Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 341 · 2017

Artur Rot

Uniwersytet Ekonomiczny we Wrocławiu
Wydział Zarządzania, Informatyki i Finansów
Katedra Systemów Informacyjnych
artur.rot@ue.wroc.pl

Bartosz Blaicke

McKinsey & Company
bartosz_blaicke@mckinsey.com

ZAGROŻENIA WYNIKAJĄCE Z IMPLEMENTACJI KONCEPCJI INTERNETU RZECZY W WYBRANYCH OBSZARACH ZASTOSOWAŃ

Streszczenie: Według raportu Cisco zagadnienia takie jak cyfryzacja, bezpieczeństwo IT oraz Internet rzeczy to zjawiska, które wyznaczały kierunek rozwoju poszczególnych branż gospodarki w 2016 r. 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 przegląd wybranych przypadków użycia Internetu rzeczy, opis zagrożeń dla cyberbezpieczeństwa wynikających z poszerzania dostępu do sieci nowych urządzeń, a także przegląd istniejących zabezpieczeń.

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

JEL Classification: G34, M19.

Wprowadzenie

Postępujący proces informatyzacji społeczeństwa tworzy coraz bardziej połączone i zaawansowane technologicznie narzędzia do zwiększania wydajności pracy oraz ułatwiania życia codziennego. Jedną ze znaczących nowych koncepcji jest Internet rzeczy (*Internet of Things*, IoT). Dzięki bardzo szybkiemu rozwojowi urządzeń wchodzących w skład Internetu rzeczy konsumenci oraz przedsiębiorcy mają możliwość wykorzystywania wielu innowacji w różnych obszarach, tym samym powiększając ilość potencjalnych punktów ataku.

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 korzystać z wprowadzenia tego typu rozwiązań. 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 istniejących rozwiązań specjalnie przeznaczonych do zabezpieczenia Internetu rzeczy w wybranych kontekstach. Istotą niniejszego artykułu jest również wskazanie, iż zabezpieczenie systemów w obszarze Internetu rzeczy nie jest wystarczająco uwzględniane w ramach zarządzania bezpieczeństwem informatycznym.

1. 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. Według Cisco Internet Business Solutions Group 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, i to wtedy właśnie narodził się Internet rzeczy. W 2011 r., dzięki popularyzacji smartfonów, tabletów i innych urządzeń mobilnych, liczba urządzeń podłączonych do Internetu wyniosła ponad 13 mld (liczba ludności osiągnęła 7 mld) [Raymond, 2014]. Badania OECD pokazują, że obecnie krajem z największą liczbą urządzeń podłączonych do Internetu na 100 mieszkańców jest Korea Południowa (wskaźnik 37,9), w pierwszej dziesiątce jest 8 państw europejskich, w Polsce współczynnik ten wynosi 6,3 [EY, 2015]. Firma Gartner szacuje, iż w 2020 r. IoT będzie dotyczył ponad 26 mld urządzeń [Middleton i in., 2013]. Ta olbrzymia ilość urządzeń będzie generować ogromne ilości informacji, które trzeba będzie w sposób bezpieczny przechowywać i przetwarzać. Według niektórych szacunków w 2020 r. na każdego człowieka będzie przypadać ok. 5,2 PB danych (1 PB = 1015 bajtów) [Evans, 2011].

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 i wielu in-

nych. Zastosowania tej koncepcji usprawniają nasze życie, ale stwarzają także zupełnie nowe zagrożenia i stanowią jednocześnie znaczące wyzwanie dla architektów systemów bezpieczeństwa. Wśród najczęstszych zagrożeń i podatności IoT wymieniane są problemy z prywatnością danych, słabe punkty w systemach autoryzacji i uwierzytelnienia, niezabezpieczone interfejsy WWW, błędy w oprogramowaniu.

Pomimo oczywistego związku IoT z wzajemnie połączonymi i komunikującymi się przedmiotami brak jednoznacznej definicji tego zjawiska [Van Kranenburg i in., 2011]. Idea Internetu rzeczy po raz pierwszy pojawiła się w artykule *The Computer for the 21st Century* autorstwa Weisera [1991] z firmy Xerox Parc, a sam termin został po raz pierwszy użyty w 1999 r. przez Ashtona [2009] z Massachusetts Institute of Technology, współtwórcy globalnego systemu identyfikacji produktów w standardzie RFID (*radio-frequency identification*). 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].

Internet rzeczy 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. Może on też wpłynąć na poprawę jakości życia ludzi, którzy będą mogli wykonywać zdalne płatności, monitorować swój stan zdrowia, sprawdzać dostępność miejsc parkingowych itp. Inteligentne systemy zarządzania odpadami, energią czy ruchem ulicznym stają się powoli codzienną rzeczywistością [EY, 2015].

2. Bezpieczeństwo Internetu rzeczy

Rozwój Internetu rzeczy wymusza opracowywanie nowych rozwiązań, zwiększanie wydajności sieci, bezpieczeństwa danych oraz tworzenie jednolitych standardów, co stanowi wyzwanie dla całego sektora IT. Możliwość podłączenia dosłownie każdego elementu codziennego życia, takiego jak pralka, lodówka czy oświetlenie, do globalnej sieci tworzy szanse dla biznesu 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), ataków na słabe hasła i ataków *cross-site scripting* (osadzenie w treści atakowanej strony kodu, który wyświetlony użytkownikom może doprowadzić do wykonania przez nich niepożądanych akcji).

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 najważniejsze niebezpieczeństwa, które wraz z rozpowszechnieniem IoT staną się realnymi zagrożeniami dla bezpieczeństwa użytkowników. 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. 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].

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,
- wspomniane ataki typu DoS, które w przypadku np. infrastruktury sieci energetycznej czy urządzeń medycznych mogą prowadzić do bardzo poważnych konsekwencji,
- nieuprawnione modyfikacje parametrów działania urządzeń,
- błędy użytkowników i przypadkowe modyfikacje, które w sieci bardzo silnie połączonych ze sobą systemów mogą prowadzić do trudnych do przewidzenia konsekwencji w skali całego systemu połączonych urządzeń.

Producenci urządzeń i oprogramowania powinni zadbać o bezpieczeństwo na każdym etapie rozwoju swojego produktu, zająć się opracowaniem możliwie najlepszych kodów oraz zapewnieniem bezpiecznego standardu współpracy między poszczególnymi urządzeniami. Wyzwaniem dla instytucji standaryzacyjnych jest wprowadzenie standardów w tym zakresie, a dla różnych organizacji wprowadzanie certyfikatów branżowych. Tworzenie dedykowanych, zamkniętych systemów znacznie zmniejszy prawdopodobieństwo nadużyć.

Wszystkie te sposoby podniesienia poziomu bezpieczeństwa są głównie odpowiedzialnością producentów i programistów tego typu rozwiązań. Użytkownik ma ograniczone możliwości, by zwiększyć swoje bezpieczeństwo [Józefiak, 2016]. Należy jednak pamiętać o konieczności zwiększania świadomości użytkowników w zakresie bezpiecznego korzystania z urządzeń oraz ich oprogramowania.

3. Wybrane obszary zastosowań Internetu rzeczy

Obszarów zastosowania Internetu rzeczy może być wiele i mogą one przenikać wiele aspektów życia. 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 prezentuje najważniejsze obszary zastosowań Internetu rzeczy.

Tabela 1. Przegląd najważniejszych obszarów występowania Internetu rzeczy

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, jak hotele, restauracje, banki, sklepy itp. Przykładem są np. 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

Źródło: Opracowanie własne.

Internet rzeczy znajdzie wiele zastosowań w różnych dziedzinach usługowych i w działalności gospodarczej. Oczekiwania na szybki rozwój Internetu rzeczy są powiązane także z zastosowaniami tej technologii w inteligentnym budownictwie, inteligentnych miastach i samochodach oraz w automatyce przemysłowej określanej mianem przemysłu 4.0.

Możliwość podłączenia wielu elementów codziennego użytkowania, takich jak pralka, lodówka czy oświetlenie, do globalnej sieci tworzy możliwości biznesowe i znaczne oszczędności dla gospodarstw domowych i organizacji. W dalszej części artykułu syntetycznie scharakteryzowane zostaną wybrane obszary zastosowań Internetu rzeczy, takie jak: miasto, dom, handel i usługi. Podane zostaną przykłady realizacji omawianej koncepcji w praktyce, przykłady ataków oraz zagrożeń, a także istniejące rozwiązania i sposoby zabezpieczeń.

4. Kontekst miasta

4.1. Zastosowania Internetu rzeczy w kontekście miasta

Internet rzeczy zaczął być rozpoznawalny głównie za sprawą zastosowań związanych z inteligentnym zarządzaniem ruchem samochodowym, inteligentnymi sieciami przesyłu elektryczności czy wody (s*mart grid*). Znaczenie tego kontekstu podnosi fakt, że coraz większa część populacji ulega urbanizacji i do 2050 r. ponad 60% ludzkości będzie mieszkać w miastach, więc ilość osób obcujących z tą technologią będzie ogromna [ONZ, 2012].

Przykładów zastosowań omawianej koncepcji w kontekście miasta jest wiele. W 2012 r. miasto Amsterdam przy współpracy z firmami Cisco oraz Philips zainstalowało inteligentny system oświetlenia ulicznego. 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, przeprowadza automatycznie ściemnianie, gdy nie ma dużego natężenia ruchu, oraz inteligentne planowanie. Obecnie mówi się już o wykorzystaniu sieci, która powstała dzięki połączeniu oświetlenia ulicznego, do innych usług publicznych [Mitchell, 2013].

W 2013 r. Szwecja postanowiła wykorzystać sieć połączonych sensorów zanurzonych w rurach do odprowadzania ścieków w celu wykrywania chemikaliów służących do budowy materiałów wybuchowych „domowej produkcji". Projekt jest nadzorowany przez Szwedzką Agencję Rozwoju Obronności [Fiddian, 2013].

Nicea przy pomocy firmy Cisco wprowadziła inteligentne usługi w mieście oparte 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 i warstwę sensorów [Mitchell, 2013].

4.2. Przykłady ataków oraz potencjalnych zagrożeń w kontekście miasta

Ataki na Internet rzeczy, który występuje w miastach czy na większą skalę w całych państwach, mogą być pierwszym etapem w konflikcie między państwami, a więc pełnić funkcję tzw. cyberwojny. Dzieje się tak dlatego, że poprzez atak na taki system atakujący są w stanie spowodować znaczące utrudnienia lub straty na dużym obszarze geograficznym. W przypadku ataków na inteligentne liczniki możemy wyróżnić następujące ataki i zagrożenia:

- 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 (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.

Jeśli weźmiemy pod uwagę scenariusze, w których 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 danego przedsiębiorstwa,
- wywołanie chaosu lub obniżenie sprawności/obronności danego 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 (SCADA) w mieście Springfield (Illinois, USA). Co więcej, nie musiał wykorzystywać do tego żadnych skomplikowanych aplikacji, gdyż trzyliterowe hasło administracyjne było bardzo proste do złamania [Townsend, 2013].

4.3. Istniejące rozwiązania oraz sposoby zabezpieczania rozwiązań w tym zakresie

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 on na trzech silnikach analitycznych, które obserwują różne elementy i ich zachowania w systemie, a w przypadku wykrycia anomalii natychmiastowo reagują [Corpuz, 2014].

5. Kontekst domu i miejsca zamieszkania

5.1. Zastosowania Internetu rzeczy w kontekście domu i miejsca zamieszkania

Inteligentne urządzenia domowe zaczynają coraz śmielej wkraczać do domów na całym świecie. Tego typu systemy zbierają informacje z różnych urządzeń domowych, takich jak centra rozrywki, inteligentne telewizory, inteligentne termostaty i in. Firmy takie jak Whirlpool, Samsung czy LG już mają na rynku pierwsze produkty inteligentnych urządzeń AGD, a inteligentne telewizory są w większości domów. Telewizory te mają własne systemy operacyjne, pozwalają na dostęp do Internetu, ściąganie aplikacji, a nawet prowadzenie rozmów wideokonferencyjnych przez wbudowane kamery. Często te same kamery i mikrofony służą do rozpoznawania gestów i słów, a tym samym obsługi telewizora, a potencjalnie nawet do ustalania liczby osób jednocześnie przebywających przed telewizorem.

Ważnym zastosowaniem Internetu rzeczy w kontekście domu są systemy monitoringu oraz przeciwwłamaniowe. Łączą one różne sensory, takie jak czujniki ruchu oraz dźwięku, kamery, sensory na oknach, w jeden system. Jest on podłączony do sieci Internet, więc pozwala na podgląd na żywo tego, co dzieje się w domu, jak również może wysyłać automatyczne komunikaty do właściciela czy odpowiednich służb [Kumar, 2014].

Inteligentne sprzęty AGD, takie jak podłączone do Internetu lodówki, mogą automatycznie zamawiać brakujące produkty lub sugerować przepisy z rzeczy znajdujących się wewnątrz, piekarniki i zmywarki mogą być zdalnie uruchamiane i kontrolowane. Zostały one wyposażone w algorytmy przetwarzania mowy ludzkiej, więc można się z nimi także komunikować za pomocą wiadomości tekstowych. Inteligentne żarówki mają wbudowany moduł komunikacyjny (Wi-Fi lub bluetooth) i pozwalają na łączenie ich w grupy, a następnie na zdalną kontrolę jasności, barwy itp. Inteligentne termostaty można programować przez aplikacje mobilne, a po połączeniu z innymi urządzeniami mogą pomagać w zmniejszaniu rachunków. Aby zobrazować potencjał Internetu rzeczy w tym kontekście warto wspomnieć, że w 2014 r. firma Google przejęła start-up zajmujący się produkcją inteligentnych termostatów Nest Labs za aż 3,2 mld dol. [Winkler iWakabayashi, 2014].

5.2. Przykłady ataków oraz potencjalnych zagrożeń w kontekście domu

Wraz z rosnącą popularnością tego typu systemów w naszych domach można spodziewać się coraz większej ilości ataków wymierzonych w te systemy. Niestety, badania części tych systemów pokazują, że bezpieczeństwo nie jest w tym przypadku najważniejszym kryterium. W styczniu 2014 r. w Internecie pojawiły się informacje o robaku komputerowym, który wysyła spam poprzez sieć zainfekowanych inteligentnych lodówek. Firma Symantec wykazała, że źródłem niechcianej poczty elektronicznej były zainfekowane komputery z systemem Windows, które współdzieliły adres IP z urządzeniami domowymi.

W 2015 r. firma Samsung zaczęła ostrzegać użytkowników swoich telewizorów z włączoną funkcją rozpoznawania mowy przed omawianiem prywatnych kwestii przy włączonym telewizorze. Okazuje się, że wszystko, co użytkownicy mówią, kiedy TV jest włączony, może zostać podsłuchane, a duża część tych nagrań może zostać wysłana przez Internet do serwerów firmy w celu analizy pod kątem tego, czy dana komenda może być zrealizowana lub czy może usprawnić działanie istniejącego mechanizmu.

Badania, które analizowały zabezpieczenia systemów inteligentnego domu wykazały, że są one stanowczo niewystarczające. Jak pokazują badania przeprowadzone przez specjalistów firmy HP [HP, 2015], wiele urządzeń IoT jest podatnych na atak, a każde z nich ma słabe punkty dotyczące bezpieczeństwa haseł, kryptografii, braku odpowiedniego zarządzania kontrolą dostępu, które rozszerzają możliwości nadużyć przez intruzów. Firma HP przetestowała 10 popularnych domowych urządzeń IoT, odkrywając średnio 25 luk w urządzeniu

(łącznie 250 zagrożeń bezpieczeństwa w analizowanych produktach). Urządzenia te wraz z ich aplikacjami mobilnymi pochodziły od producentów telewizorów, kamer, termostatów, kontrolerów energii, urządzeń do sterowania alarmami, otwieraniem drzwi garażowych itp. Najczęstsze problemy bezpieczeństwa obejmowały następujące zagadnienia:

- problemy z prywatnością danych – w 8 na 10 urządzeń wykryto podatności dotyczące prywatności związanej z gromadzeniem danych osobowych (imię i nazwisko, e-mail, adres, data urodzenia, numery karty kredytowej, 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,
- brak szyfrowania transmisji danych – 70% badanych urządzeń nie szyfrowało komunikacji, a połowa aplikacji mobilnych stosowanych do obsługi tych urządzeń przesyłała niezaszyfrowane wrażliwe dane w chmurze, Internecie lub sieci lokalnej,
- niebezpieczne interfejsy WWW – w 6 z 10 testowanych urządzeń zanotowano obawy związane z bezpieczeństwem interfejsów użytkownika, takie jak: narażenie na ataki *cross-site scripting*, złe zarządzanie sesjami itp.,
- niewystarczający poziom bezpieczeństwa oprogramowania – 60% urządzeń nie stosowało szyfrowania podczas pobierania aktualizacji oprogramowania. Niektóre pobrania mogły być przechwycone, wyodrębnione, przejrzane i modyfikowane.

Za największy problem można uznać fakt, że żaden z przetestowanych przez firmę HP systemów nie wymuszał mocnych haseł, a z 7 interfejsów do połączenia z chmurą obliczeniową można było wyciągać listę kont.

5.3. Istniejące rozwiązania oraz sposoby zabezpieczania rozwiązań w tym zakresie

Niestety, nie ma systemów bezpieczeństwa przeznaczonych specjalnie do zastosowań domowych. Każdy z producentów stosuje (bądź nie) własne zabezpieczenia, z których można korzystać niezależnie. Na szczęście można wyróżnić konkretne działania, o których użytkownicy powinni pamiętać, aby zmniejszyć ryzyko ataku [Barcena i Wueest, 2015]:

- używać silnych haseł do sieci bezprzewodowych oraz urządzeń,
- bezwzględnie zmieniać domyślnie ustawione hasła,
- używać silniejszych metod kodowania transmisji, np. WPA2 w przypadku Wi-Fi,

- wyłączać i ograniczać możliwości zdalnego dostępu do przedmiotów,
- sprawdzać, jakie zabezpieczenia w danej rzeczy zastosował producent,
- modyfikować ustawienia prywatności w urządzeniach, które na to pozwalają,
- wyłączać funkcjonalności, z których nie korzystamy,
- instalować aktualizacje oprogramowania, zwłaszcza poprawki bezpieczeństwa,
- utworzyć osobne sieci domowe z różnym przeznaczeniem, jeśli to możliwe.

Przestrzeganie powyższych rekomendacji może zdecydowanie ograniczyć ryzyko wystąpienia incydentu zagrażającego bezpieczeństwu urządzeń Internetu rzeczy.

6. Kontekst handlu i usług

6.1. Zastosowania Internetu rzeczy w kontekście handlu i usług

W ostatnim czasie, głównie za sprawą ataków na największe firmy zajmujące się handlem detalicznym w USA (Target oraz Home Depot), wiele firm zdało sobie sprawę z realności cyberzagrożeń. Ataki te powodują nie tylko utratę reputacji, wpływając na długoterminową sytuację firmy, ale również bardzo znaczące straty finansowe (46% spadku zysków firmy Target w kwartale po wykryciu ataku i nagłośnieniu go w mediach) [IBM, 2014].

Zwiększanie sprzedaży oraz optymalizacja działania łańcucha dostaw są silnym motorem napędowym inwestycji firm. Rozwiązania Internetu rzeczy celują właśnie w te potrzeby. Lokalizowane oraz personalizowane promocje prawdopodobnie będą przyszłością handlu i usług. Mamy już pewien przedsmak tego typu działań w postaci kart lojalnościowych, które zbierają informacje o zakupach, a następnie dobierają spersonalizowane promocyjne produkty na podstawie wcześniejszych zakupów. Kolejnym etapem jest podłączenie tych mechanizmów do lokalizacji GPS, gdzie dostajemy informacje o promocjach w sklepach znajdujących się niedaleko nas. Nietrudno sobie wyobrazić, że po dołączeniu do tego informacji z sensorów, takich jak pomiar aktywności fizycznej czy poziomu glukozy (ludzie są skłonni więcej kupić, będąc głodnymi), będzie można te oferty jeszcze bardziej dopasować.

Dzięki niewielkich rozmiarów sensorom czy mikroczipom cały łańcuch dostaw może być kontrolowany. Jest to szczególnie ważne w przypadku transportu żywności, gdzie parametry takie jak np. czas i temperatura przechowywania, stopień wstrząsów oraz inne pozwalają stwierdzić świeżość, a nawet przydatność do spożycia, wymuszając z jednej strony przestrzeganie norm i zasad BHP, a z drugiej gwarantując konsumentom jakość produktów.

6.2. Przykłady ataków oraz potencjalnych zagrożeń w kontekście handlu i usług

Jednym z najbardziej spektakularnych ataków na firmy z sektora handlu był atak na firmę Target sprzedającą elektronikę konsumencką, który rozpoczął się pod koniec 2013 r. Spowodował on wyciek danych z kart kredytowych aż 110 mln klientów. Atak rozpoczął się dzięki luce w zabezpieczeniach inteligentnego systemu klimatyzacji. Przez to, że sieć techniczna nie była odseparowana od sieci korporacyjnej, atakujący byli w stanie zainfekować ok. 40 tys. urządzeń do przyjmowania płatności, takich jak czytniki kart kredytowych, i przez długi czas kopiować informacje z kart klientów. Oprócz strat w działalności, jakie przyniósł ten atak (46-procentowy spadek zysków w pierwszym kwartale po ujawnieniu ataku), firma została również obciążona kosztami 10 mln dol. w ramach ugody z sądem [Griswold, 2015].

Podobnym atakiem wykorzystującym ten sam złośliwy kod był atak na sieć sklepów Home Depot z akcesoriami biurowymi. W tym przypadku nastąpił wyciek 56 mln danych kart kredytowych oraz dodatkowych 53 mln adresów e-mail klientów. Nie jest znany sposób wejścia do systemu, jednak ponownie udało się zainfekować urządzenia służące do płatności i przez długi czas nie było to wykryte m.in. dlatego, że firma używała nieaktualnych baz antywirusowych i nie prowadziła monitoringu aktywności sieciowej [Krebs, 2014].

6.3. Istniejące rozwiązania oraz sposoby zabezpieczania rozwiązań w tym zakresie

Firma IBM, oprócz gamy standardowych rozwiązań związanych z bezpieczeństwem, ma również rozwiązania przeznaczone dla tego typu przedsiębiorstw. Platforma IBM QRadar Security Intelligence stanowi podstawę, która analizuje zagrożenia, zbiera dane o podatnościach urządzeń, może kontrolować konfiguracje urządzeń oraz monitorować aktywność sieciową. Natomiast IBM Trusteer Apex jest rozwiązaniem, które dzięki analizie behawioralnej blokuje ataki i przeciwdziała atakom na podatności, które nie zostały jeszcze naprawione, oraz tzw. atakom *zero-day*, czyli takim, gdzie wykorzystuje się nieujawnione jeszcze podatności [IBM, 2014].

Podsumowanie

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 w wielu firmach i gospodarstwach domowych. Zgodnie z prognozami analityków może się to przyczynić do wzrostu wartości gospodarki o kolejne 3-6 tryliardów dol. do 2025 r., 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 liczba tych rozwiązań będzie wzrastać, poszerzając ilość potencjalnych punktów ataku.

Obecnie istnieje niewiele wyspecjalizowanych rozwiązań, które są w stanie zapobiegać lub częściowo adresować znane oraz nowe podatności i metody ataku. Jak wskazano w artykule, zabezpieczenie systemów w obszarze Internetu rzeczy nie jest wystarczająco uwzględniane w ramach zarządzania bezpieczeństwem informatycznym. Systemy te pozwalają na przeprowadzanie niespotykanych dotąd ataków zarówno na części samego Internetu rzeczy, często też stanowią punkt wejścia do sieci i pozwalają atakującym na pominięcie tradycyjnych warstw zabezpieczeń.

Podsumowując, 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 wypracowywaniu branżowych standardów, które pozwolą obniżyć poziom ryzyka do akceptowalnego poziomu [Rot, 2008].

Literatura

Ashton K. (2009), *That 'Internet of Things' Thing. In the Real World, Things Matter More Than Ideas*, „RFID Journal", 22.06, www.rfidjournal.com/articles/pdf?4986 (dostęp: 27.09.2015).

Barcena M.B., Wueest C. (2015), *Insecurity in the Internet of Things*, Symantec, Mountain View, CA, https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf (dostęp: 12.02.2017).

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

Corpuz I. (2014), *A Smart Vaccine for Smart Cities*, „GulfNews", 20.12, http://m.gulfnews.com/opinion/a-smart-vaccine-for-smart-cities-1.1429472 (dostęp: 17.01.2017).

Evans D. (2011), *The Internet of Things. How the Next Evolution of the Internet is Changing Everything*, Cisco Internet Business Solutions Group, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (dostęp: 16.12.2016).

EY (2015), *Insights on Governance, Risk and Compliance: Cybersecurity and the Internet of Things*, www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf (dostęp: 4.01.2017).

Fiddian P. (2013), *Explosives Sensors Detect Sewer Chemicals*, „Copybook", 6.11, http://www.copybook.com/security/news/explosives-sensorsdetect-sewer-chemicals (dostęp: 30.01.2017).

Griswold A. (2015), *Target Finally Agrees to Pay Up for Its Massive Data Breach*, http://www.slate.com/blogs/moneybox/2015/03/19/target_data_breach_settlement_the_company_will_pay_out_10_million_to_make.html (dostęp: 19.01.2017).

HP (2015), *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: 3.12.2016).

IBM (2014), *The Challenge of Digital Security*, IBM, Armonk, NY.

Józefiak B. (2016), *Internet rzeczy nie będzie bezpieczny*, „CyberDefence24", www.cyberdefence24.pl/384609,internet-rzeczy-nie-bedzie-bezpieczny (dostęp: 28.12.2016).

Kobyliński A. (2014), *Internet przedmiotów: szanse i zagrożenia*, „Zeszyty Naukowe" nr 808, „Ekonomiczne Problemy Usług", nr 112.

Kranenburg R. van, Anzelmo E., Bassi A., Caprio D., Dodson S., Ratto M. (2011), *The Internet of Things*, 1st Berlin Symposium on Internet and Society, October 2011, Berlin.

Krebs B. (2014), *Home Depot: Hackers Stole 53M Email Addresses*, Krebs on Security, http://krebsonsecurity.com/tag/homedepot-breach/ (dostęp: 16.12.2016).

Kumar M. (2014), *Internet of Things Spending Guide by Vertical Market*, IDC, Framingham, MA.

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

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

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

Nowakowski W. (2015), *Bliższa chmura, czyli usługi obliczeniowe we mgle*, „Elektronika – Konstrukcje, Technologie, Zastosowania", nr 5, www.imm.org.pl/imm/plik/pliki-do-pobrania-elektronika52015_nn358.pdf (dostęp: 16.12.2016).

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

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

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

Rot A. (2008), *IT Risk Assessment: Quantitative and Qualitative Approach* [w:] Ao S.I., Douglas C., Grundfest W.S., Schruben L., Burgstone J. (eds.), *Lecture Notes in Engineering and Computer Science*: *WCECS2008 World Congress on Engineering and Computer Science*, Newswood Limited, IAENG, San Francisco, CA.

Rot A., Sobińska M. (2013), *IT Security Threats in Cloud Computing Sourcing Model* [w:] M. Ganzha, L. Maciaszek, M. Paprzycki (eds.), *Proceedings of the 2013 Federated Conference on Computer Science and Information*, PTI, Kraków, fedcsis.org/proceedings/2013/pliks/fedcsis.pdf (dostęp: 18.11.2016).

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, http://www.tradearabia.com/news/REAL_267393.html (dostęp: 9.12.2016).

Weiser M. (1991), *The Computer for the 21st Century*, „Scientific American", No. 265(3).

Winkler R., Wakabayashi D. (2014), *Google to Buy Nest Labs for $3.2 Billion*, „The Wall Street Journal", http://www.wsj.com/articles/SB10001424052702303595404579318952802236612 (dostęp: 4.02.2017).

THREATS ARISING FROM THE IMPLEMENTATION OF THE CONCEPT OF THE INTERNET OF THINGS IN SELECTED AREAS OF APPLICATIONS

Summary: According to the Cisco report, issues such as digitization, IT security and the Internet of Things are phenomenon, which determined the direction of development of the economy sectors in 2016 and will be particularly important in the coming years. Among them is the IoT which is expected to find many applications in various areas, like energy, transport, industry, construction, health care. Its applications enhance our lives, but also pose new threats and is a challenge for IT security architects. Experts think that the IT security problems from the past return now with new devices and provide many opportunities for hackers to cyberattacks. The aim of the article is a review of selected cases of the usage of the IoT, description of threats to cybersecurity resulting from widening access of new devices to the Internet, and an overview of the existing safeguards.

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