INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 3(41) • 2016

ISSN 1507-3858
e-ISSN 2450-0003

Artur Rot
Uniwersytet Ekomomiczny we Wrocławiu
e-mail: artur.rot@ue.wroc.pl

Bartosz Blaicke
McKinsey&Company
e-mail: bartek_blaicke@mckinsey.com

ZAGROŻENIA WYNIKAJĄCE Z IMPLEMENTACJI KONCEPCJI INTERNETU RZECZY. REKOMENDACJE DLA ORGANIZACJI I DOSTAWCÓW ROZWIĄZAŃ

THREATS RESULTING FROM THE IMPLEMENTATION OF THE CONCEPT OF THE INTERNET OF THINGS. RECOMMENDATIONS FOR ORGANIZATIONS AND SOLUTION SUPPLIERS

DOI: 10.15611/ie.2016.3.07
JEL Classification: L86, O32, O33

Streszczenie: Jednym z istotnych trendów, które mają potencjał, by w ciągu najbliższych lat wpłynąć na życie każdego człowieka i funkcjonowanie biznesu jest Internet rzeczy (IoT). Jednak podłączenie urządzeń IoT do globalnej sieci niesie ze sobą potencjalne zagrożenia, wśród których będą cyberataki, na które zarówno organizacje jak i dostawcy rozwiązań muszą zwracać uwagę. Odpowiedzią powinno być wprowadzenie i stosowanie proaktywnego modelu bezpieczeństwa, który wyprzedzi pojawiające się zagrożenia. Internet rzeczy stanowi duże wyzwanie dla specjalistów zajmujących się bezpieczeństwem, szczególnie, że podlega on ciągłemu rozwojowi. Celem artykułu jest identyfikacja zagrożeń dla cyberbezpieczeństwa wynikających z poszerzania dostępu do sieci nowych urządzeń i procesów, które pierwotnie nie były do tego przystosowane. W artykule zawarto również rekomendacje Autorów dotyczące bezpieczeństwa rozwiązań Internetu rzeczy dla przedsiębiorstw, jak i dostawców tych rozwiązań.

Słowa kluczowe: Internet rzeczy, cyberbezpieczeństwo, prywatność, zagrożenia, podatności.

Summary: The Internet of Things is one of the most important trends that have the potential to influence the life of every human being and functioning of the business in the coming years. However, connecting IoT devices to a global network brings serious potential threats like cyberattacks to which both, organizations and solution providers have to pay special attention to.

The answer is the implementation and usage of proactive security model, which will overtake emerging threats. The Internet of Things is the major challenge for cybersecurity specialists, especially in the situation when this concept continues to grow. This article aims to identify the threats to cybersecurity resulting from the access to the network of new equipment and processes that were not originally designed for this purpose. The article also includes the authors' security recommendations for companies and suppliers of such solutions.

Keywords: Internet of Things, cybersecurity, privacy, threats, vulnerabilities.

1. Wstęp

Postępujący proces informatyzacji społeczeństwa tworzy coraz bardziej połączone i zaawansowane technologicznie narzędzia do zwiększania wydajności pracy oraz ułatwiania życia codziennego. Jedną z takich znaczących nowych koncepcji jest Internet rzeczy bądź przedmiotów (*Internet of Things* − IoT), który zakłada połączenie w sieć niemalże wszystkich rodzajów urządzeń. Pod tym pojęciem kryje się wizja przyszłego świata, w którym cyfrowe i fizyczne urządzenia czy przedmioty codziennego użytku są połączone odpowiednią infrastrukturą w celu dostarczenia wielu nowych aplikacji i usług. W najbliższych latach będziemy mieli okazję obserwować fundamentalne zmiany sposobu, w jaki współdziałamy zarówno z otaczającym nas światem urządzeń cyfrowych, jak i ze światem fizycznym [Brachman 2013].

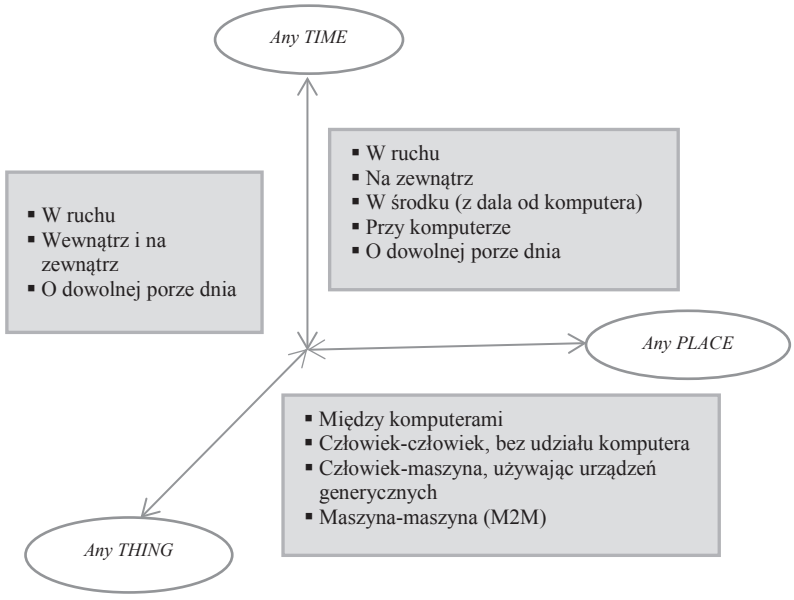
Dzięki bardzo szybkiej ewolucji urządzeń wchodzących w skład Internetu rzeczy konsumenci i przedsiębiorcy mają możliwość wykorzystywania wielu innowacji w różnorodnych kontekstach, tym samym powiększając liczbę potencjalnych punktów ataku. W związku z tym powstaje pytanie, czy rozwiązania te są wystarczająco bezpieczne, aby można je było implementować w systemach przetwarzających informacje. Ponadto należy sprawdzić, czy funkcjonują odpowiednie mechanizmy zabezpieczające te ściśle połączone systemy tak, aby w bezpieczny sposób można było korzystać z wprowadzenia tego typu rozwiązań.

Cele niniejszego artykułu to identyfikacja zagrożeń dla cyberbezpieczeństwa wynikających z realizacji koncepcji Internetu rzeczy i sformułowanie przez autorów rekomendacji dotyczących bezpieczeństwa IoT dla przedsiębiorstw i dostawców tych rozwiązań. W artykule zaprezentowano także przykładowe zagrożenia i zabezpieczenia związane z zastosowaniem tej koncepcji w kontekście inteligentnego miasta. Ponadto celem tekstu jest weryfikacja hipotezy mówiącej o tym, że zabezpieczenie systemów w obszarze „Internetu rzeczy" nie jest wystarczająco uwzględniane w zarządzaniu bezpieczeństwem informatycznym.

2. Idea koncepcji Internetu rzeczy

Według raportu opracowanego przez firmę Cisco [2016] zagadnienia, takie jak cyfryzacja, bezpieczeństwo technologii informacyjnych oraz Internet rzeczy, to zja-

wiska, które wyznaczały kierunek rozwoju poszczególnym branżom gospodarki w roku 2016 i będą szczególnie istotne w kolejnych latach. Wśród nich znajduje się Internet rzeczy, będący połączeniem urządzeń w sieć, co ma na celu umożliwienie ich zdecentralizowanej komunikacji 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 (najczęściej w postaci transmisji internetowej). Oczekuje się, że IoT znajdzie wiele zastosowań w różnych dziedzinach usługowych i w działalności gospodarczej, m.in. w energetyce, transporcie, przemyśle, budownictwie, logistyce, opiece zdrowotnej, sektorze IT. Według prognoz firmy Gartner w 2020 r. do Internetu podłączonych będzie 26 mld urządzeń, co oznacza ogromny przyrost ilości danych, które trzeba będzie w sposób bezpieczny przechowywać i przetwarzać [Middleton, Kjeldsen, Tully 2013].



Rys. 1. Koncepcja Internetu rzeczy bazująca na trzech kryteriach

Źródło: [Brachman 2013].

Jedną z często przytaczanych aktualnie definicji Internetu rzeczy jest ta zaproponowana przez International Telecommunications Union (ITU), określaca IoT jako globalną infrastrukturę dla społeczeństwa informacyjnego, umożliwiającą dostęp do zaawansowanych usług przez połączenie (fizyczne lub wirtualne) przedmiotów (obiektów), bazujące na istniejących i rozwijanych interoperacyjnych technologiach informacyjno-komunikacyjnych [Telecommunication Standardization… 2006]. Zatem

pojęcie to może być przedstawione jako rozszerzenie koncepcji Internetu o wszystkie wymienione kategorie urządzeń lub sieć łącząca różne sieci (wirtualne i fizyczne) będące w stanie komunikować się. Koncepcję Internetu rzeczy można również przedstawić jako sieć umożliwiającą komunikację w trzech wymiarach: zawsze (*ANY time*), wszędzie (*ANY place*) oraz ze wszystkim (ang. *ANY thing*) (patrz rys. 1).

Zastosowania tej koncepcji usprawniają nasze życie, ale stwarzają także zupełnie nowe zagrożenia, stanowiąc jednocześnie wyzwanie dla architektów systemów bezpieczeństwa. Eksperci są zdania, że każdy problem z bezpieczeństwem komputerowym sprzed kilkunastu lat powraca aktualnie w nowych urządzeniach i daje hakerom mnóstwo nowych możliwości i furtek do ewentualnych cyberataków [Rot, Sobińska 2013]. Wśród najczęstszych zagrożeń i podatności IoT wymieniane są problemy z prywatnością danych, słabe punkty w systemach autoryzacji i uwierzytelnienia, niezabezpieczone interfejsy WWW, luki i błędy w oprogramowaniu.

3. Potencjał ekonomiczny i przyszłość Internetu rzeczy

Według firmy badawczej McKinsey&Company, Internet rzeczy ma szanse generować znaczne korzyści ekonomiczne dla światowej gospodarki; szacuje się, że w roku 2025 mogą się one mieścić w kwocie 2,7-6,2 trylionów dolarów amerykańskich [McKinsey… 2015]. Gałęzie przemysłu, które mają największy potencjał, by wygenerować taką wartość, uwzględniają szeroko pojęte zastosowania medyczne, infrastrukturalne oraz usługi w ramach sektora publicznego, pomagając ludzkości zmierzyć się z wieloma najtrudniejszymi problemami występującymi obecnie. Na przykład zdalne monitorowanie stanu pacjentów może mieć olbrzymi wpływ na życie milionów ludzi borykających się z przewlekłymi chorobami, jednocześnie zmniejszając koszty obsługi medycznej. Możliwość kontroli i analizy sieci energetycznych oraz wodno-kanalizacyjnych może znacznie wpłynąć na ich efektywniejsze wykorzystanie, zmniejszając emisje gazów cieplarnianych czy minimalizując niepotrzebne zużycie wody. Ponadto przez wykorzystanie czujników do zbierania i analizy informacji o ruchu drogowym, a nawet wywozu śmieci można bardzo usprawnić operacyjne działania służb publicznych. Oczywiście, nie będzie łatwo uzyskać w pełni potencjał związany z tego typu rozwiązaniami, gdyż organizacje je implementujące będą potrzebowały umiejętności i narzędzi technicznych do wdrażania systemów, które będą w czasie rzeczywistym obsługiwać setki tysięcy, a nawet miliony punktów sieci. Takie połączenie skomplikowanych sieci łączących świat cyfrowy z rzeczywistym będzie, oczywiście, miało kolosalne znaczenie dla kwestii bezpieczeństwa i prywatności. Tak jak przy każdym połączeniu uwzgledniającym transfer informacji, teraz obie strony będą mogły być w pełni zautomatyzowanymi maszynami, które działają bez nadzoru człowieka. Takie rozwiązania są jeszcze bardziej podatne na ataki hakerów, przestępców czy terrorystów. Nawet sam dostęp lub podsłuch części danych, takich jak monitorowanie stanu zdrowia pacjentów, może być nielegalnie wykorzystywany. To samo dotyczy kontrolerów urządzeń inteligent-

nego domu, np. możliwość zdalnej kontroli domowych AGD. W związku z tymi i wieloma innymi zagrożeniami problemy bezpieczeństwa w tego typu systemach są z natury kwestią pierwszorzędną i będą musiały być rozwiązane, aby technologie te mogły się w pełni rozwijać w przyszłości [Manyika i in. 2013].

Możliwość podłączenia dosłownie każdego elementu codziennego życia, takiego jak pralka, lodówka czy oświetlenie, do globalnej sieci tworzy możliwości biznesowe i znaczne oszczędności zasobów dla gospodarstw domowych czy organizacji. 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) (atak na system komputerowy lub usługę sieciową w celu uniemożliwienia jej działania), ataków na słabe hasła i ataków *cross-site scripting* (polegających na osadzeniu w treści strony kodu, który wyświetlony użytkownikom, może doprowadzić do wykonania przez nich niepożądanych akcji).

4. Wybrane obszary zastosowań koncepcji Internetu rzeczy

Podstawowym celem Internetu rzeczy jest stworzenie inteligentnych przestrzeni, tj. inteligentnych miast, transportu, produktów, budynków, systemów energetycznych, systemów zdrowia czy związanych z życiem codziennym. Obszarów zastosowania Internetu rzeczy może być wiele; mogą one przenikać wiele aspektów życia (patrz tab. 1). Nie jest to tylko koncepcja przyszłości, gdyż jest już w pewnym zakresie realizowana. Jednym z pierwszych zastosowań jest centralny system sterowania tzw. inteligentnym domem, w którym funkcjonalność poszczególnych urządzeń została poszerzona o wykorzystanie danych zbieranych przez czujniki. Przykładowo czujniki wilgotności i temperatury przesyłają informacje do systemu otwierania okien, a czujniki ruchu i podczerwieni − do systemu oświetlenia pomieszczeń. Czujniki w lodówce generują potencjalną listę zakupów, która może być wysłana do systemu sklepu internetowego [Lipski 2015].

Tabela 1. Obszary zastosowań Internetu rzeczy

Lp.	Sektory	Wybrane obszary zastosowań
1	2	3
1	Budownictwo	sterowanie ogrzewaniem, wentylacją, klimatyzacją, kontrolą dostępu, oświetleniem, systemami bezpieczeństwa w budynkach itp.
2	Energetyka	– wydobycie surowców (aplikacje i urządzenia do ekstrakcji surowców i ich transportu), – poszukiwania alternatywnych, w tym odnawialnych, źródeł energii, – urządzenia dostarczające prąd do odbiorców.
3	Sektor konsumpcyjny/ domowy	– bezpieczeństwo w domu (alarmy, monitorowanie osób starszych i dzieci), – sterowanie urządzeniami, energią i oświetleniem w domu, – rozrywka

1	2	3
4	Opieka zdrowotna i nauki przyrodnicze	– telemedycyna, – domowe systemy monitoringu pacjentów (monitoring osób starszych lub np. osób z wszczepionymi rozrusznikami serca), – badania i rozwój nowych leków i sprzętu medycznego
5	Przemysł	– monitorowanie i śledzenie aktywów, urządzeń i produktów przemysłowych, – analiza lokalizacji dla szerokiej gamy procesów fabrycznych
6	Transport	– zarządzanie flotą pojazdów (systemy nawigacji, poszukiwania zaginionych pojazdów, zarządzanie systemem dystrybucji), – systemy informacji dla pasażerów, – systemy płatności za korzystanie z infrastruktury transportowej i parkingowej
7	Sektor detaliczny	– systemy sieciowe i urządzenia zarządzania łańcuchem dostaw, zarządzanie informacją o produktach i konsumentach, zarządzanie zapasami, – maszyny sprzedające (żywność, napoje, papierosy), parkometry, – urządzenia rozrywkowe (automaty do gier, systemy dźwiękowe), – urządzenia wyświetlające (billboardy, wyświetlacze, punkty informacyjne)
8	Bezpieczeństwo publiczne	– monitorowanie środowiska (w tym terenów zalewowych, oczyszczalni ścieków), – informacje meteorologiczne i klimatyczne, – śledzenie ludzi, zwierząt, przesyłek czy bagażu, – bezpieczeństwo militarne
9	Sektor IT	– urządzenia biurowe (kserokopiarki, drukarki), – infrastruktura transmisji mobilnej, centra danych (systemy utrzymania energii i klimatyzacyjne), – e-*commerce*

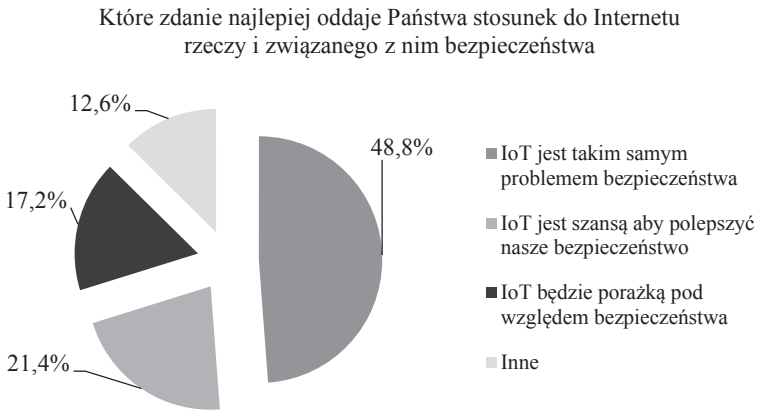
Źródło: opracowanie własne na podstawie [Beecham Research 2016; Senkus i in. 2014].

Jak wspomniano, Internet rzeczy znajdzie wiele zastosowań w różnych dziedzinach usługowych i w działalności gospodarczej, m.in. w energetyce, transporcie, przemyśle, logistyce, inteligentnej opiece zdrowotnej, sektorze IT. Oczekiwania na szybki rozwój Internetu rzeczy są powiązane także z zastosowaniami tej technologii w inteligentnym budownictwie, inteligentnych miastach i samochodach, w automatyce przemysłowej określanej mianem przemysłu 4.0.

5. Ogólny pogląd na bezpieczeństwo w nowym kontekście

Jak wspomniano, Internet rzeczy z pewnością wprowadzi wiele nowych zmiennych do kwestii szeroko pojętego bezpieczeństwa systemów teleinformatycznych. Na podstawie badań przedstawionych w dalszej części artykułu, przeprowadzonych przez Instytut SANS, można jednak stwierdzić, że około połowa badanych przedsta-

wicieli przedsiębiorstw nie zauważa znaczącej różnicy w kwestiach bezpieczeństwa (patrz rys. 2). Jednak Internet rzeczy będzie stanowić duże wyzwanie dla specjalistów zajmujących się cyberbezpieczeństwem, a zarazem będzie to okazja do przemyślenia całego ekosystemu zapewniającego akceptowalny poziom ryzyka.



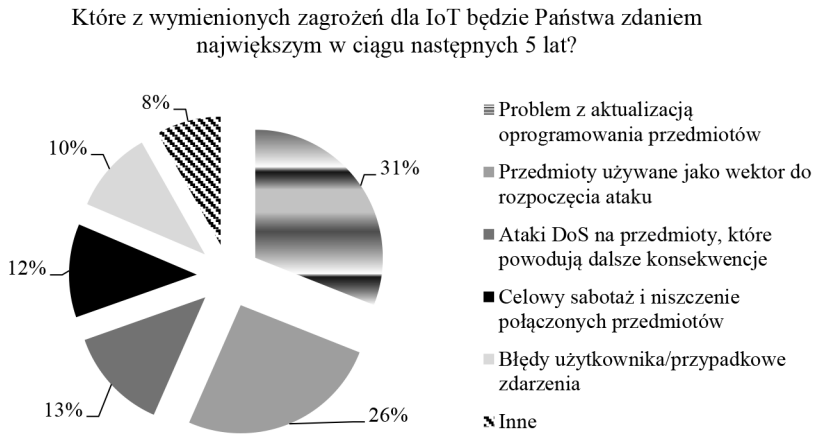
Rys. 2. Wpływ Internetu rzeczy na cyberbezpieczeństwo w opinii ankietowanych

Źródło: opracowanie własne na podstawie [Pescatore 2014].

To samo badanie ankietowe wykazało również (patrz rys. 3), że największymi zagrożeniami związanymi z rosnącą popularnością Internetu rzeczy są:

- trudności z aktualizacją oprogramowania „przedmiotów", która bardzo często jest zależna od producentów sprzętu, a użytkownicy nie mają żadnej możliwości ingerencji w tę część oprogramowania,
- wykorzystanie przedmiotów, jako najsłabiej zabezpieczonych punktów wejścia do sieci, co daje możliwość rozprzestrzeniania się złośliwego oprogramowania i dalszej infekcji kolejnych celów,
- wykonywanie ataków związanych z utrudnieniem bądź zaprzestaniem świadczenia danych usług (*Denial of Service*), które zwłaszcza w kontekście infrastruktury krytycznej, takiej jak sieć energetyczna, przesyłanie paliw czy urządzenia medyczne, może prowadzić do poważnych konsekwencji z utratą życia włącznie,
- celowy sabotaż i fizyczne niszczenie przedmiotów przez cyfrowy dostęp i modyfikacje parametrów działania,
- błędy użytkowników i przypadkowe modyfikacje, które z sieci bardzo silnie połączonych ze sobą systemów mogą prowadzić do trudnych do przewidzenia konsekwencji w skali całego systemu połączonych rzeczy i urządzeń.

Przykładem nieświadomości związanej z potencjalnym wykorzystaniem Internetu rzeczy są ostatnie debaty związane z publicznymi przetargami na inteligentne liczniki energii. Niestety, po raz kolejny głównym kryterium wyboru jest cena



Rys. 3. Główne zagrożenia dla Internetu rzeczy w opinii ankietowanych

Źródło: opracowanie własne na podstawie [Pescatore 2014].

urządzenia, a kwestie związane z bezpieczeństwem nie są w ogóle brane pod uwagę [Majdan 2015]. Na szczęście na szczeblu narodowym opublikowana Doktryna Cyberbezpieczeństwa Rzeczpospolitej Polskiej jako cel strategiczny traktuje ochronę krytycznej infrastruktury państwa, w tym sektorów finansowego, energetycznego i ochrony zdrowia. Ponadto paragraf 45 tego dokumentu [Biuro Bezpieczeństwa Narodowego 2015] mówi o potrzebie budowania krajowych kompetencji pozwalających samemu projektować, a następnie budować urządzenia wchodzące w skład naszej cyberinfrastruktury, a więc dotyczy to również sensorów i innych urządzeń wchodzących w skład IoT.

Niezależne zrzeszenie OWASP (Open Web Application Security Project) w 2014 r. wydało zestawienie 10 największych uchybień bezpieczeństwa wśród najpopularniejszych 10 urządzeń wchodzących w skład Internetu rzeczy. Tabela 2 prezentuje najczęściej występujące problemy bezpieczeństwa w tych urządzeniach i ich klasyfikację względem czterech kryteriów.

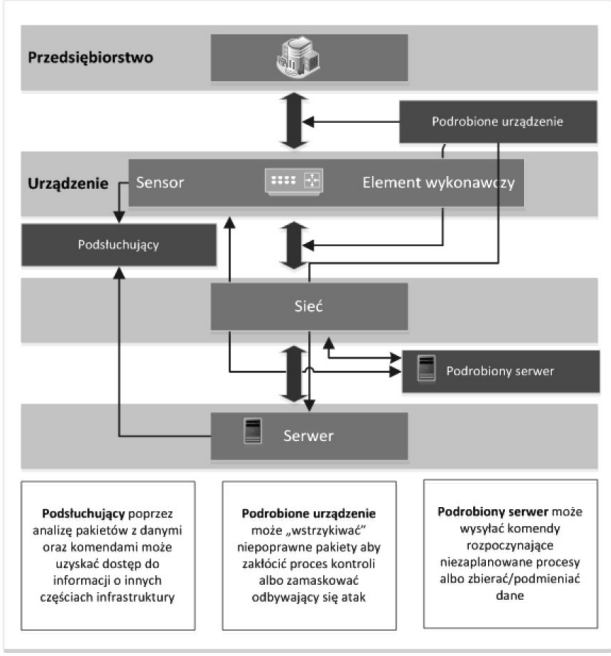
Ponieważ Internet rzeczy jest systemem połączonym, można wyróżnić różne wektory ataku, które skupiają się na różnych połączeniach między urządzeniami. Rysunek 4 przedstawia kilka potencjalnych ataków z użyciem podstawionego serwera, urządzenia oraz przez podsłuchiwanie komunikacji.

Jak pokazują badania przeprowadzone przez specjalistów firmy HP [2014], 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 intruzom możliwości nadużyć. Firma HP przetestowała dziesięć najbardziej popularnych urządzeń Internetu rzeczy, odkrywając średnio 25 luk w urządzeniu (łącznie 250 zagrożeń bezpieczeństwa we wszystkich produktach).

Tabela 2. Najważniejsze podatności i zagrożenia urządzeń Internetu rzeczy

Lp.	Podatność/zagrożenie	Łatwość wykorzystania do ataku	Częstość występowania	Łatwość wykrycia	Potencjalne skutki
1	Niezabezpieczony interfejs sieciowy	łatwy	częsty	łatwy	znaczne
2	Zbyt słaba autoryzacja	średnia	częsty	łatwy	znaczne
3	Niezabezpieczone usługi sieciowe	średnia	rzadki	średnia	średnie
4	Brak szyfrowania warstwy transportowej	średnia	częsty	łatwy	znaczne
5	Problemy z prywatnością	średnia	częsty	łatwy	znaczące
6	Niezabezpieczona transmisja z chmurą obliczen.	średnia	częsty	łatwy	znaczne
7	Niezabezpieczone interfejsy bezprzewodowe	średnia	częsty	łatwy	znaczne
8	Niewystarczające opcje konfiguracji zabezpieczeń	średnia	częsty	łatwy	średnie
9	Niebezpieczne oprogramowanie firmware	trudna	częsty	łatwy	znaczne
10	Niewystarczające zabezpieczenia fizyczne	średnia	częsty	średnia	znaczne

Źródło: opracowanie własne na podstawie [OWASP 2014].



Rys. 4. Zagrożenia dla Internetu rzeczy w różnych elementach infrastruktury

Źródło: opracowanie własne na podstawie [Infineon 2014].

Urządzenia te, testowane wraz z ich aplikacjami mobilnymi, pochodziły od producentów telewizorów, kamer, termostatów domowych, kontrolerów energii, urządzeń do sterowania alarmami, otwieraniem drzwi garażowych itp. Najczęstsze problemy bezpieczeństwa obejmowały następujące zagadnienia:

- Problemy z prywatnością danych – w ośmiu urządzeniach na dziesięć zanotowano podatności dotyczące prywatności związanej z gromadzeniem danych osobowych, takich jak imię i nazwisko, adres email, adres zamieszkania, data urodzenia, numery karty kredytowej oraz informacje na temat zdrowia. Co więcej, 90% badanych systemów przechowywało nieodpowiednio zabezpieczone dane osobowe w samym produkcie, w chmurze lub w obsługującej urządzenie aplikacji mobilnej.
- 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 łatwych do rozszyfrowania haseł. Przykładowo, ekspertom Kaspersky Lab udało się bez większego problemu włamać do systemu sterującego latarniami ulicznymi dzięki wykorzystaniu technologii Bluetooth, 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 na to, że wiele z testowanych urządzeń gromadzi i przez różne kanały przesyła komunikacji dane wrażliwe.
- Niebezpieczne interfejsy WWW – w odniesieniu do sześciu urządzeń z dziesięciu testowanych zanotowano obawy związane z bezpieczeństwem interfejsów użytkownika, takie jak: narażenie na wspomniane już, trwałe ataki *cross-site scripting*, złe zarządzanie sesjami, słaby system uwierzytelnienia. 60% urządzeń kontaktujących się w chmurze wraz z aplikacjami mobilnymi dawało potencjalnemu intruzowi możliwość przejęcia kont użytkowników za pośrednictwem np. funkcji resetowania hasła.
- Niewystarczający poziom bezpieczeństwa oprogramowania – 60% urządzeń nie stosowało szyfrowania podczas pobierania aktualizacji oprogramowania. Niektóre pobrania mogły być przechwycone, wyodrębnione i zainstalowane w środowisku systemu operacyjnego Linux, gdzie mogły być przejrzane i modyfikowane.

Przytoczone różne badania i dane ukazują, że najważniejszym wyzwaniem dla twórców rozwiązań w ramach IoT powinna być kwestia bezpieczeństwa. Jak wskazują wyniki badań, tym, czego oczekują użytkownicy, jest w pierwszej kolejności zwiększone bezpieczeństwo, zwiększona kontrola nad posiadanymi urządzeniami, a dopiero później wygoda i oszczędność. Z tego punktu widzenia od ciągłego zwiększania liczby urządzeń w infrastrukturze IoT ważniejsze jest to, aby od samego początku budować bezpieczne rozwiązania, by uniknąć narażania konsumentów

na poważne zagrożenia. W tym celu ważne jest stosowanie się do sformułowanych w dalszej części niniejszego tekstu rekomendacji autorów artykułu skierowanych do dostawców rozwiązań oraz firm wykorzystujących IoT.

6. Internet rzeczy w kontekście inteligentnego miasta – potencjalne zagrożenia i istniejące sposoby zabezpieczeń

Internet rzeczy zaczął być rozpoznawalny przez kulturę masową głównie za sprawą zastosowań związanych z inteligentnym zarządzaniem ruchem samochodowym, inteligentnymi sieciami przesyłowymi elektryczności czy wody (*smart grid*). Tego typu projekty są najczęściej finansowane przez rządy czy władze miejskie i w większości przypadków są rozwiązaniami budowanymi pod konkretne zastosowanie w danym mieście i kraju. Znaczenie tego konkretnego kontekstu zwiększa fakt, że coraz większa część populacji ulega urbanizacji, a do roku 2050 ponad 60% ludzkości będzie mieszkać w miastach, więc liczba osób obcujących z tą technologią (często nawet nieświadomie) będzie ogromna [ONZ 2012].

6.1. Wybrane zastosowania Internetu rzeczy w kontekście miasta

Przykładów zastosowań koncepcji Internetu rzeczy w kontekście inteligentnego miasta (*smart city*) można podawać wiele, w dalszej części tekstu wyszczególniono i krótko scharakteryzowano wybrane implementacje, które obrazują potencjał omawianych rozwiązań.

W 2012 r. miasto Amsterdam przy współpracy z firmami Cisco oraz Philips zainstalowało inteligentny system oświetlenia ulicznego wykorzystujący lampy LED. Każda z lamp została wyposażona w sensory i jest w stanie automatycznie zaraportować problemy związane z prawidłowym działaniem, automatycznie planuje okresowe przeglądy w taki sposób, aby jak najmniej zakłócać ruch na ulicy i chodnikach. System umożliwia także automatycznie ściemnianie, gdy nie ma dużego natężenia ruchu oraz inteligentne planowanie [Mitchell i in. 2013].

W roku 2013 Szwecja postanowiła wykorzystać sieć połączonych sensorów zanurzonych w rurach do odprowadzania ścieków w celu wykrywania chemikaliów służących do budowy materiałów wybuchowych tzw. domowej produkcji. Projekt jest nadzorowany przez Szwedzką Agencję Rozwoju Obronności i nazywa się EMPHASIS [Fiddian 2013].

Nicea wprowadziła cztery inteligentne usługi w mieście bazujące na Internecie rzeczy: inteligentne zarządzanie ruchem samochodowym (i miejscami parkingowymi), inteligentne oświetlenie, inteligentny system wywozu śmieci oraz monitorowanie parametrów środowiska. Całość oparta jest na czterowarstwowym modelu wydzielającym warstwę aplikacji, warstwę usług, warstwę sieci oraz najniżej położoną warstwę sensorów [Mitchell i in. 2013].

W Holandii w 2013 r. została oddana do użytku droga pokryta powłoką czułą na temperaturę. W razie spadku temperatury poniżej 0 na drodze pojawiają się interaktywne znaki w kształcie płatków śniegu, co ma ostrzegać kierowców przed śliską nawierzchnią. Pojawiają się one w określonych warunkach atmosferycznych, znacznie lepiej przyciągając uwagę kierowców niż tradycyjne znaki drogowe, przez co mają znaczny wpływ na bezpieczniejszą jazdę [Brachman 2013].

6.2. Przykłady ataków i potencjalnych zagrożeń w kontekście miasta

Ataki na wykorzystywane w inteligentnych miastach czy nawet – na większą skalę – w państwach – urządzenia Internetu rzeczy mogą być pierwszym etapem w konflikcie między państwami, a więc mogą mieć cechy tzw. cyberwojny. Dzieje się tak, ponieważ atak na taki system są w stanie jednocześnie spowodować znaczne utrudnienia lub straty, które dotykają dużego obszaru geograficznego lub znacznej liczby ludzi.

W przypadku ataków na inteligentne liczniki możemy wyróżnić takie zagrożenia, jak:

- Nielegalna modyfikacja, która, jeśli jest udana, pozwala na włamanie do urządzenia i zmianę wskazania, lub przez atak *man-in-the-middle* − na zmianę przesyłanego wskazania licznika do dostawcy.
- Wykorzystanie aktualnego poziomu poboru prądu przez zorganizowane grupy przestępcze do określenia, czy i kiedy domownicy przebywają w mieszkaniu, co w przypadku włamania do systemu pozwoliłoby w bardzo krótkim czasie sprawdzić setki, a nawet tysiące mieszkań na danym obszarze.
- Sam fakt wykorzystania sposobu łączności i uwzględniania inteligentnych liczników w sieci domowej (jeśli nie wykorzystują modułów GSM) 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 [TradeArabia 2014].

Jeśli weźmiemy pod uwagę sytuacje, kiedy atakowany jest cały system, a nie tylko poszczególne liczniki, mamy, oczywiście, do czynienia z atakiem na dużo większą skalę, a więc i z większymi konsekwencjami. Przykładowe scenariusze uwzględniają:

- włamania i przejęcia kontroli nad systemem, np. dostaw prądu, w celu wymuszenia okupu bądź określonego działania danego przedsiębiorstwa,
- wywołanie chaosu lub obniżenie sprawności/obronności danego regionu czy to w celach politycznych, czy militarnych, co wydaje się prawdopodobne [TradeArabia 2014].

Przykłady ataków można mnożyć. Haker znany jako „pr0f" włamał się do systemu zarządzania wodą i kanalizacją (SCADA) w mieście Springfield (Illinois, USA). Co więcej, nie musiał wykorzystywać do tego żadnych skomplikowanych aplikacji, gdyż 3-literowe hasło administracyjne było bardzo łatwe do złamania [Townsend 2013].

6.3. Wybrane systemy zabezpieczeń

Jedna z firm zajmujących się zabezpieczeniem inteligentnych miast w grudniu 2014 r. wprowadziła na rynek system CEWPS (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 to na trzech silnikach analitycznych, które obserwują różne elementy i ich zachowania w systemie, a w przypadku wykrycia anomalii natychmiastowo reagują [Corpuz 2014].

Oprócz stosowania tego typu systemów zabezpieczeń ważne jest, aby zarówno dostawcy rozwiązań, jak i użytkownicy systemów IoT stosowali się do pewnych zasad. Tego typu rekomendacje zawarto w kolejnym punkcie artykułu.

7. Rekomendacje dla dostawców rozwiązań oraz organizacji wykorzystujących Internet rzeczy

Internet rzeczy stanowi wciąż niezbadany grunt, co łatwo wywnioskować na podstawie przedstawionych wcześnie przykładów ataków i nielicznych zabezpieczeń, które dopiero powstają. W związku z tym zarówno dostawcy rozwiązań jak i użytkownicy powinni myśleć o wielu zagadnieniach związanych z kwestią bezpieczeństwa przy wdrażaniu rozwiązań Internetu rzeczy. W dalszej części tekstu zaprezentowano rekomendacje autorów dotyczące bezpieczeństwa rozwiązań IoT dla przedsiębiorstw i dostawców takich rozwiązań.

Jako najważniejsze dla organizacji wykorzystujących Internet rzeczy warto wyszczególnić następujące wytyczne:

- Należy w pełni zrozumieć potencjał Internetu rzeczy dla danej branży – nie ulega wątpliwości, że Internet rzeczy szybko zdobywa popularność w wielu różnych dziedzinach. Jeśli dana organizacja operuje w jednym z tych kontekstów i jeszcze nie myśli o Internecie rzeczy, najczęściej oznacza to, że jest nieświadoma tego, że wiele z tych elementów może już być używanych przez pracowników, przez co nieświadomie stwarzają oni zagrożenie, którego firma w ogóle nie bierze pod uwagę. Ponadto organizacje bardziej świadome powinny przeanalizować potencjalne korzyści i zagrożenia związane z implementacjami rozwiązań IoT. Pozwoli to zdecydować, które z nich warto wprowadzić jak najszybciej, a z którymi należy się wstrzymać, aż kwestie bezpieczeństwa zostaną lepiej rozwiązane.
- Należy uwzględniać dodatkowe warstwy zabezpieczeń we wszystkim, co wiąże się z Internetem rzeczy. IoT jest wciąż na bardzo wczesnym etapie rozwoju, a przez to jest nadal zbyt wcześnie, aby przewidzieć wszystkie potencjalne zagrożenia, które wiążą się z coraz większą cyfryzacją i podłączeniem miliardów urządzeń w jedną sieć. Dlatego dla organizacji, które już teraz chcą wykorzystywać Internet rzeczy, najlepszym rozwiązaniem jest bycie tak ostrożnym jak to

tylko możliwe. W przypadku projektowania systemów należy (w miarę możliwości) dołączyć zabezpieczenia przynajmniej do warstwy aplikacji i z założenia blokować wszystkie niekluczowe dostępy, działania i procesy. Należy również porozmawiać z dostawcami sprzętu i oprogramowania o tym, w jaki sposób ich aktualne rozwiązania mogą wpłynąć na taki system i jak je najlepiej skonfigurować. Wszyscy międzynarodowi dostawcy rozwiązań IT powinni być w stanie odnieść się do tego trendu i pomóc w odpowiednim dobraniu parametrów innych warstw zabezpieczeń.

Wśród rekomendacji dla dostawców rozwiązań Internetu rzeczy można sformułować m.in. następujące wytyczne:

- Należy zbadać implikacje bezpieczeństwa dla systemów IoT – dostawcy rozwiązań w obrębie Internetu rzeczy, którzy mogą przetwarzać bądź agregować dane, a także dostawcy sensorów i urządzeń, które będą łączyć się tworząc Internet rzeczy, powinni myśleć o bezpieczeństwie w szerszym kontekście. Można to zrobić, biorąc pod uwagę, jakie nowe zagrożenia wynikają z tego ściśle połączonego systemu, w jaki sposób można się przed tymi atakami bronić i jak bardzo aktualne rozwiązania (np. systemy UTM czy *firewall*) są w stanie im zapobiegać.
- Należy zacieśniać współpracę między dostawcami urządzeń i rozwiązań. Organizacje oraz specjaliści zajmujący się bezpieczeństwem IT, a jednocześnie zainteresowani Internetem rzeczy powinni ściśle kooperować z firmami zajmującymi się produkcją urządzeń i oferującymi usługi z ich wykorzystaniem. Dzięki takiej współpracy firmy te będą mogły lepiej identyfikować rozwiązania pozwalające na lepsze zabezpieczenie produktów oraz infrastruktury i razem edukować potencjalnych klientów na temat bezpieczeństwa w zakresie Internetu rzeczy.
- Przede wszystkim należy pracować nad międzynarodowymi standardami. Internet rzeczy, jako wciąż bardzo nieokreślona i ewoluująca koncepcja, jest jeszcze za krótko na rynku, by mieć standardy zapewniające współdziałanie różnych elementów przygotowywanych przez różnych producentów rozwiązań. W związku z tym próby zapewnienia bezpieczeństwa wszystkim elementom i całej infrastrukturze będą musiały być podejmowanie indywidualnie dla różnych rozwiązań. Równocześnie jest to okazja dla zainteresowanych firm i instytucji, aby wziąć udział w budowaniu standardów, które zdefiniują pojęcie i wymagania dotyczące bezpieczeństwa w Internecie rzeczy. Następną kwestią będzie adaptacja tych wypracowanych standardów do nowych i istniejących rozwiązań oraz uświadamianie klientom i partnerom, aby z nich korzystali i je rozpowszechniali.
- W miarę możliwość należy minimalizować oraz zanonimizować dane, które są domyślnie zbieranie przez urządzenia (z możliwością zmiany na bardziej spersonalizowane ustawienie dla świadomych ryzyka użytkowników). Dzięki temu nawet wyciek takich informacji nie spowoduje poważnych konsekwencji dla użytkowników.

W związku z licznymi zagrożeniami dotyczącymi Internetu rzeczy zarówno organizacje, jak i dostawcy rozwiązań powinni podejmować wiele działań mających

na celu minimalizowanie ryzyka związanego z korzystaniem z omawianych technologii. Pożądanych działań i inicjatyw jest sporo, na co dowodem jest m.in. zaproponowana lista rekomendacji.

8. Zakończenie

W artykule zostały przeanalizowane kwestie bezpieczeństwa związane z implementacją koncepcji Internetu rzeczy. Pojęcie to będzie zyskiwać na znaczeniu i w ciągu najbliższych kilku lat na pewno na stałe wejdzie do kanonu rozwiązań wykorzystywanych w wielu nowoczesnych organizacjach i gospodarstwach domowych. Zgodnie z prognozami analityków może się to przyczynić do wzrostu wartości gospodarki o kwotę mieszczącą się w granicach kolejnych 3-6 tryliardów dolarów do roku 2025, o ile nie nastąpi gwałtowny odwrót od tego typu rozwiązań, np. przez nieadekwatne potraktowanie kwestii bezpieczeństwa. Zgodnie z oczekiwaniami hipoteza mówiąca o niewystarczającym uwzględnianiu zagadnień wprowadzanych przez Internet rzeczy w zarządzaniu bezpieczeństwem informatycznym okazała się prawdziwa. Systemy te w sposób pośredni i bezpośredni pozwalają na przeprowadzanie niespotykanych dotąd ataków zarówno na elementy samego Internetu rzeczy, jak również często stanowią punkt wejścia do sieci korporacyjnych i pozwalają atakującym na pominięcie tradycyjnych warstw zabezpieczeń. Przedsiębiorcy oczekują, że odpowiedzialność za pilnowanie tej kwestii powinna spoczywać na działach cyberbezpieczeństwa oraz IT w organizacjach, jak również producentach systemów i urządzeń. Liczba rozwiązań dedykowanych do tych systemów, pozwalających zwiększać bezpieczeństwo, wciąż pozostaje niewielka.

Podsumowując, można stwierdzić, iż kwestie bezpieczeństwa Internetu rzeczy należy rozwiązywać nie tylko za pomocą metod technologicznych, które powinny być wprowadzane zarówno przez producentów sprzętu, jak i użytkowników. Należy również pamiętać o elementach zwiększania świadomości użytkowników oraz wypracowywania branżowych standardów, które pozwolą wszystkim obniżyć poziom ryzyka do akceptowalnego poziomu i cieszyć się innowacjami wpływającymi na wiele aspektów naszego życia.

Literatura

Beecham Research, 2016, *IoT Sector Map*, http://www.beechamresearch.com/article.aspx?id=4 (14.12.2016).

Biuro Bezpieczeństwa Narodowego, 2015, *Doktryna cyberbezpieczeństwa Rzeczpospolitej*, Warszawa, http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf (05.01.2017).

Brachman A., 2013, *Internet przedmiotów. Raport Obserwatorium ICT*, Park Naukowo-Technologiczny „Technopark Gliwice", Gliwice, http://www.technopark.gliwice.pl/files/artykuly/Internet%20 przedmiot%C3%B3w.pdf (1.02.2017).

Cisco, 2016, *Cisco Technology Radar Trends*, http://www.cisco.com/ web/solutions/trends/tech-radar/ (18.12.2016).

Corpuz I., 2014, *A smart vaccine for smart cities*, GulfNews, 20.12.2014, http://m.gulfnews.com/opinion/a-smart-vaccine-for-smart-cities-1.1429472 (17.01.2017).

Fiddian P., 2013, *Explosives Sensors Detect Sewer Chemicals*, Copybook, 6.11.2013, http://www.copybook.com/security/news/explosives-sensorsdetect-sewer-chemicals (30.01.2017).

HP, 2014, *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*, http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676 (3.12. 2016).

Infineon, 2014, *The Right Security for the Internet of Things (IoT)*, http://www.infineon.com/cms/en/applications/smart-card-and-security/internet-of-things-security/ (14.01.2017).

Lipski J., 2015, *Internet rzeczy w zastosowaniu do sterowania produkcją*, [w:] *Innowacje w zarządzaniu i inżynierii produkcji*, t. 2, Knosala R. (red.), Polskie Towarzystwo Zrządzania Produkcją, Opole.

Majdan K., 2015, *Jak się szykować do cyberobrony?,* Gazeta.pl, nr 50, 2.03.2015, http://wyborcza.biz/biznes/1,101716,17503432,Jak_sie_szykowac_do_cyberobrony_.html (17.08.2016).

Manyika J., Chui M., Bughin J., Dobbs R., Bisson P., Marrs A., 2013, *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy*, McKinsey Global Institute, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies (4.02.2017).

McKinsey&Company: McKinsey Global Institute, 2015, *The Internet Of Things: Mapping The Value Beyond The Hype*, http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world (30.10. 2016).

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

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

ONZ, 2012, *State of World Cities*, UN-Habitat, http://mirror.unhabitat.org/pmss/listItemDetails.aspx?publicationID=3387&AspxAutoDetectCookieSupport=1 (7.08.2016).

OWASP, 2014, Open Web Application Security Project, *Internet of Things Top 10*, http://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf (22.12.2016).

Pescatore J., 2014, *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, January 2014, http://www.sans.org/reading-room/whitepapers /covert/securing-internet-things-survey-34785 (5.01.2017).

Rot A., Sobińska M., 2013, *IT security threats in cloud computing sourcing model*, [w:] *Proceedings of the 2013 Federated Conference on Computer Science and Information*, Ganzha M., Maciaszek L., Paprzycki M. (red.), PTI, Kraków, fedcsis.org/proceedings/2013/pliks/fedcsis.pdf (18.11.2016).

Senkus P., Skrzypek A., Łuczak M., Malinowski A., 2014, *Internet of Things: przeszłość – teraźniejszość – przyszłość*, Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, nr 103/2014.

Telecommunication Standardization Sector of ITU, 2006, *Overview of the Internet of things*, ITU, Szwajcaria.

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

TradeArabia, 2014, *Smart cities must protect utilities from cyber-attacks*, TradeArabia, 13.10.2014, http://www.tradearabia.com/news/REAL_267393.html (9.12.2016).