://www.technopark.gliwice.pl/files/artykuly/Internet%20przedmiot%C3%B3w.pdf (dostęp: 11.08.2017).

Castro, D. i Misra, J. (2013). *The Internet of Things*. Center for Data Innovation. Pozyskano z: http://www2.datainnovation.org/2013-internet-of-things.pdf (dostęp: 21.09.2017).

Cohen, B. (2012). *The Top 10 Smart Cities On The Planet.* CO. Design. Pozyskano z: http://www.fastcoexist.com/1679127/the-top-10-smart-cities-on-the-planet (dostęp: 28.09.2017).

Corpuz, I. (2014). *A smart vaccine for smart cities*, GulfNews z dn. 20.12.2014. Pozyskano z: http://m.gulfnews.com/opinion/a-smart-vaccine-for-smart-cities-1.1429472 (dostęp: 19.08.2017).

Courtney (2011). *When Buses Talk, Maintenance Listens: Smart Bus Maintenance Means Greater Efficiencies, Big Savings*. Nextstop, z dn. 15.03.2011. Pozyskano z: http:// www.nextstopstl.org/3702/when-buses-talk-maintenancelistens-smart-bus-maintenance-means-greater-efficiencies-bigsavings/ (dostęp: 25.09.2017).

Dziennik internautów (2015). *Internet Rzeczy. Bezpieczeństwo Smart City – VII Konferencja Naukowa Bezpieczeństwo w Internecie*. Dziennik internautów z dn. 08.05.2015. Pozyskano z: http://di.com.pl/internet-rzeczy-bezpieczenstwo-smart-city-vii-konferencja-naukowa-bezpieczenstwo-w-internecie-52089 (dostęp: 28.09.2017).

Evans, D. (2011). *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*. Cisco Internet Business Solutions Group. Pozyskano z: http://www.cisco.com/c/dam/en_us/about/ac79 /docs/innov/IoT_IBSG_0411FINAL.pdf (dostęp: 16.07.2017).

EY (2015). *Insights on governance, risk and compliance: Cybersecurity and the Internet of Things*. Pozyskano z: http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf (dostęp: 14.07.2017).

Gazeta Prawna (2016). *Inteligentne miasta mogą być niebezpieczne.* Pozyskano z: http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/936993,inteligentne-miasta-internet-rzeczy-cyberbezpieczenstwo.html (dostęp: 04.09.2017).

HP (2015). *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*. Pozyskano z: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676 (dostęp: 23.06.2017).

Intel (2016). *Internet rzeczy nie tylko w smart city.* Pozyskano z: http://evertiq.pl/news/18023 (dostęp: 10.09.2017).

Metcalfe, J. (2012). *Air Pollution Kills More Than 2 Million a Year*. The Atlantic Cities, July 16, 2012. Pozyskano z: http://m.theatlanticcities.com/neighborhoods/2013/07/air-pollutionkills-more-2-million-year/6209/ (dostęp: 14.09.2017).

 DOI 10.7172/1644-9584.71.3

Middleton, P., Kjeldsen, P. i Tully, J. (2013). *Forecast: The Internet of Things, Worldwide 2013*. Gartner, November 2013. Pozyskano z: http://www.gartner.com/doc/2625419/forecast-internet-things-worldwide- (dostęp: 19.12.2016).

Mitchell, S., Villa, N., Stewart-Weeks, M. i Lange, A. (2013). *The Internet of Everything for Cities*. San Jose, CA: Cisco Press.

Nowakowski, W. (2015). Bliższa chmura, czyli usługi obliczeniowe we mgle. *Elektronika – konstrukcje, technologie, zastosowania 5*, Instytut Maszyn Matematycznych, Warszawa. Pozyskano z: http://www.imm.org.pl/imm/plik/pliki-do-pobrania-elektronika52015_nn358.pdf (dostęp: 16.12.2016).

Nowicka, K. (2014). Smart City – miasto przyszłości. *Gospodarka Materiałowa i Logistyka*, *5*(1233).

Nylec, K. (2012). *Smart cities, idea i praktyka.* Pozyskano z: http://www.portalsamorzadowy.pl/gospodarka-komunalna/smart-cities-idea-i-praktyka,32600.html (dostęp: 8.09.2017).

Pescatore, J. (2014). *Securing the Internet of Things Survey*. SANS Institute InfoSec Reading Room. Pozyskano z: http://www.sans.org/reading-room/whitepapers/covert/securing-internet-things-survey-34785 (dostęp: 9.06.2017).

Polski, M. (2017). *Internet rzeczy – potęga danych*. Warsaw Press. Pozyskano z: http://www.smartcity.warsawpress.com/index.php/2017/07/25/internet-rzeczy-potega-danych/ (dostęp: 26.09.2017).

Raymond, J. (2015). *The Internet of Things – A Study in Hyde, Reality, Disruption, and Growth*. Pozyskano z: http://www.supplychain247.com/paper/the_internet_of_things_a_study_in_hype_reality_disruption_and_growth (dostęp: 8.09.2016).

Rot, A. (2016). Mgła obliczeniowa jako nowy paradygmat wsparcia transmisji i przetwarzania danych w koncepcji Internetu rzeczy. *Informatyka Ekonomiczna*, *3*(41), 51–63, DOI:10.15611/ie.2016.3.05.

Rot, A. (2017). Wybrane zagadnienia bezpieczeństwa danych i usług w modelu Cloud Computing. W: A. Gąsiorkiewicz i in. (red.), *Gospodarka cyfrowa 2016. Zarządzanie, innowacje, społeczeństwo i technologie*. Wydawnictwo Wydziału Zarządzania Politechniki Warszawskiej, 98–108.

Rot, A. i Blaicke, B. (2016). Zagrożenia wynikające z implementacji koncepcji Internetu rzeczy. Rekomendacje dla organizacji i dostawców rozwiązań. *Informatyka Ekonomiczna*, *3*(41), 76–91, https://doi.org/10.15611/ie.2016.3.07

Rot, A. i Sobińska, M. (2013). IT security threats in cloud computing sourcing model. W: M. Ganzha, L. Maciaszek i M. Paprzycki (red.), *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems*. Wyd. IEEE.

Shoup, D. (2007). Cruising for Parking. *Access*, *30*. Pozyskano z: http://shoup.bol.ucla.edu/CruisingForParkingAccess.pdf (dostęp: 7.09.2017).

Stawasz, D., Sikora-Fernandez, D. i Turała, M. (2012). Koncepcja Smart City jako wyznacznik podejmowania decyzji związanych z funkcjonowaniem i rozwojem miasta. *Zeszyty Naukowe Uniwersytetu Szczecińskiego Nr 721, Studia Informatica Nr 29*. Wydawnictwo Uniwersytetu Szczecińskiego, Szczecin.

Townsend, A.M. (2013). *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: W.W. Norton & Company Inc.

TradeArabia (2014). Smart cities must protect utilities from cyber-attacks. *TradeArabia*, 13.10.2014. Pozyskano z: http://www.tradearabia.com/news/REAL_267393.html (dostęp: 22.08.2017).

Wiśniewski, M. (2013). Smart cities – definicje i pomiar (przegląd koncepcji). *Prace Naukowe WWSZIP*, *24*(4).