https://doi.org/10.21784/ZC.2023.016

Krzysztof Ciemcioch
Uczelnia Nauk Społecznych

ORCID: https://orcid.org/0000-0002-9654-8227

Internet Rzeczy – zastosowanie, zagrożenia, bezpieczeństwo

Internet of Things – application, dangers, security

Streszczenie. Pojęcie Internet Rzeczy jest znane od początku XXI wieku, lecz mimo wielu zalet tej technologii wynikającej z jej użytkowania i wykorzystania, wciąż pozostaje spora grupa osób, która nie zdaje sobie sprawy, że korzystając ze smart urządzeń, tak naprawdę korzystają z najnowszych rozwiązań wchodzących w skład IoT. Celem artykułu jest zaprezentowanie zebranych informacji o Internecie Rzeczy, jego zastosowaniu i implementacji w różnych gałęziach gospodarki i korzyściach dla użytkowników w życiu codziennym. Kolejnym celem jest również identyfikacja zagrożeń IoT, wpływających na nasze bezpieczeństwo oraz samo zabezpieczanie przetwarzanych zbieranych danych.

Słowa kluczowe: Internet Rzeczy, zastosowanie IoT, zagrożenia IoT, bezpieczeństwo IoT, nowe technologie

Abstract. The concept of the Internet of Things has been known since the beginning of the 21st century, but despite many advantages of this technology resulting from its use and application, there is still a large group of people who do not realize that when using smart devices, they actually use the latest solutions included in the IoT. The aim of the article is to present a collection of information concerning the Internet of Things, its application and implementations in various branches of the economy as well as its benefits for users in everyday life. Another goal is also the identification of IoT threats affecting our security as well as protecting the collected processed data.

Keywords: Internet Rzeczy, zastosowanie IoT, zagrożenia IoT, bezpieczeństwo IoT, nowe technologie

The Internet of Things has the potential to change
the world, just as the Internet did. Maybe even more so.

[Kevin Ashton]

Wstęp

Rozwój nowych technologii towarzyszy nam w każdej dziedzinie codziennego życia. Czwarta rewolucja przemysłowa[1] sięga początkiem XXI wieku, ale dzięki Internetowi Rzeczy (ang. *Internet of Things* IoT) stała się jednym z najważniejszych komponentów w rozwoju Przemysłu 4.0[2]. Smart technologia znana jest od końca ubiegłego wieku, ale dopiero teraz można zaobserwować jej zwiększone tempo rozwoju i rozkwit. Technologia ta „stała się synonimem swego rodzaju «tech rewolucji» - zarówno z perspektywy biznesu, konsumentów, jak i dostarczanych za jej sprawą usług"[3]. Producenci z różnych branż prześcigają się w implementowaniu najnowszych innowacji technologicznych opartych o inteligentne rozwiązania, zamykając je w jak najmniejsze urządzenia (smart urządzenia). Wszystko po to, by dać społeczeństwu kolejne gadżety, narzędzia i urządzenia, całe systemy poprawiające standard życia, dające poczucie zwiększonego bezpieczeństwa. Dostęp do tej technologii stał się bardziej powszechny, ponieważ realizowany jest generalnie poprzez smartfon, który obecnie jest przedłużeniem ręki każdego przeciętnego obywatela. „Dzięki najróżniejszym aplikacjom, z poziomu smartfona sterujemy światłem, infrastrukturą bezpieczeństwa, telewizorem, a nawet piekarnikiem"[4].

[1] G. Owczarek, A. Hłobaż, *Bezpieczeństwo teleinformatyczne w systemach przemysłowego Internetu rzeczy na przykładzie środowiska pracy*, Bezpieczeństwo pracy 2/2019, s. 8.

[2] J Pizon, *Koncepcja wdrożenia technologii „Internetu Rzeczy" w systemie logistycznym przedsiębiorstwa*, Systemy Logistyczne Wojsk nr 4/2015, s. 122; Ł. Dragun, G. Dąbrowska, P. Olszyńska, *Identyfikacja barier wdrażania rozwiązań z zakresu Internetu Rzeczy w wybranych segmentach gospodarki*, Akademia Zarządzania 5(1)/2021, s.178.

[3] M. Sikorski, *Internet Rzeczy*, Real IT World nr 1/2020, Adam Roman (red.), PWN, s.12

[4] M. Kanwnik, *Smart home, smart cities, smart world. Rozwój Internetu Rzeczy (IoT)*, Raport Cyfrowej Polski, https://cyfrowapolska.org/wp-content/

Mimo wielu zalet z wykorzystania technologii Internetu Rzeczy, wciąż pozostaje spora grupa osób, która nie zdaje sobie sprawy, że używając smart urządzeń, tak naprawdę korzystają z najnowszych rozwiązań wchodzących w skład IoT. „Gdyby zapytać statystycznego obywatela świata o IoT, to śmiem wątpić, czy byłby on w stanie opisać i wymienić, czym jest IoT, z czego się składa i gdzie na co dzień można się zetknąć z tymi rozwiązaniami”[5].

Celem artykułu jest zaprezentowanie zebranych informacji o Internecie Rzeczy, jego zastosowaniu i implementacji w różnych gałęziach gospodarki oraz korzyściach i zagrożeniach, wpływających na nasze bezpieczeństwo.

Celem podjętych działań było rozwiązanie problemu badawczego zawartego w pytaniach: Czy korzystanie z technologii Internetu Rzeczy jest bezpieczne dla użytkowników indywidualnych, firm, miast czy państwa? W jaki sposób wykorzystać nową technologię w codziennym życiu? Co wiemy o otaczającej nas cyfrowej rewolucji jaką jest Internet Rzeczy?

Jako hipotezę przyjęto, iż większość urządzeń wykorzystywanych w Internecie Rzeczy nie posiada odpowiednich technicznych zabezpieczeń dbających o bezpieczeństwo, które byłyby w stanie zmniejszyć podatność na istniejące zagrożenia. Kolejnym elementem jest zbyt mała świadomość użytkowników dotycząca zarówno korzyści jakie drzemią w nowej technologii, jak również wpływu czyhających na nich zagrożeń dotyczących m.in. prywatności.

Osiągnięcie tego celu badawczego było możliwe dzięki zastosowaniu metody jakościowej wykorzystywanej do analizy treści. Metoda ta bazuje na zgromadzonym materiale dotyczącym danego tematu, który odzwierciedla dotychczasowe doświadczenia, przekonania, opinie i wyniki badań. Analizowany materiał zawarty był w licznych artykułach i publikacjach, a także wybranych tekstach na portalach i w witrynach internetowych.

uploads/2020/11/Raport_Rynek-IOT_2020_net.pdf?fbclid=IwAR161N-T6_kg0PpW03yn9lnqdwCgd9AAWW3vjDdBsWejKUk8UOlc0g5ytsw (dostęp: 25.02.2023), Warszawa, 2020, s. 4.

[5] M. Sikorski, *Internet Rzeczy…*, op.cit., s. 11.

Internet Rzeczy – charakterystyka zjawiska

Pierwsze wzmianki dotyczące idei „Internetu Rzeczy", jakie pojawiły się w literaturze, to badania amerykańskiego socjologa Marka Weisera z firmy Xerox Parc, opublikowane w artykule *The Computer for the 21st Century*[6] w 1991 roku. Opisane tam twierdzenia zyskały miano zasad Weisera, które mówią, że „urządzenia powinny pozostać niezauważone i uaktywniać się w tych momentach, w których mają świadczyć pewne usługi ludziom"[7]. Natomiast samego terminu „Internet Rzeczy" (ang. *Internet of Things* – IoT) użył Kevin Ashton z Auto-ID Center w Massachusetts Institute of Technology podczas prezentacji dla koncernu Procter&Gamble w 1999 roku, gdzie powiązał to pojęcie z koncepcją wykorzystania fal radiowych w technologii RFID w łańcuchach dostaw koncernu[8]. K. Ashton zauważył, iż większość informacji, które znajdują się w internecie zostały wprowadzone przez ludzi, czy to w formie pisanej, plików audio, wideo, czy zdjęć. Ludzie ze względu na ograniczony czas, nieuwagę i małą dokładność byli według niego wąskim gardłem w przechwytywaniu danych o rzeczach w prawdziwym świecie. I tu powstała możliwość wprowadzenia zmian w technologii poprzez wyposażenie komputerów „w ich własne środki gromadzenia informacji, aby mogły widzieć, słyszeć i wąchać świat dla siebie, w całej jego przypadkowej chwale. Technologia RFID i czujników umożliwia komputerom obserwowanie, identyfikowanie i rozumienie świata — bez ograniczeń związanych z danymi wprowadzanymi przez człowieka"[9]. Jednak o narodzinach „Internetu Rzeczy" można mówić od 2011, kiedy to, zgodnie z opracowaniem Cisco Internet Bussines Solutions Group, nastąpił moment, gdy liczba urządzeń rzeczy, obiektów podłączonych

[6] M. Weiser, *The Computer for the 21st Century*, Scientific American Special Issue on Communications, Computers, and Networks, 265(3), 1991, s. 94-104.

[7] J. Rykowski, *Internet Rzeczy – czy mamy zacząć się bać?*, Napędy i Sterowanie Nr 3 Marzec 2017 r., s.121.

[8] B. Krupanek, R. Bogacz, *Węzły końcowe systemów Internetu* Rzeczy, Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej Nr 59/2018, s. 111-116; Kavin Ashton jest współtwórcą globalnego systemu identyfikacji wyrobu w standardzie RFID (ang. *Radio-Frequency IDentification).*

[9] K. Ashton, *That "Internet of Things"…,* op.cit.

do Internetu przekroczyła liczbę ludności na świecie[10]. Było to możliwe dzięki gwałtownemu wzrostowi popularności technologii mobilnej i powszechnemu dostępowi do urządzeń, np. smartfonów. Każdy potencjalny użytkownik tego typu urządzenia, posiadał dostęp do niezliczonej liczby aplikacji, za pomocą których mógł sterować i komunikować się z innymi inteligentnymi urządzeniami w domu, np. oświetleniem, piekarnikiem, lodówką czy ustawić temperaturę za pomocą termostatu.

Ciągły rozwój IoT i różnorodność urządzeń z wielu dziedzin życia podłączonych do Internetu spowodował, że ciężko jest jednoznacznie zdefiniować tą technologię. Jednocześnie wielu badaczy tematu oraz autorów licznych publikacji podaje własne zmodyfikowane wersje definicji. Coraz częściej Internet Rzeczy (IoT) utożsamiany jest błędnie jako Internet Wszechrzeczy (ang. Internet Everything – IoE). IoT składa się tylko z „rzeczy", natomiast IoE tworzą oprócz „rzeczy", także „procesy, dane, ludzie, a nawet zwierzęta czy zjawiska atmosferyczne – wszystko, co może zostać potraktowane jako zmienna"[11].

Związek Pracodawców Branży Internetowej IAB Polska definiuje „pojęcie Internetu Rzeczy rozumiane jest jako ekosystem, w którym przedmioty mogą komunikować się między sobą, za pośrednictwem człowieka lub bez jego udziału" [12].

[10] Zob.: A Rot, *Bezpieczeństwo jako najważniejsze wyzwanie koncepcji Internetu rzeczy*, Przedsiębiorczość i Zarządzanie 2017, Tom XVIII, Zeszyt 4, Część II, s.286; M. Ogórek, P, Zaskórski, *Internet Rzeczy w integracji procesów zarządzania kryzysowego*, Organizacja i Zarządzanie Nr 76, 2018, Zeszyty Naukowe Politechniki Poznańskiej, s.201.

[11] P. Kolenda, *Raport – Internet Rzeczy w Polsce*, iab Polska, 2016, s. 8; Należy wspomnieć również o rozwoju i wdrażaniu Internetu Nano Rzeczy (ang. *Internet of Nano Things* – IoNT), Przemysłowym Internecie Rzeczy (ang. *Industrial Internet of Things* – IIoT) oraz o Internecie Zachowań (ang. *Internet of Behaviour* – IoB). Za: E. Musiał, *Bezpieczeństwo człowieka w świecie smart. Analiza wyników badań wśród studentów*, Studia Administracji i Bezpieczeństwa nr 12/2022, s.84 i 86; A. Abramczyk, *Raport: Internet Rzeczy w przemyśle*, Controling Engineering Polska, 19.02.2020, https://controlengineering.pl/raport-internet-rzeczy-w-przemysle/ (dostęp: 26.02.2023).

[12] Ibidem.

Grupy robocza ds. Internetu Rzeczy[13] przy Ministerstwie Cyfryzacji przedstawiła natomiast własny raport, w którym zaproponowała definicje IoT z różnych perspektyw:

„Definicja technologiczna – IoT to sieć łącząca przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym (niewymagającym zaangażowania człowieka) działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych lub wchodzenia w interakcje z otoczeniem pod wpływem tych danych. Jest to koncepcja budowy sieci telekomunikacyjnych i systemów informatycznych o wysokim stopniu rozproszenia, które służyć mogą między innymi tworzeniu inteligentnych systemów kontrolno-pomiarowych, analitycznych, czy układów sterowania, praktycznie w każdej dziedzinie życia, gospodarki czy nauki.

Definicja architektoniczna – IoT to koncepcja architektury informatycznej, która umożliwia współpracę (interoperacyjność) różnorodnych systemów teleinformatycznych wspierających rozmaite zastosowania dziedzinowe i jest oparta na następujących warstwach:

Sprzęt – urządzenia (lub przedmioty w nie wyposażone), w szczególności sensory, elementy wykonawcze, ale także sterowniki, smartfony, tablety, laptopy czy komputery, które zdolne są do komunikacji i przetwarzania danych bez zaangażowania człowieka lub w ograniczonej z nim interakcji.

Komunikacja – infrastruktura telekomunikacyjna oraz sieć telekomunikacyjna (przewodowa lub bezprzewodowa), pracująca w oparciu o dowolne standardy transmisji danych o dowolnym zasięgu (tu Internet).

Oprogramowanie – systemy informatyczne urządzeń IoT oraz oprogramowanie służące do wymiany danych, ich przetwarzania, zarządzania systemem i jego zabezpieczenia.

[13] Grupa Robocza ds. Internetu Rzeczy (ang. *Internet of Things* – IoT) stanowi forum dialogu administracji rządowej ze stroną społeczną - biznesem, organizacjami pozarządowymi, ośrodkami akademickimi i naukowo-badawczymi na temat obszarów, w których konieczna jest poprawa warunków dla rozwoju i upowszechniania wdrożeń IoT oraz technik przetwarzania danych z nim związanych (Cloud, Edge, Fog Computing), https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-internetu-rzeczy-internet-of-things-iot (dostęp: 26.02.2023).

Integracja – zbiory zdefiniowanych usług informatycznych zapewniających interoperacyjność oprogramowania na wszystkich poziomach architektury.

Definicja biznesowa – IoT to ekosystem usług biznesowych, wykorzystujących przedmioty zdolne do zbierania i przetwarzania informacji (interakcji), połączone w sieć, zapewniające interoperacyjność i synergię zastosowań. Łączenie produktów/usług Internetu Rzeczy pozwala na lepsze zrozumienie konsumenta, środowiska, produktów oraz procesów, identyfikację istotnych zdarzeń i reagowanie celem natychmiastowego optymalizowania czy precyzyjniejszej personalizacji" [14].

Z przytoczonych powyżej definicji można przedstawić model działania Internetu Rzeczy (rys. 1), który w swojej koncepcji bazuje na komunikacji zawsze, wszędzie i z każdym innym urządzeniem podłączonym do dowolnej sieci. Ale żeby doszło do takiej komunikacji pomiędzy rzeczami a ludźmi, lub pomiędzy rzeczami między sobą (ang. *Machine to Machine* – M2M) muszą zostać spełnione następujące warunki:

„Urządzenie wyposażone w sensor, które jest w stanie zebrać z otoczenia określone informacje, a następnie przekazać je dalej. Mogą to być przedmioty wyposażone w rozmaitego rodzaju czujniki: temperatury, drgań, wilgotności, ruchu, GPS, itd. Rolę nadajnika pełnić może również smartfon, z poziomu którego wydaje się polecenia. Różnica polega jedynie na tym, że dane nie są pobierane automatycznie, tylko za pośrednictwem akcji wywołanej przez użytkownika (np. kliknięcia, polecenia głosowego). Przykładami mogą być: opaska na rękę typu smartband monitorująca tętno, prześcieradło wyposażone w czujnik ruchu czy też beacon[15] wykrywający ruch człowieka.

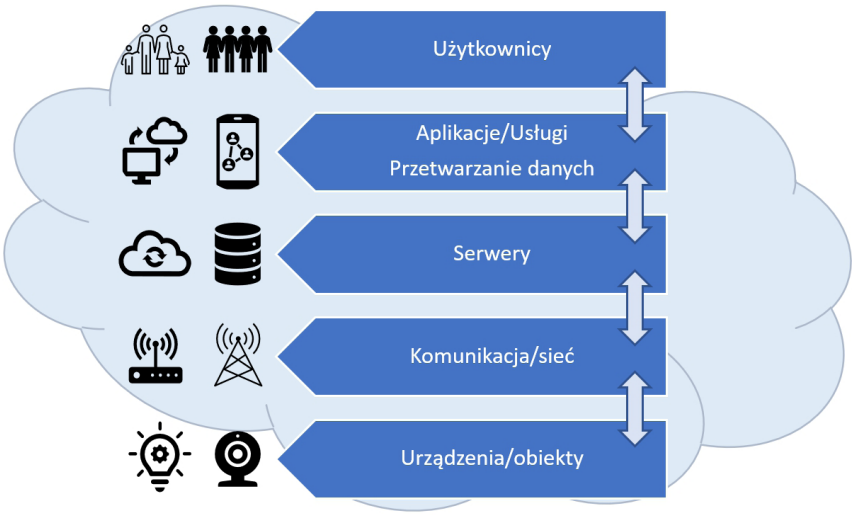
[14] L. Maśniak, M. Kawecki, Ministerstwo Cyfryzacji, *IoT w polskiej gospodarce*, Raport grupy roboczej do spraw Internetu Rzeczy przy Ministerstwie Cyfryzacji, Warszawa, s. 5.

[15] Beacon – małe urządzenie, działające na wydajnych bateriach, mikroprzekaźnik, którego zadaniem jest emisja stałego, unikalnego sygnału korzystając z technologii Bluetooth. Zob. J Pizon, *Koncepcja wdrożenia technologii „Internetu Rzeczy"…*, op.cit., s. 123; P. Smejda, *Internet Rzeczy (IoT) we współczesnej gospodarce. Rola, zadania i bariery rozwoju*, Zeszyty Naukowe Politechniki Łódzkiej, Organizacja i Zarządzanie, z. 64, Nr 1208/2016, s. 46.

Urządzenie, które będzie w stanie odebrać przesyłany sygnał, przetworzyć go i wywołać określoną reakcję. Może to być smartfon, tablet lub komputer, na którym wyświetli się konkretna informacja, ale również inny przedmiot, który automatycznie wykona określone działanie, np. rozwijające się rolety zintegrowane z systemem home-automation, sygnalizacja świetlna dostosowana do natężenia ruchu czy też książka z biblioteki wyświetlająca przypomnienie o dacie zwrotu.

Środek komunikacji, czyli sposób przesyłania danych. Obecnie na rynku istnieje szereg technologii umożliwiających przekazywanie informacji między dwoma obiektami, począwszy od tych najbardziej popularnych jak WiFi czy Bluetooth, a skończywszy na NFC czy też Z-WAVE (wykorzystywany np. w systemach automatyki budynkowej)”[16].

Rysunek 1. Model działania IoT



Źródło: Opracowanie własne na podstawie zebranej literatury

W praktyce komunikacja człowiek - rzecz działa tak, że użytkownik poprzez aplikację w swoim smartfonie wysyła komunikat do urządzenia z poleceniem wykonania, np. polecenie uruchomienia odkurzacza samo jezdnego. Odkurzacz po otrzymaniu polecenia uruchamia się

[16] P. Kolenda, *Raport...,* op.cit., s. 8

i zaczyna zaprogramowane działanie, a dzięki wbudowanym czujnikom i sensorom omija przeszkody i robi mapę terenu, zapisując ją w pamięci. Użytkownik na smartfonie jest w ciągłym kontakcie z urządzeniem, które przesyła poprzez aplikację informacje o błędach, postępach pracy, zakończeniu jej itp. Natomiast komunikacja pomiędzy rzeczami, maszynami (M2M), polega na wymianie informacji pozyskanych, zbieranych przez czujniki i sensory za pomocą dostępnej dla nich platformy programowej. Przykładem może być inteligentna lodówka, która posiada wprowadzoną listę rzeczy, jakie powinny się znajdować w jej wnętrzu oraz zapisane linki stron internetowych sklepów. W momencie, gdy w lodówce zaczyna brakować produktów, czujniki i kamerki zamontowane w lodówce automatycznie przekazują tą informację do aplikacji obsługującej zamówienia w internetowych sklepach, dokonując zakupu wraz z dostawą do domu. Dzięki takim rozwiązaniom użytkownicy zaoszczędzają czas, zwiększają własne bezpieczeństwo i wygodę.

Internet Rzeczy z racji swojej różnorodności i zastosowania nie powinien być rozpatrywany tylko pod kątem samych użytkowników jako potencjalnych konsumentów. Na podstawie różnych opracowań można zauważyć, że technologia IoT zagościła w każdej dziedzinie gospodarki, ponieważ w rzeczywistości to przede wszystkim „przedsiębiorstwa są głównymi beneficjentami postępującej cybernetyzacji, pozwalającej między innymi na: zwiększenie wydajności, poprawę jakości, skrócenie czasu dostaw, obniżenie kosztów produkcji i usług czy też poprawę wykorzystania informacji w procesie podejmowania decyzji”[17].

Zastosowania IoT

Nie ulega wątpliwości, że rynek technologii IoT cały czas się rozwija, nie zwalniając tempa. Urządzenia podłączone do sieci i wzajemnie komunikujące się, znajdują zastosowanie w coraz to nowszych elementach gospodarki, która przenika nasze codzienne obowiązki. Dzięki temu

[17] A. Tybura, *Internet rzeczy – Biznes – Marketing – Wyzwanie*, [w:] *Współczesne trendy bezpieczeństwa biznesu. Problemy i wyzwania gospodarek* wschodnich, B. Glinkowska (red.), Wydawnictwo Uniwersytetu Łódzkiego, s. 63.

trendowi eksperci szacują wzmożone zapotrzebowanie na zwiększenie prędkości transferu przesyłanych informacji między urządzeniami a centrami obliczeniowymi, co spowoduje wzrost efektywności w wielu sektorach gospodarki. Szacuje się, iż w roku 2030 na świecie będzie w użyciu od 29 do nawet 35 miliardów urządzeń podłączonych do internetu, korzystających z technologii IoT.[18] W raporcie Grupy Robocze ds. Internetu Rzeczy czytamy, że wydatki w poszczególnych branżach na IoT będą wzrastać, a „według danych dotyczących rynku globalnego, liderami wzrostów i wolumenu wydatków w obszarze IoT są: rynek konsumencki, branża logistyczna i transportowa oraz przemysł"[19]. Według raportu McKinsey Global Institute opublikowanym w 2015 minimalna wartość rynku IoT na świecie w 2025 roku osiągnie poziom ok. 4 bln dolarów, a w scenariuszu dynamicznym może dojść nawet do 11 bln. Natomiast w 2021 roku został opublikowany kolejny raport, w którym podane są wartości rynku do 2030 roku na poziomie od 5,5 bln do 12,6 bln dolarów.[20]

Aby w pełni zrozumieć skalę wykorzystania urządzeń podłączonych do Internetu Rzeczy, przedstawionych w powyższych szacunkach, należy zapoznać się z obszarami, w jakich te urządzenia pracują obecnie lub będą pracowały w przyszłości. W tabeli 1 zamieszczone zostały najważniejsze obszary zastosowań Internetu Rzeczy wraz z opisem i przykładami. Często te obszary ściśle są ze sobą związane, a nawet wzajemnie się przenikają czy uzupełniają.

[18] Cyfryzacja KPRM, Serwis Rzeczpospolitej Polskiej gov.pl, *Internet rzeczy*, https://www.gov.pl/web/cyfryzacja/internet-rzeczy (dostęp: 28.02.2023).

[19] L. Maśniak, M. Kawecki, Ministerstwo Cyfryzacji, *IoT w polskiej…*, op.cit., s. 18.

[20] M. Patel, M. Chui, M. Collins, The Internet of Things: Catching up to an accelerating opportunity, McKinsey & Company, 2021, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf (dostęp: 28.02.2023).

Tabela 1. Wybrane sektory zastosowań Internetu Rzeczy

Sektory zastosowań	**Wybrane obszary zastosowań**	**Przykłady urządzeń**
Bezpieczeństwo publiczne	monitorowanie środowiska (terenów zalewowych, oczyszczalni ścieków), informacje meteorologiczne i klimatyczne, śledzenie ludzi, zwierząt, przesyłek czy bagażu, bezpieczeństwo militarne	czujniki monitorujące infrastrukturę krytyczną, czytniki linii papilarnych, systemy rozpoznawania twarzy, inteligentne bramki na lotniskach, drony i urządzenia monitorujące smog w miastach, drony (wojskowe, cywilne), zdalnie sterowane systemy alarmowe, systemy zarządzania kryzysowego (czujniki powodziowe, monitoring miejski)
Budownictwo (domy i miasta)	Inteligentne budynki (domy) z systemami bezpieczeństwa w budynkach, automatyzacja budynków, osiedli, obiektów, inteligentne miasta	systemy sterowania ogrzewaniem, wentylacją, klimatyzacją, kontrolą dostępu, oświetleniem, bezpieczeństwem (w tym przeciwpożarowym), inteligentne przystanki autobusowe, kontrolowanie za pomocą czujników działania sieci wodociągowej
Energetyka	wydobycie surowców, poszukiwania alternatywnych, w tym odnawialnych źródeł energii, urządzenia dostarczające prąd do odbiorców	aplikacje i urządzenia do ekstrakcji surowców i ich transportu, zdalne liczniki energii elektrycznej, wykrywanie surowców naturalnych, roboty
Nauka	wspomaganie doświadczeń naukowych, baza danych naukowych	inteligentne urządzenia analizy laboratoryjnej, e-biblioteki, e-booki.

Opieka zdrowotna i nauki przyrodnicze	Systemy monitorujące pacjentów, telemedycyna, nowe leki, chirurgia, operacje na odległość, badania i rozwój nowych leków i sprzętu medycznego	inteligentne protezy kończyn ,opaski monitorujące funkcje życiowe, biomedyczne chipy, inteligentne łóżka szpitalne, kamery wysokiej rozdzielczości monitorujące noworodki wcześniaki, czujniki analizujące aktywność osób starszych wraz z powiadamianiem służb ratunkowych
Przemysł	monitorowanie i śledzenie aktywów, urządzeń i produktów przemysłowych, analiza lokalizacji dla szerokiej gamy procesów fabrycznych, systemy monitorowania warunków pracy (w tym BHP)	automatyczne linie produkcyjne z analizą i kontrolą jakości, roboty przemysłowe, czujniki analizujące czasy trwania procesów i operacji, czasy postojów maszyn, czujniki monitorujące płynność produkcji i wskazujące „wąskie gardła" procesu, samo jeżdżące wózki widłowe, systemy wysokiego składowania
Rolnictwo	Inteligentne systemy wykorzystywane przy uprawie roślin, w sadownictwie, w ogrodnictwie, szkółkach leśnych	Systemy podlewania pól, monitorowanie wilgotności w szklarniach, systemy monitorujące dane o warunkach atmosferycznych w danym miejscu, czujniki wykorzystywane w maszynach do zbioru upraw
Sektor detaliczny (handel)	systemy sieciowe i urządzenia do zarządzania łańcuchem dostaw, zarządzanie informacją o produktach i konsumentach, zarządzanie zapasami	maszyny sprzedające (żywność, napoje, papierosy), automatyczne stacje tankowania, maszyny do gier, e-zakupy, e-sklepy, urządzenia wyświetlające (billboardy, wyświetlacze, punkty informacyjne), systemy rozrywkowe (automaty do gier, systemy dźwiękowe)

Sektor IT	wyposażenie biur, infrastruktura biurowa, urządzenia transmisji mobilnej, sieci publiczne i prywatne, centra danych	systemy utrzymania energii i samoregulacyjne klimatyzacje, inteligentne drukarki i urządzenia wielofunkcyjne, E-commerce
Sektor konsumpcyjny/domowy	bezpieczeństwo domu – smart dom, sterowanie urządzeniami, energią i oświetleniem w domu, rozrywka	elektroniczne nianie, aktywny monitoring i systemy samo-alarmujące, uchlanie/zasłanianie okien, czujniki poboru prądu, wody, inteligentne termostaty, żarówki, lodówki, piekarniki, głośniki
Transport	zarządzanie flotą pojazdów, systemy informacji dla pasażerów, systemy płatności za korzystanie z infrastruktury transportowej i parkingowej, system kontroli ruchu lotniczego	drony pocztowe, sterowanie ruchem i sygnalizacją uliczną, zielona fal, inteligentne samochody, inteligentny monitoring parkingów i płatności kartami płatniczymi, GPS w środkach transportowych, systemy alarmowe w samochodach, czujniki zużytego paliwa, czujniki informujące o zdarzeniach drogowych
Inne	technologie kosmiczne, sztuczna inteligencja, sieci neuronowe	systemy obróbki dużej ilości danych, systemy Big-Data

Źródło: Opracowanie własne na podstawie zebranej literatury

Ciągły rozwój Internetu Rzeczy stwarza coraz nowsze możliwości zastosowań w wielu dziedzinach życia, gospodarki, a nawet obronności państwa. Urządzenia komunikujące się miedzy sobą, na podstawie gromadzonych informacji, będą same podpowiadały nowe rozwiązania poprawiające jakość naszego życia.

Zagrożenia IoT

Internet Rzeczy obejmuje swoim zasięgiem ogromną liczbę różnego rodzaju sprzętu, który komunikuje się ze sobą, wykorzystując do tego

celu własne interfejsy komunikacyjne oparte o protokoły dedykowane każdej z warstw modelu działania (komunikacji) IoT. „Brak standaryzacji w zakresie Internetu Rzeczy skutkuje brakiem na chwilę obecną pewnych jednolitych rozwiązań. Nie ma jednego jednolitego uniwersalnego standardu technologicznego, który były używany do komunikacji między urządzeniami w ramach M2M. w praktyce używa się wielu standardów[21]. Tym samym IoT narażony jest niestety na liczne zagrożenia, mające wpływ na poziom bezpieczeństwa.

W raporcie firmy HP[22] z 2014 roku wynika, iż 70% urządzeń Internetu Rzeczy było narażanych na zagrożenia bezpieczeństwa, które umożliwiały hakerom dostęp do danych osobowych użytkowników, danych o ich stanie zdrowia czy informacji o karcie kredytowej. Po przetestowaniu 10 najbardziej popularnych urządzeń, firma HP odkryła średnio 25 luk bezpieczeństwa w każdym urządzeniu. Do najczęstszych problemów wskazanych przez firmę HP można zaliczyć:

- „Problemy z prywatnością
- Słabe punkty w systemie autoryzacji i uwierzytelnienia
- Brak szyfrowania transmisji danych
- Niebezpieczne interfejsy WWW
- Niewystarczający poziom bezpieczeństwa oprogramowania” [23].

Open Web Application Security Project (czyli globalna fundacja non-profit działająca w obszarze poprawy cyfrowego bezpieczeństwa) również w 2014 roku opublikowała własny zestaw 10 zagrożeń i podatności na nie. Opracowali je na podstawie badań własnych przeprowadzonych na 10 urządzeniach Internetu Rzeczy. Wyniki są podobne do przedstawionych powyżej, mianowicie:

- Niebezpieczny interfejs sieciowy
- Zbyt mała autoryzacja
- Niezabezpieczone usługi sieciowe
- Brak szyfrowania warstwy transportowej

[21] B. Krupanek, *Przegląd protokołów przeznaczonych do transmisji danych w systemach Internetu Rzeczy*, Przegląd Elektotechniczny, R. 94, Nr 11/2018, s. 47.

[22] C. Hopping, HP: 70% of Internet of Things devices vulnerable to attack, ITPro., 2014, https://www.itpro.co.uk/security/22804/hp-70-of-internet-of-things-devices-vulnerable-to-attack (dostęp: 28.02.2022).

[23] A Rot, *Bezpieczeństwo…*, op.cit. 291.

- Problemy z prywatnością
- Niezabezpieczona transmisja danych z chmurami obliczeniowymi
- Niezabezpieczone interfejsy bezprzewodowe
- Niewystarczające opcje konfiguracji zabezpieczeń
- Niebezpieczne oprogramowanie firmware
- Niewystarczające zabezpieczenia fizyczne[24].

Użytkownicy również dostrzegają zagrożenia i niedogodności płynące z wykorzystania IoT. Jak wynika z badania przeprowadzonego przez autorów raportu o Internecie Rzeczy w Polsce, aż 43% badanych obawia się utraty poczucia prywatności, natomiast 47% respondentów boi się o wyciek danych o nich lub o ich bliskich. Poczucie zagrożenia deklarowało 16% badanych, a obawę o bezpieczeństwo bliskich podało 18%. „Te lęki i obawy z pewnością muszą zostać uwzględnione przez firmy i instytucje proponujące rozwiązania IoT"[25].

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)[26] również szczegółowo opisuje w swoim raporcie kluczowe grupy aktywów i zasobów, które powinny być chronione w ekosystemie IoT przed zagrożeniami wynikającymi z korzystania z urządzeń IoT podłączonych do sieci internetowej. Zagrożenia te zostały dodatkowo podzielone na trzy poziomy mające wpływ na potencjalne skutki, jakie mogą wywołać:

- poziom krytyczny: Malware, Exploit Kits, DDoS, Słabe hasła, Wyciek delikatnych danych/modyfikacja informacji;

[24] Ibidem, s. 292.

[25] P. Kolenda, *Raport…,* op.cit., s. 26-27.

[26] Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) to centrum wiedzy eksperckiej w zakresie bezpieczeństwa sieci i informacji dla UE, jej państw członkowskich, sektora prywatnego i obywateli Europy. ENISA współpracuje z tymi grupami w celu opracowania porad i zaleceń dotyczących dobrych praktyk w zakresie bezpieczeństwa informacji. Pomaga państwom członkowskim UE we wdrażaniu odpowiedniego prawodawstwa UE i pracuje nad poprawą odporności krytycznej infrastruktury informatycznej i sieci w Europie. ENISA dąży do poszerzenia istniejącej wiedzy specjalistycznej w państwach członkowskich UE poprzez wspieranie rozwoju społeczności transgranicznych zaangażowanych w poprawę bezpieczeństwa sieci i informacji w całej UE. Więcej informacji o ENISA i jej pracy można znaleźć na stronie www.enisa.europa.eu.

- poziom wysoki: Atak na prywatność, Podsłuchiwanie;
- poziom średni: Awaria sieci, Zaawansowane techniki ataku, Podrobienie przez zainfekowane urządzenia.[27]

Większość z podanych powyżej zagrożeń może być wyeliminowana już na etapie projektowania konkretnych rozwiązań dedykowanych w IoT. Niestety wdrożenie niektórych istniejących rozwiązań wiązało by się ze znacznym podwyższeniem kosztów produkcji, a co za tym idzie podniesieniem ceny końcowej, co mogłoby przełożyć się na kiepskie wyniki sprzedaży i fiasko całego przedsięwzięcia. Użytkownik, klient decydując się na zakup urządzenia IoT, musi mieć świadomość istniejących zagrożeń wynikających z korzystania z urządzenia, na które się poniekąd godzi.

Bezpieczeństwo w IoT

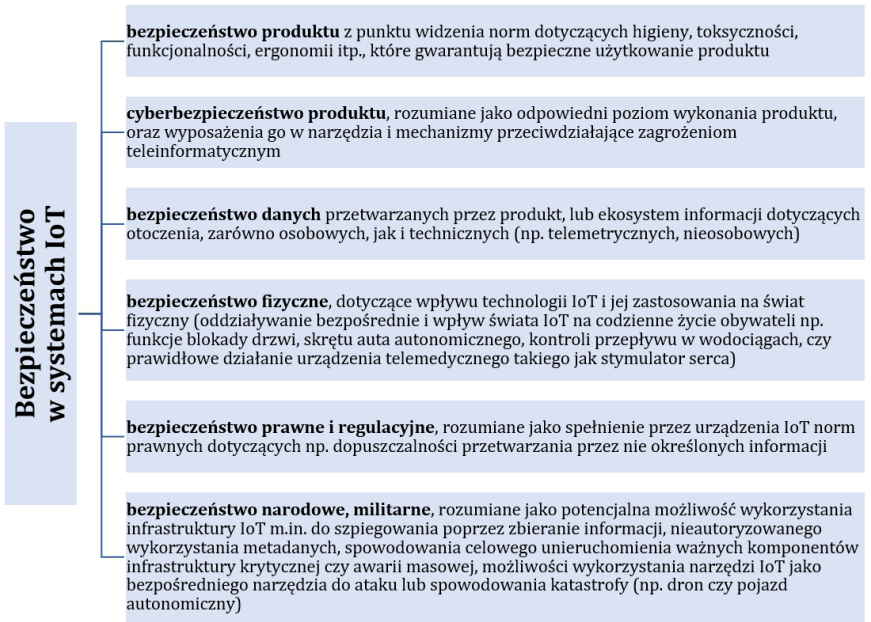
Bezpieczeństwo w IoT to obecne najważniejsze wyzwanie dla firm produkujących, wdrażających i wprowadzających na rynek urządzenia wchodzące w skład Internetu Rzeczy. Większość z dużych przedsiębiorstw potwierdza, że obecne zabezpieczenia w stosowanych rozwiązaniach są niewystarczające. „Coraz częściej zdarzają się cyberataki na systemy bezpieczeństwa zarówno małych jak i dużych firm, instytucji państwowych i samorządowych oraz organizacji pozarządowych. Także w przypadku urządzeń końcowych – smartfonów, drukarek, komputerów czy tabletów – zarówno tych w obszarze prywatnym, jak i państwowym, jest to obszar, który wymaga dużych inwestycji”[28]. Dlatego bezpieczeństwo ma ogromne znaczenie zarówno dla poszczególnych jednostek, jak i całych społeczności, w tym również dla obronności państwa. Zgodnie z informacjami zawartymi w raporcie Grupy Roboczej ds. Internetu Rzeczy: „IoT nie może istnieć bez cyberbezpieczeństwa. […] Bezpieczeństwo należy postrzegać jako podstawową funkcję świata IoT. Bez spełnienia wymogów bezpieczeństwa, stosowania

[27] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA, 2017, s. 17, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (dostęp:28.02.2023).

[28] M. Kanwnik, *Smart home, smart cities, smart world…*, op.cit., s.12.

standardów i dobrych praktyk, świat IoT stanowi samodzielnie większe zagrożenie, niż w przypadku rezygnacji z tego typu technologii. Bezpieczeństwo to zatem warunek niezbędny dla rozwoju IoT. Natomiast bez adekwatnej certyfikacji produktów IoT, nie można zapewnić odpowiedniego poziomu bezpieczeństwa”[29]. Na rysunku 2 przedstawione zostały podkategorie bezpieczeństwa IoT, które powinny spełniać firmy produkujące urządzenia IoT, ponieważ „bezpieczeństwo jest krytycznym elementem jakości produktu”[30].

Rysunek 2. Podkategorie bezpieczeństwa systemów IoT



Źródło: Opracowanie własne na podstawie *Raport Internet Rzeczy – Polska Przyszłości*.

Bezpieczeństwo jest najważniejszą kwestią, która będzie miła wpływ na dalszy rozwój całej technologii IoT. Niestety jak wynika z przytoczonych powyżej raportów, również zagrożenia ewaluują

[29] L. Maśniak, M. Kawecki, Ministerstwo Cyfryzacji, *IoT w polskiej …*, op.cit., s. 21.

[30] Ibidem.

wraz z wprowadzaniem na rynek najnowszych rozwiązań IoT. Dane przedstawione przez Huawei nie pozostawiają wątpliwości, iż zadbanie o bezpieczeństwo danych użytkowników powinno być priorytetem każdego projektanta urządzeń przeznaczonych do IoT. W raporcie *Building a Trused and Managed IoT World*[31] wskazano problem dotyczące bezpieczeństwa:

- 27% systemów kontroli pada ofiarą infekcji lub ataku,
- 80% istniejących urządzeń korzysta z prostego (często niezmienionego) hasła,
- 70% zachodzącej komunikacji nadal jest nieszyfrowane,
- 90% aktualizacji oprogramowania nie weryfikuje sygnatur i podpisów, a co gorsza wiele z istniejących urządzeń w żaden sposób nie obsługuje aktualizacji.

Wiele z powyższych problemów można rozwiązać stosując znane od wielu lat normy ISO/IEC 27000 odnoszące się do międzynarodowych standardów technik bezpieczeństwa, ochrony danych i systemów komputerowych, o których firmy produkcyjne dość często zapominają. Można również skorzystać z wytycznych różnych organizacji, które pomagają w zabezpieczaniu danych w sieciach firmowych czy aktualizowaniu oprogramowania. Jedną z takich firm jest CSA (Cloud Security Alliance), która udostępniła zalecenia, jak powinno się implementować bezpieczną (F)OTĘ (File Over The Air – metoda aktualizacji za pomocą sieci):

- Kopia zapasowa (backup) aktualnie istniejącej konfiguracji urządzenia IoT za nim się rozpocznie i wymusi aktualizację.
- Powrót do poprzednio działającego systemu (rollback) powinien być obsługiwany, ale wyłącznie z uwzględnieniem autoryzacji producenta.
- Projekt systemu powinien umożliwiać administratorom systemu planowanie aktualizacji z wyprzedzeniem, aby w ten sposób uniknąć przeciążenia łącza lub saturacji sieci.
- Dystrybutor powinien wspierać możliwość konfiguracji serwera przez administratorów zarządzających smart topologią.
- Pojedynczy komponent powinien być odpowiedzialny za za-

[31] Za: M. Sikorski, *Internet Rzeczy…*, op.cit., s. 69.

rządzanie wszystkimi mikrokontrolerami znajdującymi się wewnątrz urządzenia.
- Aktualizacja powinna być dostarczona w pakietach przygotowywanych z myślą o słabej przepustowości sieci.
- Aktualizacje i integracja zmian powinny być uwierzytelniane i chronione po stronie wysyłającego aktualizację i odbierającego (e2e – end 2 end).
- Klucze użyte do podpisów MUSZĄ być bardzo dobrze zabezpieczone przed hakerami.
- Zapewnienie procedury odzyskiwania i przywracania ustawień na wypadek nieudanej aktualizacji.
- Zapewnienie długoletniego kontraktu dotyczącego wsparcia urządzenia przez wszystkie strony.[32]

Bezpieczeństwo w większości przypadków leży po stronie producentów. To oni odpowiadają za proces projektowania, produkcji, testów, a następnie wdrożenia i na końcu sprzedaży. Każde urządzenie IoT oparte jest na oprogramowaniu, które powinno być aktualizowane. Ale czy zwykły użytkownik ma taką możliwość? Nie zawsze, ponieważ w wielu urządzeniach jest to po prostu nie możliwe. Użytkownik nie ma dostępu nawet do interfejsu urządzenia. Aktualizacja wykonuje się sama poprzez sieć po uprzednim udostępnieniu jej przez producenta, tak że użytkownik nawet tego nie zauważy. Niestety każde urządzenia IoT jest inne i posiada odmienne ustawienia do których dostęp mają tylko producenci.

Jak wynika z wielu badań, „obszar bezpieczeństwa stanowi kluczową przeszkodę w implementacji koncepcji internetu rzeczy w organizacjach […] oraz również wykazały, że głównym ograniczeniem rozwoju tej innowacyjnej technologii są obawy dotyczące bezpieczeństwa"[33]. Ma to zasadniczy związek ze stale zwiększającą się liczbą podłączonych

[32] Za: M. Sikorski, Internet Rzeczy…, op.cit., s. 70-72; B. Ruseell, *Recommendations for IoT Firmware Update Processes*, Cloud Security Alliance, 2018, https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/recommendations-for-iot-firmware-update-processes.pdf (dostęp: 28.02.2023).

[33] K. Liwarska-Fulczyk, *Internet rzeczy – implikacje organizacyjne*, e-mentor, 3(85), s. 25.

urządzeń do sieci, które stanowią potencjalne cele przyszłych cyberataków i wykradania danych przesyłanych między urządzeniami IoT.

Znajomość IoT wśród użytkowników – przyczynek do badań

Internet Rzeczy zadomowił się w polskich domach, miastach, przemyśle, gospodarce. Korzystamy z niego na co dzień w mniejszym lub większym stopniu. Ale czy wiemy na czym to polega? Jak to działa? Jaki ma to wpływ na nasze codzienne życie? I co najważniejsze, jak to wpływa na nasze bezpieczeństwo?

Jak wynika z badania polskich internautów w wieku powyżej 14 lat, przeprowadzonego w 2015 roku w ramach raportu Internet Rzeczy w Polsce tylko 11% badanych spotkało się wcześniej z pojęciem Internet Rzeczy, ale połowa z nich posiada w domu inteligentne urządzenia AGD. Mężczyźni statystycznie częściej deklarowali znajomość tego pojęcia niż kobiety. Co istotne, osoby częściej korzystające z internetu na urządzeniach mobilnych, również, zdecydowanie częściej deklarowały, że spotkały się z pojęciem IoT[34].

W badaniu przeprowadzanym w 2020 roku przez O. Pawłowską wśród osób powyżej 30 roku życia, widać znaczącą zmianę w porównaniu z powyższymi wynikami dotyczącymi znajomości pojęcia Internet Rzeczy. Tu aż 71% potwierdziło znajomość tego pojęcia. Natomiast z badania wynika, iż „technologia Internetu Rzeczy nie jest jeszcze bardzo popularna wśród przeciętnych użytkowników, ale wydaje się, że ze względu na wygodę używania, rozwiązania wykorzystujące tę technologię przyjmą się"[35].

Natomiast badania E. Musiał w 2021 roku wśród studentów wykazały, że inteligentne „rzeczy" w większości przypadków są im znane i korzystają z nich na co dzień, szczególnie z urządzeń „smart home". Jednak warto zauważyć, iż studenci „krytycznie odnieśli się do techno-

[34] P. Kolenda, *Raport…,* op.cit., s. 29.

[35] O. Pawłowska, *Internet Rzeczy – zjawisko rewolucjonizujące życie. Znajomość tej technologii i jej zagrożeń wśród osób 30+*, Edukacja Ustawiczna Dorosłych, 2/2020, s. 160.

logii IoT i zdecydowanie nie zamierzają w najbliższej przyszłości testować lub skorzystać z dostępnych na rynku inteligentnych urządzeń”[36]. Wynika to z faktu, że obawy przed zagrożeniami były większe niż podawane zalety wykorzystania IoT.

Analizując powyższe badania nasuwa się wiele pytań dotyczących wiedzy użytkowników o technologii IoT, o jej potencjalnych zagrożeniach oraz bezpieczeństwie urządzeń i naszych danych przetwarzanych przez te urządzenia. Warto podjąć się przeprowadzenia głębszej analizy tematu, by móc porównać, jak zmienia się świadomość użytkowników w miarę rozwoju i dostępności IoT.

Zakończenie

Internet Rzeczy analizowany jest w wielu opracowaniach naukowych, badaniach, raportach, zarówno od strony technicznej, jak i społecznej. Szerokie zastosowanie tej technologii w wielu gałęziach gospodarki i w życiu codziennym uwypukla jego zalety. Inteligentne rozwiązania zaobserwować możemy w miastach, w budynkach, na ulicach i skrzyżowaniach, w domach – dosłownie wszędzie tam, gdzie można zastosować urządzenia IoT podłączone do sieci. Można rzec, że obecny cyfrowy świat, ale również nasza codzienna rzeczywistość jest wypełniona przez IoT. Dzięki zastosowaniu tej technologii można zauważyć zmiany, które wpływają na życie mieszkańców naszego globu. Technologia IoT rewolucjonizuje przemysł 4.0, poprawia bezpieczeństwo jednostek i całych społeczności, wyznacza kolejne kierunki rozwoju w różnych dziedzinach gospodarki. IoT w połączeniu ze sztuczną inteligencją i uczeniem maszynowym nadaje nowe możliwości, z którymi przyjdzie się nam zmierzyć w przyszłości.

Jednak IoT to nie tylko zalety i wygoda, to także zagrożenia wynikające w wykorzystywania tej technologii. W wielu opracowaniach można znaleźć informację, iż urządzenia IoT nie są w odpowiedni sposób zabezpieczone, co przyznają również sami producenci. Mała moc obliczeniowa tych urządzeń w połączeniu z różnorodnością oprogramowania i wykorzystywanych protokołów stają się źródłem potencjalnych za-

[36] E. Musiał, *Bezpieczeństwo człowieka*…, op.cit., s. 89.

grożeń. Ta mnogość rozwiązań technicznych IoT i komunikacji między nimi spowodowała, że słabo zabezpieczone urządzenia narażone są na wyciek danych. Przesyłanie ogromnych ilości informacji między urządzeniami w sieciach staje się narażone na potencjalne ataki hakerów. Jak wynika z niniejszego opracowania wraz z rozwojem IoT, powstają również nowe zagrożenia. Obecnie firmy wprowadzające na rynek kolejne urządzenia dokładają starań by bezpieczeństwo ich produktów było na wysokim poziomie. Stało się ono priorytetem dla producentów technologii IoT, co można zaobserwować w raportach wskazujących na zwiększanie funduszy przeznaczanych na bezpieczeństwo. Również sam proces produkcji uwzględnia elementy dbające o bezpieczeństwo już na etapie projektowania.

Jak przedstawiono w opracowaniu, użytkownicy chętnie sięgają po najnowsze rozwiązania, dzięki którym oszczędzają czas, zwiększają poczucie komfortu, mogą monitorować swoje zdrowie, dbać o środowisko, korzystając z systemów inteligentnego oświetlenia czy ogrzewania. Świadomość użytkowników zmienia się wraz z rozwojem IoT. Wyniki badań pokazują, że społeczeństwo korzysta z różnych urządzeń Internetu rzeczy, choć nie do końca znając jego pojęcie. Nawet świadome korzystanie z urządzeń IoT nie uchroni nas w pełni przed zagrożeniami, ponieważ nie zawsze możemy dokonywać choćby aktualizacji oprogramowania, nie mamy dostępu do interfejsu. Jesteśmy zanurzeni w cyfrowym świecie, gdzie nasz smartfon stał się przedłużeniem ręki, dzięki czemu możemy obsługiwać różne urządzenia na odległość. Wszystko to realizowane jest poprzez najnowsze technologie, sieci rozproszone, sieci bezprzewodowe. IoT jest obecnie technologią, która daje nam nowe możliwości. Niestety użytkownicy chcący wykorzystywać te nowinki technologiczne muszą się zgadzać na przekazywanie swoich danych prywatnych, np. poprzez dostęp do geolokalizacji, poprzez akceptację dostępu aplikacji obsługujących urządzenia IoT do danych zawartych w smartfonie. Każdy staje przed dylematem: czy ważniejsza jest dla mnie wygoda, chęć zaoszczędzenia czasu, przy jednoczesnym „świadomym" oddawaniu swojej prywatności czy rezygnacja z dobrodziejstw oferowanych przez IoT. Z badań wynika, że użytkownicy pomimo wielu zagrożeń oraz wysokich kosztów, korzystają i zamierzają w przyszłości korzystać z urządzeń IoT.

„Podłączenie całego naszego świata do internetu może potencjalnie przynieść ogromne korzyści, ale dopóki wszystkie podmioty nie wezmą na siebie zadań związanych z zapewnieniem bezpieczeństwa, dopóki IoT będzie raczej problemem, a nie rozwiązaniem”[37].

Działania państw powinny zmierzać do poprawy bezpieczeństwa nie tylko poprzez zwiększanie nakładów finansowych, ale również poprzez dostosowanie regulacji prawnych w stosunku do nowych technologii. Regulacje te powinny dawać możliwość wykorzystania technologii IoT nie tylko indywidualnym użytkownikom, ale również instytucjom publicznym, firmom, przy zachowaniu ochrony danych przesyłanych w sieci. By zwiększyć świadomość społeczną korzyści i zagrożeń płynących z użytkowania IoT powinno być organizowanych więcej kampanii społecznych i edukacyjnych przedstawiających technologię IoT, zarówno jej zalety, ale i wady. Edukacja użytkowników IoT jest jednym z elementów na poprawę bezpieczeństwa ich samych, ale także na bezpieczeństwo całych społeczności. Warto przedstawiać koncepcję IoT wszystkim pokoleniem, a w szczególności młodym ludziom, by wykształcić w nich postawę społecznego obowiązku dbania o dobro wspólne, dbania o przekazywane informacje.

Bibliografia

Abramczyk A., *Raport: Internet Rzeczy w przemyśle*, Controling Engineering Polska, 19.02.2020, https://controlengineering.pl/raport-internet-rzeczy-w-przemysle/ (dostęp: 26.02.2023).

Ashton K., *That “Internet of Things” Thing*, RFiD Journal, nr 22(7) 2009, ss.97-114, https://www.rfidjournal.com/that-internet-of-things-thing (dostęp: 26.02.2023).

Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, ENISA, 2017, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (dostęp: 28.02.2023).

[37] Bezpieczeństwo internetu rzeczy, COMPUTERWORLD, Materiał promocyjny, https://www.computerworld.pl/news/Bezpieczenstwo-internetu-rzeczy,408302.html (dostęp: 28.02.2023).

Bezpieczeństwo internetu rzeczy, COMPUTERWORLD, Materiał promocyjny, https://www.computerworld.pl/news/Bezpieczenstwo-internetu-rzeczy,408302.html (dostęp: 28.02.2023).

Cyfryzacja KPRM, Serwis Rzeczpospolitej Polskiej gov.pl, *Internet rzeczy*, https://www.gov.pl/web/cyfryzacja/internet-rzeczy (dostęp: 28.02.2023).

Dragun Ł., Dąbrowska G., Olszyńska P., *Identyfikacja barier wdrażania rozwiązań z zakresu Internetu Rzeczy w wybranych segmentach gospodarki*, Akademia Zarządzania 5(1)/2021, ss. 178.7–189.

Hopping C., *HP: 70% of Internet of Things devices vulnerable to attack*, ITPro., 2014, https://www.itpro.co.uk/security/22804/hp-70-of-internet-of-things-devices-vulnerable-to-attack (dostęp: 28.02.2022).

Kanwnik M., *Smart home, smart cities, smart world. Rozwój Internetu Rzeczy (IoT)*, Raport Cyfrowej Polski, https://cyfrowapolska.org/wp-content/uploads/2020/11/Raport_Rynek-IOT_2020_net.pdf?fbclid=IwAR161N--T6_kg0PpW03yn9lnqdwCgd9AAWW3vjDdBsWejKUk8UOlc0g5ytsw (dostęp: 25.02.2023), Warszawa, 2020.

Kolenda P., *Raport – Internet Rzeczy w Polsce*, iab Polska, 2016

Krupanek B., Bogacz R., *Węzły końcowe systemów Internetu* Rzeczy, Zeszyty Naukowe Wydziału Elektroniki i Automatyki Politechniki Gdańskiej Nr 59/2018, ss. 111-116.

Krupanek B., *Przegląd protokołów przeznaczonych do transmisji danych w systemach Internetu Rzeczy*, Przegląd Elektotechniczny, R. 94, Nr 11/2018, ss. 47–50.

Liwarska-Fulczyk K., (2020), *Internet rzeczy – implikacje organizacyjne*, e-mentor, 3(85), ss. 23–31.

Maśniak L., Kawecki M., Ministerstwo Cyfryzacji, *IoT w polskiej gospodarce*, Raport grupy roboczej do spraw Internetu Rzeczy przy Ministerstwie Cyfryzacji, Warszawa, 2019, ss. 5-101, https://www.gov.pl/web/cyfryzacja/polska-przyszlosci-to-polska-z-internetem-rzeczy (dostęp: 25.02.2023).

Musiał E., *Bezpieczeństwo człowieka w świecie smart. Analiza wyników badań wśród studentów*, Studia Administracji i Bezpieczeństwa nr 12/2022, ss. 83–97.

Ogórek M., Zaskórski P., *Internet Rzeczy w integracji procesów zarządzania kryzysowego*, Organizacja i Zarządzanie Nr 76, 2018, Zeszyty Naukowe Politechniki Poznańskiej, ss.199–215.

Owczarek G., Hłobaż A., *Bezpieczeństwo teleinformatyczne w systemach przemysłowego Internetu rzeczy na przykładzie środowiska pracy*, Bezpieczeństwo pracy 2/2019, ss. 8–12.

Patel M., Chui M., Collins M., *The Internet of Things: Catching up to an accelerating opportunity*, McKinsey & Company, 2021, https://www.mck-

insey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf (dostęp: 28.02.2023).

Pawłowska O., *Internet Rzeczy – zjawisko rewolucjonizujące życie. Znajomość tej technologii i jej zagrożeń wśród osób 30+*, Edukacja Ustawiczna Dorosłych, 2/2020, ss. 147–161.

Pizon J., *Koncepcja wdrożenia technologii „Internetu Rzeczy" w systemie logistycznym przedsiębiorstwa*, Systemy Logistyczne Wojsk nr 4/2015, ss. 120-135.

Rot A., *Bezpieczeństwo jako najważniejsze wyzwanie koncepcji Internetu rzeczy*, Przedsiębiorczość i Zarządzanie 2017, Tom XVIII, Zeszyt 4, Część II, ss. 285–296.

Ruseell B., *Recommendations for IoT Firmware Update Processes*, Cloud Security Alliance, 2018, https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/recommendations-for-iot-firmware-update-processes.pdf (dostęp: 28.02.2023).

Rykowski J., *Internet Rzeczy – czy mamy zacząć się bać?*, Napędy i Sterowanie Nr 3 Marzec 2017 r., ss. 120–129.

Sikorski M., *Internet Rzeczy*, Real IT World nr 1/2020, Roman A. (red.), PWN.

Smejda P., *Internet Rzeczy (IoT) we współczesnej gospodarce. Rola, zadania i bariery rozwoju*, Zeszyty Naukowe Politechniki Łódzkiej, Organizacja i Zarządzanie, z. 64, Nr 1208/2016, ss. 43–55.

Tybura A., *Internet rzeczy – Biznes – Marketing – Wyzwanie*, [w:] *Współczesne trendy bezpieczeństwa biznesu. Problemy i wyzwania gospodarek* wschodnich, Glinkowska-Krauze B. (red.), Wydawnictwo Uniwersytetu Łódzkiego, ss. 61–69.

Weiser M., *The Computer for the 21st Century*, Scientific American Specjal Issue on Communications, Computers, and Networks, 265(3), 1991, ss. 94–104.