



BEZPIECZEŃSTWO INTERNETU RZECZY. WYBRANE ZAGROŻENIA I SPOSOBY ZABEZPIECZEŃ NA PRZYKŁADZIE SYSTEMÓW PRODUKCYJNYCH

Artur Rot¹, Bartosz Blaike²

¹Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów

²McKinsey & Company
Boston, Massachusetts, USA

Streszczenie: W opinii wielu ekspertów oraz firm analitycznych zagadnienia takie jak cyfryzacja, bezpieczeństwo IT oraz Internet rzeczy to zjawiska, które wyznaczały kierunek rozwoju poszczególnym branżom gospodarki w minionym roku i będą szczególnie istotne w przyszłości. Wśród nich znajduje się Internet rzeczy, wobec którego oczekuje się, że znajdzie wiele zastosowań w różnych dziedzinach, m.in. w energetyce, transporcie, przemyśle, opiece zdrowotnej. Jego zastosowania usprawniają nasze życie, ale stwarzają też nowe zagrożenia i stanowią wyzwanie dla architektów systemów bezpieczeństwa. Eksperci są zdania, że problemy z bezpieczeństwem IT sprzed lat powracają obecnie w nowych urządzeniach i dają hakerom wiele możliwości do cyberataków. Celem artykułu jest przybliżenie koncepcji Internetu rzeczy, obszarów jej zastosowań, ale przede wszystkim identyfikacja zagrożeń wynikających z zastosowań tej koncepcji. Artykuł zawiera również przegląd przypadków użycia Internetu rzeczy w obszarze produkcji, opis zagrożeń dla cyberbezpieczeństwa wynikających z poszerzania dostępu do sieci nowych urządzeń, a także przegląd istniejących zabezpieczeń w tej dziedzinie.

Słowa kluczowe: cyberbezpieczeństwo, Internet rzeczy, podatności, ryzyko, zagrożenia

DOI: 10.17512/znpcz.2017.2.17

Wprowadzenie

Postępujący proces informatyzacji tworzy coraz bardziej połączone i zaawansowane technologicznie narzędzia do zwiększania wydajności pracy oraz ułatwiania życia codziennego. Jedną ze znaczących nowych koncepcji jest Internet rzeczy (ang. *Internet of Things* – IoT). Dzięki bardzo szybkiemu postępowi adopcji urządzeń wchodzących w skład Internetu rzeczy konsumenci oraz przedsiębiorcy mają możliwość wykorzystywania wielu innowacji w różnych obszarach, tym samym powiększając ilość potencjalnych punktów ataku. Szybko rozwijający się Internet rzeczy niesie ze sobą całkiem nowe rodzaje ryzyka dla jego użytkowników. W związku z tym należy zadać sobie pytanie, czy rozwiązania te są już wystarczająco bezpieczne, aby można je było wdrażać do systemów przetwarzających informacje? Ponadto należy sprawdzić, czy istnieją już odpowiednie mechanizmy

zabezpieczające te ściśle połączone systemy tak, aby w bezpieczny sposób można było korzystać z wprowadzenia tego typu rozwiązań.

Zastosowania IoT niosą wiele korzyści, ale stwarzają także zupełnie nowe zagrożenia, wśród których najczęściej wymieniane są problemy z prywatnością danych, słabe punkty w systemach autoryzacji i uwierzytelnienia, niezabezpieczone interfejsy WWW, luki i błędy w oprogramowaniu. Dlatego też celem artykułu jest przegląd obecnie występujących przypadków użycia Internetu rzeczy, opis zagrożeń dla cyberbezpieczeństwa wynikających z poszerzania dostępu do sieci nowych urządzeń i procesów, które pierwotnie nie były do tego przystosowane, a także przegląd wybranych rozwiązań dedykowanych do zabezpieczenia Internetu rzeczy w obszarze produkcji. Istotą artykułu jest także przedstawienie argumentów potwierdzających hipotezę, mówiącą, iż zabezpieczenie systemów w obszarze IoT nie jest aktualnie wystarczająco uwzględniane w ramach zarządzania bezpieczeństwem informatycznym.

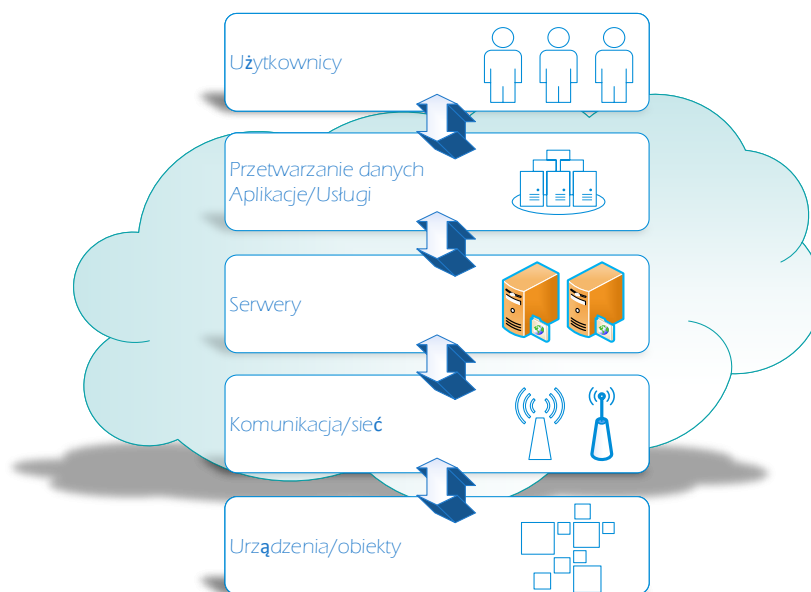
Koncepcja Internetu rzeczy

Internet rzeczy może być interpretowany jako ogół inteligentnych przedmiotów, mogących reagować na środowisko oraz przetwarzać i pamiętać informacje cyfrowe, a także przysyłać je do innych obiektów (i ich użytkowników) za pośrednictwem protokołów internetowych (Nowakowski 2015). Jest on 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. Według prognoz firmy Gartner w 2020 roku do Internetu podłączonych będzie 26 mld urządzeń, co oznacza ogromny przyrost ilości danych, które trzeba będzie odpowiednio (przede wszystkim bezpiecznie) przechowywać i przetwarzać (Middleton, Kjeldsen, Tully 2013).

Koncepcja ta staje się powoli obowiązkowym elementem technologii w biznesie, a dzięki sieci połączonych urządzeń, zasobów ludzkich i zgromadzonych danych firmy będą mogły lepiej zrozumieć wymagania klientów i szybciej wprowadzać zmiany w łańcuchu dostaw czy implementować innowacje. IoT może też wpłynąć na poprawę jakości życia ludzi, którzy będą mogli wykonywać zdalne płatności, monitorować swój stan zdrowia, sprawdzać dostępność miejsc parkingowych itp. (EY 2015). Na *Rysunku 1* zaprezentowano koncepcję IoT, gdzie przedstawiona jest interakcja pomiędzy warstwami, a całość obejmuje chmura obliczeniowa, w której zachodzi większość procesów.

Elastyczność i skalowalność usług chmury obliczeniowej umożliwia obsługę dużej liczby danych i użytkowników. IoT składa się z zasobów materialnych i wirtualnych. Do elementów infrastruktury materialnej należy zaliczyć (Maciejewski, Morawski 2016):

- czujniki (np. wizualne, dźwiękowe, pozycyjne, temperatury);
- siłowniki oraz urządzenia (serwery, komputery, urządzenia przenośne).



Rysunek 1. Ogólny model Internetu rzeczy

Źródło: Opracowanie własne na podstawie (Niyato i in. 2012)

Do zasobów wirtualnych zaliczamy (Maciejewski, Morawski 2016):

- komunikację (sieć bezprzewodowa i przewodowa, podczerwień);
- pamięć (bazy danych, zdecentralizowane systemy rozproszone DHT);
- identyfikację (obraz video, kody, odczyty biometryczne, informacje z tagów i kodów kreskowych);
- lokalizację (sygnały GSM, GPS);
- procesy (serwis, sieci czujników, obsługa sieci).

Do najczęstszych zastosowań technologicznych Internetu rzeczy należy zaliczyć technologię automatycznej identyfikacji RFID, która wykorzystuje fale radiowe do przesyłania danych oraz zasilania elektronicznego układu stanowiącego etykietę obiektu przez czytnik, w celu jego identyfikacji.

Obszary zastosowań Internetu rzeczy

Obszarów zastosowania Internetu rzeczy może być wiele oraz mogą one przenikać wiele aspektów życia. Według firmy Gartner IoT będzie generować przychody przekraczające 300 mld USD, głównie w usługach (Middleton, Kjeldsen, Tully 2013). Z kolei według raportu McKinsey & Company (McKinsey & Company 2015) IoT ma szansę utworzyć korzyści ekonomiczne dla światowej gospodarki szacowane między 2,7 a 6,2 trylionów USD już w 2025 roku. IoT znajdzie wiele zastosowań w wielu dziedzinach działalności gospodarczej, m.in. w energetyce, produkcji, logistyce, opiece zdrowotnej, sektorze IT. Oczekiwania na szybki roz-

wój IoT są powiązane z zastosowaniami tej technologii w inteligentnym budownictwie, inteligentnych miastach i samochodach, w automatyce przemysłowej określanej jako Przemysł 4.0. Jedną z klasyfikacji obszarów zastosowań koncepcji przedstawiona została przez Beecham Research (Beecham Research 2016) (Tabela 1).

Tabela 1. Najważniejsze obszary zastosowań Internetu rzeczy

Lp.	Sektor	Przykładowe wybrane obszary zastosowań
1	Budownictwo	Sterowanie ogrzewaniem, wentylacją, klimatyzacją, kontrolą dostępu, oświetleniem, systemami bezpieczeństwa w budynkach itp.
2	Energetyka	Wydobycie surowców, poszukiwania alternatywnych (odnawialnych) źródeł energii, urządzenia dostarczające prąd.
3	Sektor konsumpcyjny/ domowy	Bezpieczeństwo w domu (alarmy, monitorowanie osób starszych i dzieci), sterowanie urządzeniami, energią i oświetleniem w domu, rozrywka.
4	Opieka zdrowotna i nauki przyrodnicze	Telemedycyna, domowe systemy monitoringu pacjentów (osób starszych lub np. osób z wszczepionymi rozrusznikami serca), badania i rozwój nowych leków i sprzętu medycznego.
5	Przemysł/produkcja	Monitorowanie i śledzenie aktywów, urządzeń i produktów przemysłowych, analiza lokalizacji dla szerokiej gamy procesów fabrycznych.
6	Transport	Zarządzanie flotą pojazdów (systemy nawigacji, zarządzanie systemem dystrybucji), systemy informacji dla pasażerów, systemy płatności za korzystanie z infrastruktury transportowej i parkingowej.
7	Sektor detaliczny	Zarządzanie łańcuchem dostaw, zarządzanie informacją o produktach/klientach, zarządzanie zapasami, maszyny sprzedające (żywność, napoje), parkometry, urządzenia wyświetlające (billboardy, wyświetlacze).
8	Bezpieczeństwo publiczne	Monitorowanie środowiska, informacje meteorologiczne i klimatyczne, śledzenie ludzi, zwierząt, przesyłek, bezpieczeństwo militarne.
9	Sektor IT	Urządzenia biurowe, infrastruktura transmisji mobilnej, centra danych (systemy utrzymania energii i klimatyzacyjne), e-commerce itp.

Źródło: Opracowanie własne na podstawie (Beecham Research 2017)

Istnieją pewne sfery życia społeczno-gospodarczego, które posiadają największy potencjał do tworzenia wartości przez wykorzystanie koncepcji Internetu rzeczy. Według firmy konsultingowej McKinsey & Company jest ich dziewięć i obejmują one rozwiązania przeznaczone dla (Bauer, Pater, Veira 2014): ludzi (*human*), mieszkań (*home*), handlu detalicznego (*retail environments*), biur (*office*), fabryk (*factories*), miejsc pracy / placów budowy (*worksites*) (np. miejsca wydobywania ropy naftowej), pojazdów (*vehicles*), miast (*cities*), obszarów zewnętrznych (*outside*), tj. obszarów znajdujących się pomiędzy środowiskami zurbanizowanymi.

Jednocześnie potencjalny wpływ ekonomiczny Internetu rzeczy będzie się mocno różnić w odniesieniu do poszczególnych sfer jego oddziaływania. Według prognoz firmy McKinsey do roku 2025 największy będzie w sferze związanej

z produkcją (1,2-3,7 biliona USD), najmniejszy natomiast w sferze biurowej (70-150 mld USD) (Bauer, Pater, Veira 2014). Podsumowując, można stwierdzić, iż Internet rzeczy wspiera nieomal wszystkie dziedziny życia i jest już nieodłącznym elementem funkcjonowania społeczeństwa informacyjnego.

Bezpieczeństwo jako najważniejsze wyzwanie Internetu rzeczy

Jeśli chodzi o kwestie bezpieczeństwa, to fakt, iż systemy IoT zbudowane są z olbrzymiej ilości różnego typu połączonych urządzeń stanowiących potencjalnie nowe punkty nieautoryzowanego dostępu, powoduje, że aspekty związane z zapewnieniem odpowiedniego poziomu ich bezpieczeństwa stają się kluczowe (Wielki 2016).

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. Niekontrolowana inwigilacja ludzi, zagrożenia wynikające z działalności hakerów oraz przejęcie kontroli nad urządzeniami to najważniejsze niebezpieczeństwa, które wraz z rozpowszechnieniem IoT staną się realnymi zagrożeniami dla bezpieczeństwa użytkowników. Luki znajdują się w szeregu urządzeń, 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. Włamanie się do inteligentnego zegarka czy opaski, która mierzy puls i ciśnienie oraz rejestruje i transmituje dane o stanie zdrowia użytkownika, nie stanowi często dużego wyzwania (Józefiak 2016). Wiele urządzeń umożliwiających odczytywanie zawartych w nich danych przy zastosowaniu technologii bezstykowej jest podatnych na podsłuchy i skimming, czyli nielegalne skopiowanie zawartości bez wiedzy jej posiadacza w celu utworzenia kopii i wykonywania nieuprawnionych transakcji (Kobyliński 2014).

Badania Instytutu SANS zidentyfikowały największe ryzyka związane z Internetem rzeczy, do których zaliczono (Pescatore 2014):

- problemy z aktualizacją oprogramowania obiektów;
- wykorzystanie obiektów, jako najsłabiej zabezpieczonych punktów wejścia do sieci, w celu kolejnych infekcji czy ataków;
- ataki typu DoS (ang. *Denial of Service*), które w przypadku np. infrastruktury sieci energetycznej czy urządzeń medycznych mogą prowadzić do 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 systemu połączonych urządzeń.

Jak pokazują badania przeprowadzone przez specjalistów firmy HP (HP 2014), wiele urządzeń IoT jest podatnych na atak, a praktycznie każde z nich posiada słabe punkty, dotyczące bezpieczeństwa haseł, kryptografii, braku odpowiedniego zarządzania kontrolą dostępu. Firma HP przetestowała 10 popularnych urządzeń

Internetu przedmiotów, odkrywając średnio 25 luk w urządzeniu. Najczęstsze problemy bezpieczeństwa obejmowały:

- Problemy z prywatnością danych – zanotowano podatności dotyczące prywatności związanej z gromadzeniem danych osobowych (imię, nazwisko, e-mail, adres zamieszkania, data urodzenia, numer karty kredytowej oraz informacje na temat zdrowia itp.). Wiele 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 (wiele urządzeń pozwalało na używanie trywialnych haseł).
- Brak szyfrowania transmisji danych – 70% badanych urządzeń nie szyfrowało komunikacji z Internetem i sieciami lokalnymi, a połowa aplikacji mobilnych stosowanych do obsługi tych urządzeń przysyłała niezaszyfrowane komunikaty w chmurze obliczeniowej, Internecie lub sieci lokalnej.
- Niebezpieczne interfejsy WWW – w 6 z 9 testowanych urządzeń zanotowano obawy związane z bezpieczeństwem interfejsów użytkownika.
- Niewystarczający poziom bezpieczeństwa oprogramowania – 60% urządzeń nie stosowało szyfrowania podczas aktualizacji oprogramowania.

Eksperti HP zaznaczają, że wraz z dynamicznym rozwojem IoT konieczne jest, aby organizacje tworzące rozwiązania w ramach Internetu rzeczy identyfikowały podatność systemu, zanim zostaną one wykorzystane w praktyce. Odbywać się to powinno poprzez m.in. dokładne testy oprogramowania i proaktywne eliminowanie podatności w rozwijanych aplikacjach (HP 2014).

Kontekst środowiska produkcyjnego

Zastosowania Internetu przedmiotów w kontekście produkcji

Systemy przemysłowe od dawna wykorzystują automatyzację, roboty i różnego rodzaju połączenia w celu usprawniania procesów produkcji. Obecnie jednak widzimy wyraźne zacieranie granicy między systemami informatycznymi, tzw. IT, a systemami operacyjnymi, tzw. OT. Zostało to zapoczątkowane przez programowalne kontrolery logiczne (ang. *Programmable Logic Controller* – PLC) oraz zdalne jednostki transmisji (ang. *Remote Terminal Unit* – RTU), które podłączają urządzenia do Internetu w celach monitoringu, utrzymania i zarządzania tymi maszynami zdalnie często nawet z urządzeń mobilnych (Turner 2014). Jak już wspomniano, prognozy firmy McKinsey & Company przewidują, iż do roku 2025 największy wpływ ekonomiczny Internetu rzeczy będzie miał miejsce w sferze związanej z produkcją (1,2-3,7 biliona USD).

Pomimo że linie produkcyjne stają się coraz bardziej zautomatyzowane, a roboty zastępują ludzi, to obecnie szacuje się, że tylko około 10% środowisk produkcyjnych jest podłączonych do Internetu (Wakefield 2014). To, co w kontekście produkcji przynosi Internet rzeczy, wspierany przez chmurę obliczeniową, to większa możliwość kontroli procesów w czasie rzeczywistym, co przekłada się na

większą ich efektywność (Kapeliński 2016), a tym samym lepszą pozycję konkurencyjną przedsiębiorstwa, bez względu na to, czy jest to fabryka samochodów, farma czy inny rodzaj produkcji.

W obszarze produkcji omawiana koncepcja może znaleźć i znajduje zastosowanie w następujących trzech głównych obszarach (Lipski 2015):

- Systemy diagnostyki maszyn technologicznych – w systemy sterowania maszyn technologicznych wbudowuje się procedury diagnostyczne, zabezpieczając je już w trakcie uruchamiania przed eksploatacją w stanach awaryjnych. Te systemy diagnostyczne służą identyfikacji nieprawidłowej pracy systemów (wykrywają problemy np. z zasilaniem elektrycznym, hydraulicznym, diagnozują niesprawność podzespołów oraz niesprawność układów pomiarowych) oraz potrafią diagnozować także poprawność swojego działania, informując o tym w odpowiednich komunikatach.
- Systemy diagnostyki narzędzi i oprzyrządowania produkcyjnego – systemy wykrywające zużycie narzędzi. Informacje takie transmitowane są do chmury obliczeniowej, gdzie po obliczeniach generowana jest decyzja o wysłaniu i automatycznej wymianie narzędzia, np. zainstalowane na obrabiarce czujniki wysyłają dane o bieżącym stanie narzędzi.
- Systemy kontroli jakości wyrobów – analiza zmian parametrów kolejnych wyrobów pozwala pozyskać informację o zmianach w czasie cech istotnych dla jakości produktów, co zmierza do zmniejszenia ryzyka powstania braków.

Dla zobrazowania powyższych możliwości warto przytoczyć przykład firmy General Electric, która w fabryce baterii Durathon zainstalowała 10 000 sensorów na linii produkcyjnej oraz instaluje sensor w każdej produkowanej baterii. Dzięki temu istnieje możliwość sprawdzania w czasie rzeczywistym stanu produkcji nawet indywidualnej sztuki produktu i udostępniania tych danych pracownikom. Dzięki temu eliminuje się jakiegokolwiek braki informacji i pozwala uzyskać optymalne środowisko produkcji (Wakefield 2014).

Sieci sensoryczne zbudowane z elementów Internetu rzeczy są również wykorzystywane w rolnictwie, np. do pomiaru parametrów gruntu przy uprawach, takich jak wilgotność, poziom pH, ilość związków mineralnych oraz chemicznych, które mogą znacząco zwiększyć efektywność upraw. Internet rzeczy w tym kontekście często wykorzystuje koncepcje sieci opartej na topologii siatki, w której każdy punkt może się łączyć z każdym, tworząc skomplikowaną strukturę. Dzięki temu sieć taka będzie w stanie działać, nawet jeśli część sensorów ulegnie uszkodzeniu lub zostanie przemieszczona. Coraz popularniejsze stają się również wszczepianie bydłu hodowlanemu specjalnych sensorów. Istnieją już zaawansowane systemy automatyzacji hodowli bydła, które mogą monitorować skład krwi, temperaturę mleka, a nawet markery płodności w celu zwiększania efektywności produkcji (Billhardt 2015).

Przykłady ataków oraz potencjalnych zagrożeń w kontekście produkcji

Systemy produkcji z założenia nie były projektowane jako elementy Internetu rzeczy. Potwierdza to m.in. badanie przeprowadzone pod koniec 2013 roku, które

zidentyfikowało 25 błędów niewykrytych przez producentów oprogramowania systemów SCADA (ang. *zero-day exploit*). Błędy te mogą zostać wykorzystane przez potencjalnych atakujących (Ashford 2013).

Jednym z bardziej spektakularnych ataków przeprowadzonych z wykorzystaniem złośliwego oprogramowania o nazwie Stuxnet był atak na irańskie ośrodki wzbogacania uranu. Robak Stuxnet został odkryty w czerwcu 2010 roku i na początku rozprzestrzenił się dzięki lukom w systemie operacyjnym Microsoft Windows, jednak jego ostatecznym celem były systemy SCADA firmy Siemens, które były wykorzystywane przez irański program nuklearny. Systemy te nie były nawet podłączone do Internetu, ale Stuxnet przedostał się do tej zamkniętej sieci poprzez zainfekowanie przenośnej pamięci, która została podłączona do systemu operacyjnego Windows w jednej z placówek. Nieoficjalnie mówi się, że robak ten był efektem współpracy tajnych służb Stanów Zjednoczonych oraz Izraela (Kelley 2013).

Wybrane rozwiązania oraz sposoby zabezpieczania rozwiązań w kontekście produkcji

Istnieją firmy, które pomagają zabezpieczać systemy w obszarze produkcji, ale wywodzą się one bardziej z tradycyjnego podejścia do cyberbezpieczeństwa niż koncepcji IoT. Pojawiają się jednak również rozwiązania dedykowane, np.:

- Firma Bayshore w czerwcu 2014 roku wprowadziła do swojej oferty cztery specjalnie zaprojektowane systemy SCADA firewall warstwy 7, właśnie w celu zabezpieczenia tych systemów w kontekście IoT. Według firmy istniejące systemy nie mają żadnej możliwości zarządzania politykami bezpieczeństwa, zalecając, aby osoby na stanowiskach administratorów bezpieczeństwa skupiły się na zabezpieczaniu istniejących systemów w konkretnych zastosowaniach poprzez identyfikację możliwych wektorów ataku (Bayshore 2014).
- Firma Alutech ma w swojej ofercie usługi testów penetracyjnych, projektowania zabezpieczeń, jak również procesów biznesowych wpływających na bezpieczeństwo systemów SCADA oraz kontroli przemysłowej (Alutech 2017).
- Jedną z firm, która stworzyła rozwiązanie bezpieczeństwa dla Internetu rzeczy w tym kontekście od podstaw jest Skkynet, która na targach M2M Expo 2015 otrzymała nagrodę za najlepsze rozwiązanie w kategorii bezpieczeństwa. System Skkynet Cloud System pozwala systemom przemysłowym na bezpieczne przesyłanie danych w czasie rzeczywistym do dowolnej lokalizacji wewnątrz bądź na zewnątrz sieci firmowej. Jest to rozwiązanie, które łączy każdy z istniejących elementów sieci w chmurę obliczeniową i z założenia nie wymaga połączeń VPN, otwartych portów na urządzeniu firewall ani żadnych modyfikacji oprogramowywania i sprzętu. Jest w stanie obsłużyć do 50 000 jednoczesnych połączeń na sekundę, jak również daje możliwość równoczesnego dostępu do danych przez wielu użytkowników (Skkynet Cloud Systems 2015).

Jednakże z uwagi na szybki postęp Internetu rzeczy rozwiązania, których celem jest ochrona niektórych elementów systemów IoT w obszarze środowiska produkcyjnego, dopiero się pojawiają i jeszcze nie stanowią powszechnego standardu.

Podsumowanie

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 firmach i gospodarstwach domowych. Zgodnie z oczekiwaniami, hipoteza mówiąca o niewystarczającym uwzględnianiu zagadnień wprowadzanych przez IoT w zarządzaniu bezpieczeństwem informacyjnym okazała się prawdziwa. Systemy te, w sposób pośredni i bezpośredni pozwalają na przeprowadzanie niespotykanych dotąd ataków zarówno na części samego Internetu rzeczy, jak również często stanowią punkt wejścia do sieci korporacyjnych i pozwalają atakującym na pominięcie tradycyjnych warstw zabezpieczeń. Taki stan rzeczy istnieje również w obszarze systemów produkcji, co wskazano w artykule na wybranych przykładach.

Podsumowując, należy stwierdzić, iż kwestie bezpieczeństwa Internetu rzeczy w różnych obszarach, w tym i produkcji, 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.

Literatura

1. Alutech (2017), *SCADA & ICS Cyber Security*, <http://www.alutech-ics.com> (dostęp: 24.04.2017).
2. Ashford W. (2013), *US Researchers Find 25 Security Vulnerabilities in SCADA Systems*, Computer Weekly, <http://www.computerweekly.com/news/2240207488/US-researchers-find-25-securityvulnerabilities-in-SCADA-systems> (dostęp: 12.05.2017).
3. Bauer H., Patel M., Veira J. (2014), *The Internet of Things: Sizing up the Opportunity*, McKinsey & Company, <http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity> (dostęp: 12.05.2017).
4. Bayshore (2014), *Bayshore Networks Announces Four New SCADA Firewalls*, <http://www.bayshorenetworks.com/2014/07/bayshore-networks-announces-four-newscada-firewalls/> (dostęp: 30.04.2017).
5. Beecham Research (2016), *IoT Sector Map*, <http://www.beechamresearch.com/article.aspx?id=4> (dostęp: 17.02.2017).
6. Billhardt K. (2015), *IoT in Action: The Connected Cow*, Industrial Internet Consortium, <http://blog.iiconsortium.org/2015/01/staying-connected-through-cows.html> (dostęp: 04.05.2017).
7. EY (2015), *Insights on Governance, Risk and Compliance: Cybersecurity and the Internet of Things*, [http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/\\$FILE/EY-cybersecurity-and-the-internet-of-things.pdf](http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf) (dostęp: 19.03.2017).
8. 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> (dostęp: 27.02.2017).
9. Józefiak B. (2016), *Internet rzeczy nie będzie bezpieczny*, CyberDefence24, <http://www.cyberdefence24.pl/384609,internet-rzeczy-nie-bedzie-bezpieczny> (dostęp: 28.12.2016).

10. Kapeliński W. (2016), *Wpływ technologii Cloud Computing na organizację oraz efektywność procesu operacyjnego planowania produkcji*, „Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie”, nr 23, t. 1, s. 83-91.
11. Kelley M.B. (2013), *The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, *Business Insider*, <http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11> (dostęp: 09.05.2017).
12. Kobyliński A. (2014), *Internet przedmiotów: szanse i zagrożenia*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług”, nr 112, t. 1, s. 101-109.
13. Lipski J. (2015), *Internet rzeczy w zastosowaniu do sterowania produkcją*, [w:] Knosala R. (red.), *Innowacje w zarządzaniu i inżynierii produkcji*, t. 2, Polskie Towarzystwo Zarządzania Produkcją, Opole, s. 755-766.
14. Maciejewski M., Morawski P. (2016), *Wykorzystanie koncepcji Internetu rzeczy w społeczeństwie informacyjnym*, „Przedsiębiorczość i Zarządzanie”, t. 17, z. 11, cz. 1: *Agile Commerce – zarządzanie informacją i technologią w biznesie*, s. 141-153.
15. McKinsey & Company (2015), *The Internet of Things: Mapping the Value Beyond the Hype*, *McKinsey Global Institute*, <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world> (dostęp: 30.10.2016).
16. Middleton P., Kjeldsen P., Tully J. (2013), *Forecast: The Internet of Things*, Worldwide 2013, Gartner, www.gartner.com/doc/2625419/forecast-internet-things-worldwide- (dostęp: 23.02.2017).
17. Niyato D., Lu X., Wang P., Kim D.I., Han Z. (2012), *Economics of Internet of Things (IoT): An Information Market Approach*, Computer Science.
18. Nowakowski W. (2015), *Bliższa chmura, czyli usługi obliczeniowe we mgle*, „Elektronika – Konstrukcje, Technologie, Zastosowania”, nr 5, http://www.imm.org.pl/imm/plik/pliki-dobrania-elektronika52015_nn358.pdf (dostęp: 18.02.2017), s. 34-37.
19. Pescatore J. (2014), *Securing the Internet of Things Survey*, SANS Institute InfoSec Reading Room, <http://www.sans.org/reading-room/whitepapers/covert/securing-internet-things-survey-34785> (dostęp: 17.03.2017).
20. Skkynet Cloud Systems (2015), *Skkynet Wins Best IoT Security Solution Award at M2M Expo 2015*, Reuters, <http://www.reuters.com/article/2015/02/03/skkynet-cloud-systemsidUSnBw035226a+100+BSW20150203> (dostęp: 11.03.2017).
21. Turner R. (2014), *Security Implications of the Internet of Things*, December 2014, <https://www.ovum.com/research/security-implications-of-the-internet-of-things/> (dostęp: 12.05.2017).
22. Wakefield K.J. (2014), *How the Internet of Things Is Transforming Manufacturing*, „Forbes”, 1 July 2014, www.forbes.com/sites/ptc/2014/07/01/how-the-internet-of-things-is-transformingmanufacturing (dostęp: 15.03.2017).
23. Wielki J. (2016), *Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu rzeczy przez współczesne organizacje gospodarcze*, „Przedsiębiorczość i Zarządzanie”, t. 17, z. 11, cz. 1: *Agile Commerce – zarządzanie informacją i technologią w biznesie*, s. 127-140.

INTERNET OF THINGS SECURITY. SELECTED THREATS AND PROTECTIONS METHODS ON THE EXAMPLE OF MANUFACTURING SYSTEMS

Abstract: In the opinion of many experts and research companies, issues such as digitization, IT security and the Internet of Things are the phenomena that set the direction for different economy sectors in the past year and will be particularly important in the future. The Internet of Things is expected to find many applications in various fields, like in power engineering, transport, industry, healthcare etc. Its applications improve our lives, but also create new threats and challenges for security architects. Experts are of the opinion that IT security problems from past years are coming back in new devices and giving hackers a lot of opportunities for cyber-attacks. The aim of the article is to describe the concept of the Internet of Things, areas of its applications, but above all, to identify the risks arising from the applications of this concept in practice. The article also includes an overview of the use of the Internet for Things in the area of manufacturing sector, a description of the cyber security risks resulting from widening access to the network of new devices, and an overview of selected existing security countermeasures in this area.

Keywords: Cybersecurity, Internet of Things, Risk, Threats, Vulnerabilities