MATEUSZ DECYK*

INTERNET RZECZY-WISTYCH ZAGROŻEŃ

Abstrakt

Internet Rzeczy to technologia zwiększającą komfort użytkownika, niezależnie od sfery życia, w której się pojawia. Zjawiskiem powszechnym jest podłączanie urządzeń codziennego użytku do sieci, co sprawia że bezpieczeństwo w cyberprzestrzeni zaczyna mieć rosnący wpływ na szeroko pojęte bezpieczeństwo w świecie realnym. Urządzenia te nie są odpowiednio zabezpieczone, a przeciętny użytkownik sam nie jest w stanie zadbać o swoje bezpieczeństwo. To stwarza szeroką gamę możliwości dla przestępców, ale też wiele nowych zagrożeń nie tylko dla jednostki, ale również innych podmiotów.

Słowa kluczowe: Internet Rzeczy, cyberprzestrzeń, ochrona informacji, bezpieczeństwo, cyberbezpieczeństwo, hacking.

Wprowadzenie

Dynamiczny rozwój nowych technologii pozwala na zwiększenie dotychczasowego potencjału państw, społeczeństw, a także jednostek. Aparat państwowy staje się bardziej skuteczny i szybszy w wykonywaniu swoich obowiązków względem obywateli, społeczeństwa są lepiej zintegrowane i skomunikowane. Obywatele zyskują szeroką gamę nowych możliwości, a ich życie staje się wygodniejsze. Postępująca cyfryzacja zmusza świat nauki do nieustannego rozszerzania definicji bezpieczeństwa, wprowadzając do życia człowieka nie tylko szereg udogodnień, ale także nowe, nieznane dotąd zagrożenia. Znaczącym wpływem na bezpieczeństwo jednostki odznacza się środowisko „Internetu Rzeczy", technologii niezwykle trudnej do wąskiego zdefiniowania, wnikającej w niemal każdy aspekt życia człowieka. Często użytkownik nie jest nawet świadom korzystania z konkretnych udogodnień. „Internet Rzeczy" wspiera procesy związane z komunikacją międzyludzką, przemysłem, handlem, opieką zdrowotną, czy transportem, a koszty jego wykorzystania wykraczają daleko poza konieczność zakupu urządzeń, czy oprogramowania. Wprowadza-

* Mateusz Decyk – student stosunków międzynarodowych ze specjalizacją bezpieczeństwo i studia strategiczne na Wydziale Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego. Kontakt e-mail: decykopen@gmail.com

jąc do cyberprzestrzeni ogromne ilości informacji oraz przenosząc odpowiedzialność za czynności i procesy na maszyny, użytkownik żyje wygodniej, jednocześnie narażając się na nowe zagrożenia. Do stworzenia skutecznych zabezpieczeń potrzebny jest czas, a także praktyka. Jak w każdym przypadku, budowanie infrastruktury bezpieczeństwa polega na pościgu za światem przestępczym i jego metodami działania, a Internet oraz technologie pokrewne zaopatrują przestępców w nowe możliwości działania, obnażając podatności i wrażliwość społeczeństwa informacyjnego[1]. To pokrewne technologie informacyjne posiadają największy potencjał kryminogenny oraz nieprzewidywalne kierunki rozwoju wskutek kolaboracji z technologią sztucznej inteligencji. Coraz więcej przedmiotów podłączonych jest do sieci, przetwarzając dane o nieświadomych tego użytkownikach. W nadchodzących latach liczba urządzeń codziennego użytku przetwarzających dane i łączących się z Internetem będzie wzrastać, w ramach obniżających się kosztów samej technologii[2]. Cyberbezpieczeństwo nie figuruje na szczycie listy priorytetów producentów sprzętu, jednak nawet zwiększenie wydatków na ten cel nie gwarantuje skuteczności podjętych działań. Temat „Internetu Rzeczy" staje się coraz bardziej popularny wśród ekspertów, a reforma prawa ochrony danych osobowych[3] oraz kroki podejmowane przez Komisję Europejską wskazują kierunek nadchodzącej rewolucji w zakresie cyberbezpieczeństwa.

Czym jest „Internet Rzeczy"?

Termin „Internet of Things" przypisuje się osobie Kevina Ashtona, brytyjskiego badacza MIT[4], który w 1999 roku stwierdził: „gdyby wszystkie przedmioty w codziennym życiu były wyposażone w identyfikatory i łączność bezprzewodową, mogłyby porozumiewać się ze sobą i być zarządzane za pomocą komputera[5]". W latach dziewięćdziesiątych wizja była niemożliwa to zrealizowania, jednak rozwój łączności bezprzewodowej sprawił, że słowa naukowca stały się fundamentem prób definiowania tego zjawiska. To zadanie wypełnił m.in. Międzynarodowy Związek Telekomunikacji[6], który określa „Internet Rzeczy" jako „globalną infrastrukturę dla społeczeństwa informacyjnego, umożliwiającą działanie zaawansowanym usługom poprzez łączenie fizycznych i wirtualnych rzeczy w oparciu

1 *European Police Chiefs Convention: The future of organised crime chellenges and recommended*, uropol, źródło:https://www.europol.europa.eu/publications-documents/european-police-chiefs-convention-future-of-organised-crime-challenges-and-recommended [dostęp: 02.2017 r.], s. 2.

2 *Twitter, Snapchat, Internet Rzeczy. Dane konsumenta na wyciągnięcie ręki*, źródło: http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1017004,twitter-snapchat-iot-czyli-dane-konsumenta-na-wyciagniecie-reki-20-00.html [dostęp: 02.2017 r.].

3 The General Data Protection Regulation została zatwierdzona 24 maja 2016 roku i wejdzie w życie 25 maja 2018 roku, źródło: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679 &from=en [dostęp: 09.2017 r.].

4 Massachusetts Institute of Technology, amerykańska prywatna politechnika założona w 1861 roku.

5 M. Goodman, *Zbrodnie przyszłości: jak cyberprzestępcy, korporacje i państwa mogą użyć technologii przeciwko Tobie*, Gliwice 2016, s. 250.

6 International Telecommunication Union – najstarsza na świecie organizacja międzynarodowa powstała pierwotnie jako Międzynarodowy Związek Telegraficzny 17 maja 1865 roku w Paryżu.

o istniejące i rozwijane zdolne do współpracy technologie informacyjne i komunikacyjnej[7]". Rzecz rozumiana jest jako „obiekt fizycznego lub wirtualnego świata, który jest zdolny do bycia zidentyfikowanym i zintegrowanym w sieci komunikacyjnej[8]". Popularnym stało się określenie „ekosystemu", który umożliwia pełną synchronizację działań podejmowanych przez urządzenia, bez udziału człowieka[9]. Technologia ta zakłada wyposażanie wszystkich urządzeń codziennego użytku w zaawansowaną elektronikę w celu zwiększenia ich funkcjonalności[10]. Infrastruktura „Internetu Rzeczy" dzieli się na czujniki i mikrokontrolery. Ich rozmiar oraz zapotrzebowanie na energię ulegają zmniejszeniu. Tym samym w danym systemie będzie można zastosować więcej takich urządzeń, potęgując tym samym pobór danych i potencjał „ekosystemu". Wydajniejsze sieci bezprzewodowe pozwolą „rzeczom" na lepszą komunikację nie tylko w sieci Internet, ale także między sobą. Do telefonów, czy tabletów podłączonych do Internetu dołączać będą mieszkania, pojazdy, elementy infrastruktury miejskiej oraz urządzenia medyczne[11].

Nie samo zwiększanie funkcjonalności przedmiotów, a proces przetwarzania przez nie danych tworzy potencjalne zagrożenia dla człowieka. Często to użytkownik wprowadza do sieci dane na swój temat, ale w ramach rosnącego zaawansowania technologii, to urządzenia zbierają dane o nim, niezależnie od jego woli. W ten sposób „Internet Rzeczy" łączy się bezpośrednio z koncepcją „Big Data", reprezentującą innowacyjne sposoby analizy, wizualizacji oraz pozyskiwania ogromnej ilości informacji w czasie rzeczywistym[12]. Dane zbierane przez urządzenia wysyłane są na ogół do tzw. „chmury obliczeniowej"[13]. „Ekosystem" obejmujący fizyczne przedmioty zbierające dane oraz mechanizm gromadzący je w jednym miejscu, do wypełnienia koncepcji Ashtona, wymaga dodatkowo procesu odpowiedniej analizy danych i podejmowania autonomicznych działań niezależnych od woli człowieka. Do tego służy technologia sztucznej inteligencji. W kontekście „Internetu Rzeczy" należy odejść od klasycznego rozumowania tego pojęcia, w którym propagowano wizję stworzenia robota, o inteligencji przewyższającej ludzką[14]. Właściwsze jest

---

7 W. Rorot, *Rzeczy Internetu Rzeczy*, źródło: http://2016.dariah.pl/wpcontent/uploads/sites/3/2016/04/Wiktor.Rorot_.pdf [dostęp: 02.2017 r.].

8 *ITU-T Y.4000/Y.2060 (06/2012) – Overview of the Internet of things*, ITU, 15.06.2015, źródło:http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 [dostęp: 02.2017], s. 1 (tłum. własne).

9 P. Kolenda (red.), Raport – *Internet Rzeczy w Polsce*, IAB Polska, źródło: http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf [dostęp: 02.2017 r.].

10 K. Świrski, *Internet Rzeczy(Internet of Things), czyli trend, który zmieni nasz sposób kupowania i używania*, źródło: http://konradswirski.blog.tt.com.pl/internet-rzeczy-internet-of-things-czyli-trend-ktory-zmieni-nasz-sposob-kupowania-i-uzywania/ [dostęp: 04.2017 r.].

11 M. Goodman, *Zbrodnie*..., dz. cyt., s. 360.

12 *IOCTA – Internet Organised Crime Threat Assessment*, Europol, źródło: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [dostęp: 04.2017 r.].

13 Według Głównego Urzędu Statystycznego usługi chmury obliczeniowej to możliwość korzystania ze skalowalnych usług ICT przy zastosowaniu Internetu. Usługi świadczone w chmurze obliczeniowej mogą obejmować dostęp do oprogramowania, korzystanie z określonej mocy obliczeniowej, przechowywanie danych, *Chmura obliczeniowa*, źródło: http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3086,pojecie.html [dostęp: 04.2017 r.].

14 B. Hołyst, *Bezpieczeństwo gatunku ludzkiego*, t. 4, Warszawa 2016, s. 135–139.

postrzeganie sztucznej inteligencji jako zbioru systemów informatycznych, które przy użyciu odpowiednich algorytmów są w stanie wykonywać czynności, do których normalnie potrzebna jest ludzka inteligencja, takich jak podejmowanie decyzji, czy rozpoznawanie. To pozwala na stworzenie procesów autonomicznych, uniezależnionych od człowieka, za pomocą narzędzi oferowanych przez infrastrukturę „Internetu Rzeczy"[15]. Technologia ta jest mocno niedoceniana, jednak wszechobecna, zainteresowane są nią wszystkie sektory przemysłu (w tym zbrojeniowy), usług, a także podmioty państwowe. Bez niej nie mogłyby funkcjonować współczesne systemy nawigacji, portale społecznościowe, czy wyszukiwarki internetowe. Rozwój sztucznej inteligencji wywołuje ogromne kontrowersje w środowisku naukowców, ale też producentów powiązanych usług i produktów, zdominowanego przez entuzjastów reklamujących same zalety swoich produktów[16]. Na czele sceptyków przesadnego uniezależniania procesów od ludzkiej woli stoi E. Musk, który stał się propagatorem stwierdzenia: „sztuczna inteligencja i rywalizacja na polu jej rozwoju na szczeblu narodowym może być czynnikiem, który wywoła trzecią wojnę światową". Musk stanął na czele grupy 116 ekspertów, którzy wystosowali list otwarty do ONZ[17], apelując o podjęcie działań mających zatrzymać rozwój broni autonomicznej, która ma być przyczynkiem do „trzeciej rewolucji pola walki" po wprowadzeniu prochu strzelniczego i broni nuklearnej w przeszłości. Główną obawą sygnatariuszy listy jest możliwość wymknięcia się maszyn spod ludzkiej kontroli[18].

Z powyższych twierdzeń można wysnuć wniosek, że zwyczajne przedmioty stają się *de facto* urządzeniami o podobnej charakterystyce co komputery. Poparciem dla takiego rozumowania wydaje się próba legalnego zdefiniowania pojęcia „komputer" podjęta w Stanach Zjednoczonych – „wszelkie obiekty przeznaczone do przechowywania danych lub komunikacji bezpośrednio związane lub współdziałające z takimi urządzeniami"[19]. Stopniowo kolejne przedmioty codziennego użytku uzyskują możliwość podłączenia do sieci. Dla uporządkowania, warto przywołać klasyfikację systemowych zastosowań Internetu Rzeczy utworzoną przez M. Kołodzieja:

1) inteligentne domy, budynki, posesje;
2) inteligentne miasta;
3) monitoring pojazdów;
4) inteligentne sieci medyczne;
5) inteligentne przedsiębiorstwa i przemysł;
6) inteligentne systemy energetyczne i pomiarowe;

---

15 Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, *Innowacyjna gospodarka, analiza na zlecenie Ministerstwa Cyfryzacji*, źródło: https://mc.gov.pl/files/innowacyjna_cyfryzacja_0.pdf [dostęp: 03.2017 r.], s. 34–35.

16 G. Hall, *Zuckerberg blasts Musk warnings against artificial intelligence as 'pretty irresponsible'*, źródło: https://www.bizjournals.com/sanjose/news/2017/07/24/elon-musk-artificial-intelligence-risk-zuckerberg.html [dostęp: 09.2017 r.].

17 Organizacja Narodów Zjednoczonych.

18 S. Gibbs, *Elon Musk leads 116 experts calling for outright ban of killer robots*, źródło: https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war [dostęp: 09.2017.].

19 M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 10.

7) systemy monitorowania środowiska[20].

Ten sam autor wśród przykładowych zastosowań „Internetu Rzeczy" wymienia między innymi inteligentny budzik, który dostosuje porę alarmu w zależności od natężenia ruchu na drodze do pracy, sportowe obuwie zastępujące powszechnie używane już opaski sportowe wykonujące pomiary poszczególnych parametrów takich jak tętno, pojemnik na leki przypominający choremu o konieczności zażycia lekarstwa, czy też systemy w infrastrukturze miejskiej ułatwiające kierowcom znalezienie miejsca parkingowego.

Według raportu „Digital in 2017" udział urządzeń mobilnych na rynku elektroniki stale rośnie. Polska znajduje się w czołówce państw, pod względem korzystania z Internetu za pomocą urządzeń mobilnych. Około 57% ruchu internetowego w Polsce w 2016 roku przypadało w udziale smartfonom i tabletom. Skala wzrostu znaczenia tych urządzeń widoczna jest w statystykach światowego udziału urządzeń mobilnych w ruchu internetowym. W 2009 roku udział ten wynosił poniżej 0,7%. W roku 2016 było to już około 50% globalnego ruchu internetowego. Po raz pierwszy urządzenia mobilne wyprzedziły tradycyjne komputery w udziale w globalnym ruchu internetowym. Ten wzrost pokazuje pewien trend, który będzie się utrzymywał, a największy na to wpływ mają państwa rozwijające się, co zdają się potwierdzać światowi liderzy w zestawieniu – Nigeria, Indie, RPA i Indonezja, z udziałem urządzeń mobilnych w sieci około 80%[21]. Według Komisji Nadzoru Finansowego w 2015 roku 43% użytkowników smartfonów w Polsce korzystała z usługi bankowości mobilnej[22]. O rosnącej skali zjawiska opróżniania kont bankowych użytkowników smartfonów za pomocą złośliwego oprogramowania media informowały wraz ze wzrostem skalą tego zjawiska. Już kilka lat temu zauważono, że nie są to przypadkowe ataki, a przestępczy biznes, ukierunkowany na możliwie jak największą efektywność. Koncentracja hakerów[23] na urządzeniach mobilnych nie może dziwić, gdyż zabezpieczenia w nich stosowane są jeszcze mniej skuteczne niż te w komputerach personalnych, czy laptopach[24]. Od wielu lat firma KasperskyLab w swoich raportach umieszcza szczegółowe dane dotyczące ataków i standardowych zagrożeń czyhających w sieci na urządzenia mobilne. Do największych należy zaliczyć:

1) niekontrolowane wycieki danych powodowane przez aplikację;

---

20 M. Kołodziej, *Internet Rzeczy, nowe spojrzenie na ochronę prywatności*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2015*, Szczytno 2015, s. 14–19.

21 S. Kemp, *Digital 2017: Global Overview*, źródło: https://wearesocial.com/special-reports/digital-in-2017-global-overview [dostęp: 09.2017 r.].

22 *KNF wydała rekomendację dot. bezpieczeństwa transakcji płatniczych w internecie*, bankier.pl, z dn. 17.11.2015, źródło: http://www.bankier.pl/wiadomosc/KNF-wydala-rekomendacje-dot-bezpieczenstwa-transakcji-platniczych-w-internecie-3442312.html [dostęp: 02.2017 r.].

23 Według Administratora Bezpieczeństwa Informacji UW T. Śmigielskiego, obecnie nie istnieje potrzeba szczególnego tytułowania złośliwych sprawców w cyberprzestrzeni. Istnieje terminologiczny podział na hackerów (hakerów) i crackerów ze względu na typy i charakter działań tych jednostek, jednak dla osoby potencjalnie zaatakowanej nie ma to znaczenia, a sformułowanie „hacker" weszło już do powszechnego użycia, T. Śmigielski, *Hacker i cracker*, źródło: https://portal.uw.edu.pl/web/ado/hacker-i-cracker [dostęp: 04.2017 r.].

24 M. Sparkes, *Hackers focus on stealing money from mobile banking*, źródło: http://www.telegraph.co.uk/technology/internet-security/10662106/Hackers-focus-on-stealing-money-from-mobile-banking.html [dostęp: 02.2017 r.].

2) korzystanie z darmowych, niezweryfikowanych sieci Wi-Fi;
3) „spoofing"oraz „phishing"[25] (szeroka gama metod wyłudzania danych);
4) złośliwe oprogramowanie gromadzące informacje – „ransomware", „malware", „spyware";
5) ataki na aplikacje modyfikujące ich kod, a w efekcie działanie.

W 2016 roku w ponad 30% państw członkowskich Unii Europejskiej organa ścigania wszczęły postępowania w sprawach nadużyć dotyczących przetwarzania danych w chmurze, a w blisko 50% z nich informowało o potrzebie gromadzenia dowodów z tego źródła. „Internet Rzeczy" stanie się w przyszłości nieodłącznym elementem „infrastruktury krytycznej", która będzie narażona na zagrożenia płynące z cyberprzestrzeni mogące skutkować fizycznym lub psychicznym uszczerbkiem na zdrowiu[26]. Zagrożenie dostrzega Europol, obecnie na celowniku cyberprzestępców znajdują się głównie dane osobowe i informacje biznesowe[27]. Techniki te nie są nowym wynalazkiem, jest to po prostu adaptacja metod wymyślonych już na początku istnienia sieci Internet, przy wykorzystaniu pełni możliwości jaką daje „Internet Rzeczy". Większość cyberprzestępców nieustannie skupia się na kradzieży danych, bo to one stanowią wartość samą w sobie, bądź są swego rodzaju „wytrychem" do dalszej przestępczej i szkodliwej działalności. Już w 2012 roku dane okrzyknięto „nową ropą naftową", a slogan ten jest szeroko powtarzany w środowiskach naukowych i publicystycznych[28].

Dla „Internetu Rzeczy" największym zagrożeniem wydaje się być „hacking", którego definicja sensu *stricto* została ujęta w kodeksie karnym, jako uzyskanie nieautoryzowanego dostępu do informacji. Nie oddaje to pełni zagrożeń, jakie „hacking" tworzy dla przedmiotów podłączonych do sieci. F. Radoniewicz rozszerza samo pojęcie na art. 267–269b Kodeksu Karnego. Jest to zjawisko, które może być rozumiane na wiele sposobów, a jego definicja będzie musiała obejmować coraz szersze spektrum czynności w toku postępu technologicznego. Prawo od dawna nie nadąża za rozwojem cyberprzestrzeni, a dystans ten będzie się pogłębiał. Problemem jest nie tylko definiowanie pojęć, ale również atrybucja czynów przestępczych i transgraniczny charakter działań[29]. Uściślając pojęcie, „hacking" można określić jako uzyskanie dostępu do systemu teleinformatycznego, zakłócenie jego

---

25 Definicje firmy Avast: „Spoofing" ma miejsce, gdy hacker podszywa się pod inne urządzenie lub innego użytkownika w sieci, aby wykraść dane, zainstalować złośliwe oprogramowanie lub ominąć mechanizmy kontroli dostępu, źródło: https://www.avast.com/pl-pl/c-spoofing [dostęp: 04.2017 r.], „Phishing" to przebiegła metoda, której używa cyberprzestępca, aby nakłonić użytkownika do ujawnienia informacji osobistych, takich jak hasła lub numery kart kredytowych, ubezpieczeń i kont bankowych. Robią to poprzez wysyłanie fałszywych e-maili lub przekierowywanie na fałszywe strony internetowe, *Phishing*, źródło: https://www.avast.com/pl-pl/c-phishing [dostęp: 04.2017 r.].

26 Europol, IOCTA…, *cyt. wyd*., s. 54.

27 *SOCTA 2017 – Serious and Organized Crime Threat Assesments*, Europol, źródło: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [dostęp: 04.2017 r.], s. 24.

28 P. Rotella, *Is Data The New Oil?*, źródło: https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#41d038e57db3 [dostęp: 09.2017 r.].

29 A. Brachman, *Internet przedmiotów – raport*, Obserwatorium ICT, wrzesień 2013 r.

pracy oraz modyfikację lub usunięcie danych w nim zawartych[30]. Większość ekspertów do spraw cyberbezpieczeństwa jest zgodna, że ścisłe definiowanie każdego cyberzagrożenia jest niezwykle trudne, a będzie ono zawsze zależało od atrybucji i celu napastnika, którym może być uzyskanie dostępu, oszustwo, kradzież, bądź zniszczenie danych[31]. Wykorzystywane przez hakerów narzędzia różnią się, są przedmiotem specjalistycznej debaty, w której osoba nie będąca informatykiem łatwo może się pogubić. Dlatego na potrzeby zwykłego użytkownika National Cyber Security Centre (komórka GCHQ[32]) utworzyła klasyfikację cyberataków (na potrzeby przedsiębiorstw, jednak dotyczą one również użytkownika indywidualnego):

1) atak nieukierunkowany – napastnik obiera za cel jak największą liczbę urządzeń, usług i użytkowników. Najważniejsza jest liczba ofiar, a nie ich tożsamość. Do ich przeprowadzenia używane są techniki takie jak:
   a) „phishing" – uzyskiwanie wrażliwych danych poprzez wysłanie wiadomości e-mail i użycie narzędzi inżynierii społecznej,
   b) „waterholing" – tworzenie fałszywej strony internetowej, bądź przejmowanie tej prawdziwej w celu wykorzystania odwiedzających użytkowników,
   c) „ransomware" – rozpowszechnianie złośliwego oprogramowania szyfrującego urządzenia (np. dyski twarde),
   d) „scanning" – wyrywkowe ataki na przypadkowe urządzenia podłączone do Internetu;
2) atak ukierunkowany – w tym przypadku napastnik atakuje określonego użytkownika urządzenia, bądź usługi. Atak tego rodzaju może być złożoną operacją trwającą miesiące i na ogół jest procesem o specyfikacji dostosowanej do ofiary, dlatego może wyrządzić znacznie większe szkody. Takie ataki należy podzielić na:
   a) „spear-phishing" – dystrybucja wiadomości e-mail, zawierających załącznik ze złośliwym oprogramowaniem, bądź link powodujący automatyczne pobieranie i instalacje takiego programu,
   b) „botnet" – przejęcie kontroli nad urządzeniem, w celu przeprowadzenia ataku DDoS na innym urządzeniu,
   c) przerywanie łańcucha dostaw – bezpośrednie atakowanie urządzeń, bądź oprogramowania zapewniającego usługi[33].

Do powyższej klasyfikacji warto dodać tezę K. Mitnick'a, który jako najsłabsze ogniwo w każdym systemie bezpieczeństwa informatycznego określa człowieka. Inżynieria społeczna wykorzystuje perswazję i wpływ do oszukania jednostki. Dobry inżynier społeczny jest w stanie wykorzystać ludzi do uzyskania potrzebnej mu informacji, nawet bez użycia

---

30 F. Radoniewicz, *Odpowiedzialność karna za przestępstwo hackingu*, Instytut Wymiaru Sprawiedliwości, Warszawa 2012, źródło: https://www.iws.org.pl/pliki/files/IWS_Radoniewicz_Odp%20za%20przest%20hackingu.pdf [dostęp: 02.2017 r.], s. 1–3.

31 B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, źródło: http://docplayer.pl/14827446-Artykuly-cyberprzestepczosc-ochrona-informacji-i-kryptologia-brunon-holyst-jacek-pomykala-streszczenie.html#show_full_text [dostęp: 04.2017 r.], s. 6.

32 Government Communications Headquarters (pol. Centrala Łączności Rządowej) – służba specjalna Wielkiej Brytanii zbierająca informacje pochodzące z wywiadu radioelektronicznego.

33 National Cyber Security Centre, źródło: https://www.ncsc.gov.uk/articles/how-cyber-attacks-work [dostęp: 09.2017 r.]

technologii[34]. Jeszcze do niedawna wydawało się, że tego typu zagrożenia dotyczą tylko komputerów personalnych, ale właśnie ze względu na internetową ekspansję „rzeczy" już dziś wiele urządzeń z podłączeniem do sieci można zainfekować za pomocą najbardziej prymitywnych działań, takich jak wysłanie wiadomości MMS na smartfon[35]. Jak wskazuje raport Europolu dotyczący zorganizowanej przestępczość internetowej, gama złośliwego oprogramowania stosowanego przez cyberprzestępców nieustannie rozszerza się, a sztywne definiowanie zagrożeń traci na znaczeniu. Wpływ miał na to postęp w telefonii komórkowej, zamieniający aparaty w *de facto* mobilne komputery. Oprócz złośliwego oprogramowania cyberprzestępcy wykorzystują system płatności anonimowych oraz rozwój tzw. „kryptowalut"[36] do działań korupcyjnych, fałszerstw, czy prania brudnych pieniędzy. Internet oraz sieci ukryte stały się rynkiem handlu nielegalnymi dobrami oraz przestępczymi usługami. Kryminaliści wykorzystują zakodowane kanały komunikacji w taki sposób, by pozostać nieuchwytnymi dla organów ścigania[37].

Wprowadzanie autonomicznych procesów w ramach „Internetu Rzeczy" zwiększa liczbę zsynchronizowanych urządzeń, czujników, czipów i mikrokontrolerów, które często nie są nawet objęte ochroną oprogramowania antywirusowego[38]. Skuteczność programów to kolejny problem wymagający pogłębionej refleksji. Dowodem na ich słabość stał się antywirus „Flame", który wstrząsnął sektorem informatycznym i obnażył prawdziwą skalę zaniedbań producentów i ich bezbronność w obliczu zagrożeń. Mimo pogłębionej dyskusji w środowisku, nie znaleziono do tej pory złotego środka[39]. Problemem jest nie tylko sama świadomość, ale również możliwość wykrycia ataku, która jest czasem mocno ograniczona, podobnie jak szansa na wykrycie sprawcy[40].

Współczesne systemy zabezpieczeń M. Goodman określił mianem „cyfrowej linii Maginota", ze względu na mnogość połączonych ze sobą urządzeń, danych wprowa-

---

34 K. Riccio, *Kevin Mitnick: 'People, Not Technology, Weakest Security Link'*, źródło: https://www.afcom.com/Public/Resource_Center/Articles/Kevin_Mitnick_People_Not_Technology_Weakest_Security_Link.aspx [dostęp: 09.2017 r.].

35 *Największa w historii luka w Androidzie. Twój telefon rozbroi zwykły MMS*, źródło: http://tvn24bis.pl/tech,80/luka-w-androidzie-na-atak-hakerow-narazonych-jest-950-mln-smartfonow,563931.html [dostęp: 02.2017 r.].

36 Wg Rafała Prabuckiego – „Pomimo tego, że w działaniu przypominają one pieniądz elektroniczny to w kontekście prawa nie są one ani pieniądzem, ani też walutą, na co wskazywałaby ich potoczna nazwa. Mimo to zyskały one rzeszę sympatyków, którzy monetom kryptograficznym nadali wartość i wyprowadzili tą ideę poza ramy cyberprzestrzeni, czyniąc pierwszą z nich – bitcoina – obiecującym eksperymentem w ujęciu płatności on-line za dobra, usługi i treści cyfrowe", R. Prabucki, *Kryptologia, a prawo – wybrane zagadnienia: idea kryptowaluty i jej wpływu na ewolucję oszustw w internecie*, [w:] M. Zieliński (red.), *Przegląd Nauk Stosowanych*, Nr 10, źródło: http://pns.po.opole.pl/pns/PNS_10.pdf#page=106 [dostęp: 04.2017 r.], s. 106.

37 *IOCTA…*, *cyt. wyd.*, s. 10–11.

38 *Top 7 Mobile Security Threats: Smart Phones, Tablets & Mobile Internet Devices – What the Future Has in Store*, źródło: https://usa.kaspersky.com/internet-security-center/threats/mobile-device-security-threats#.WJ7UxlU1_IU [dostęp: 02.2017 r.].

39 T. Simonite, *The Antivirus Era is Over*, źródło: https://www.technologyreview.com/s/428166/the-antivirus-era-is-over/ [dostęp: 02.2017 r.].

40 L. Greenemeier, *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, źródło: https://www.scientificamerican.com/article/tracking-cyber-hackers/ [dostęp: 09.2017 r.].

dzanych do sieci i brak skutecznych środków bezpieczeństwa[41]. Flagowym przykładem wykorzystania podatności układu „naczyń połączonych" jest historia amerykańskiego dziennikarza M. Honana z 2012 roku. Głównym celem cyberprzestępców, którzy zaatakowali Honana było jego konto na Twitterze, jednak w międzyczasie uzyskali oni dostęp do kilku kont ofiary oraz wrażliwych danych osobowych. W pierwszej kolejności hakerzy uzyskali podstawowe dane osobowe dziennikarza. Te informacje dosyć łatwo można było znaleźć w Internecie, a dane te posłużyły przestępcom do zmanipulowania pracownika centrali telefonicznej firmy Amazon, obsługującej sklep internetowy, w taki sposób, by ten wyjawił cztery ostatnie cyfry karty kredytowej Honana. Te dane w połączeniu z adresem zamieszkania ofiary i odpowiednimi zabiegami inżynierii społecznej zastosowanymi wobec pracowników działu obsługi klienta pozwoliły na uzyskanie dostępu do konta AppleID, do którego przypisany był adres konta Google, połączonego z kontem Twitter. Włamanie się na te konta, przy zebranych już informacjach nie stanowiło problemu. W trakcie całej operacji cyberprzestępcy uzyskali dane o obecnej lokalizacji dziennikarza, usunęli zawartość dysków wszystkich urządzeń firmy Apple, które znajdowały się w pobliżu. Honan utracił dostęp do kilku kont, a jego reputacja została nadszarpnięta, bowiem hakerzy wykorzystali konto Twitter to publikacji obraźliwych komentarzy i wiadomości. Warto zwrócić uwagę, że napastnicy posiadali już tak ogromną liczbę danych, że wyrządzone przez nich szkody mogły być znacznie większe, w przypadku włamania się na konto bankowe Honana. Okazało się, że połączenie odpowiednich narzędzi inżynierii społecznej z podstawową wiedzą na temat informatyki, pozwala na wyrządzenie ogromnych szkód użytkownikowi sieci Internet i urządzeń „Internetu Rzeczy". Obnażone zostały słabości systemów bezpieczeństwa największych światowych korporacji, obsługujących miliony klientów na całym świecie i gromadzących dane na ich temat. W tym przypadku został wykorzystany nie tylko mechanizm synchronizacji kont internetowych, ale również urządzeń, ponieważ uzyskując dostęp do jednego urządzenia Apple, „włamywacz" zlokalizował pozostałe zsynchronizowane urządzenia tej firmy w pobliżu, przez co również one stały się obiektem ataku[42]. Brak spójności i integralności między poszczególnymi zabezpieczeniami, różne standardy bezpieczeństwa poszczególnych dostawców usług są przyczynkiem dodatkowych zagrożeń dla użytkowników[43]. „Internet Rzeczy" to przestrzeń, w której przetwarzane są informacje zawierające dane osobowe, ale również informacje dotyczące ich aktywności i działań. Celowa ingerencja, bądź wpłynięcie na działanie jednego z elementów sytemu, może bardzo źle wpłynąć na pozostałe, powodując reakcję łańcuchową, a w efekcie spowodować dysfunkcję całego systemu. Urządzenia zbierają i przetwarzają dane o coraz większym stopniu wrażliwości, zwiększając dolegliwość konsekwencji ich nieodpowiedniego zabezpieczenia[44].Urządzenia mobilne stają się nieodłączną częścią ludzkiej codzienności. Jednak nie tylko dorośli stają się beneficjentem coraz szerszego dostępu do zaawansowanej technologii. Również osoby niepełnoletnie korzystają z urządzeń podłączonych do sieci i mogą

41 M. Goodman, *Zbrodnie…*, dz. cyt., s. 15.

42 M. Honan, *How Apple and Amazon security flaws let to my epichacking*, źródło: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/ [dostęp: 02.2017 r.].

43 M. Goodman, *Zbrodnie…*, dz. cyt., s. 15.

44 M. Kołodziej, *Internet…*, [w:] J. Kosiński (red.), dz. cyt., 2015, s. 20–21.

stać się ofiarą cyberprzestępców. Dane dotyczące dzieci po raz pierwszy padły łupem hakerów w 2015 roku, kiedy to jedna z firm produkujących zabawki podłączone do sieci została okradziona z danych około sześciu milionów osób nieletnich[45]. Było to wydarzenie bezprecedensowe, w trakcie postępowania wykryto rażące nieprawidłowości w zakresie polityki ochrony danych osobowych, a rodzice zostali wezwani do zbojkotowania produkowanych przez nią zabawek[46]. Obecnie większą obawę wzbudzają zabawki z technologią „Internetu Rzeczy". Jednym z takich przypadków jest sprawa „Hello Barbie" – lalki umożliwiającej dziecku rozmowę z zabawką wyposażoną w mikrofony oraz funkcję rozpoznawania głosu. Nie budziłoby to wielkich kontrowersji, gdyby nie fakt, że zabawki posiadają połączenie z siecią, która umożliwia jej zsynchronizowanie ze smartfonem, a treść rozmów dziecka i zabawki zostaje przetrzymywana w „chmurze" producenta. Nie jest jasne do czego te dane są wykorzystywane[47]. Norwescy eksperci przeprowadzili eksperyment, po którym określili „Hello Barbie" jako najbardziej podatną na cyberataki w związku z podłączeniem zabawki do sieci, które sprawia, że niemal każdy może dokonać próby jej zaatakowania[48]. Podobne obawy pojawiają się w społeczeństwie niemieckim. Federalna Agencja ds. Sieci (Bundesnetzagentur) określiła inną zabawkę tego typu – „My FriendCayla" jako „nielegalne narzędzie szpiegowskie", wymuszając na producencie wyłączenie funkcji sieciowych zabawki, która mogła zostać uznana za „narzędzie inwigilacyjne" w świetle niemieckiego Kodeksu Karnego[49]. Wyniki przeprowadzonego przez niemieckich dziennikarzy eksperymentu pokazały, że za pomocą łączności Bluetooth można uzyskać nieuprawniony dostęp do lalki i rozmawiać z dzieckiem. Lalka nie została zabezpieczona hasłem[50].

Praktyka pokazuje również, że urządzenia podłączone do sieci mogą stać się narzędziem znacznie poważniejszych nadużyć wobec nieletnich. Zagadnienie stało się poważne wraz z wybuchem afery w USA, kiedy to dyrekcja jednej ze szkół, udostępniając szkolne laptopy do użytku domowego swoim uczniom, jednocześnie zainstalowała w nim oprogramowanie szpiegowskie w celu obserwacji ich zachowań[51]. Wykorzystanie urządzeń rejestrujących w komputerach, czy smartfonach staje się powszechne w gronie cyberprzestępców. Rynek „elektronicznych niani" zyskuje na coraz większej popularności, a problemy z zabezpieczeniami zastosowanymi w tych urządzeniach pojawiły się w 2008 roku, gdy

---

45 *Millions of children's data hacked after 'biggest ever cyber attack' on toy firm*, Telegraph, 25.12.2015, źródło: http://www.telegraph.co.uk/news/uknews/law-and-order/12051439/Millions-of-childrens-data-hacked-after-biggest-ever-cyber-attack-on-toy-firm.html [dostęp: 02.2017 r.].

46 L. Kelion, *Parents Arged to boycott VTech toy safter hack*, źródło: http://www.bbc.com/news/technology-35532644 [dostęp: 02.2017 r.].

47 A. Walkowiak, *Szpieg pod choinkę?*, źródło: https://panoptykon.org/wiadomosc/szpieg-pod-choinke [dostęp: 02.2017 r.].

48 A. Johnsen, *Investigation of privacy and security issues with smart toys*, źródło: https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf [dostęp: 02.2017 r.].

49 P. Olterman, *German parents told to destroy doll that can spy on children*, źródło: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children [dostęp: 02.2017 r.].

50 C. Leistenschneider, *Die Abhöranlage im Kinderzimmer*, źródło: http://www.saarbruecker-zeitung.de/sz-spezial/internet/art371089,6380949 [dostęp: 02.2017 r.].

51 D. Kravets, *School District Allegedly Snapped Thousands of Student Webcam Spy Pics*, źródło: https://www.wired.com/2010/04/webcamscanda/ [dostęp: 02.2017 r.].

pewien mieszkaniec Stanów Zjednoczonych odkrył, że jego sąsiad posiadający takie samo urządzenie, tego samego producenta, jest w stanie podsłuchiwać i podglądać, co dzieje się w jego domu[52]. Poważniejszy przypadek miał miejsce w stanie Texas (USA) kilka lat później. Nieznany sprawca przejął kontrolę nad „elektroniczną nianią", służącą do opieki nad dwuletnim dzieckiem użytkowników. „Włamywacz" oprócz możliwości rejestrowania tego co dzieje się w pokoju dziecka, uzyskał dostęp do mikrofonu, mówił do dziecka po imieniu, dodatkowo napastując je nieprzyzwoitymi wyrażeniami[53]. Podobny przypadek miał miejsce w Ohio (USA), kiedy to kobieta odkryła, że z używanej przez nią „elektronicznej niani" wydobywa się męski głos, używający „obscenicznych" słów skierowanych do dziecka[54]. Tego typu urządzenia nie tylko posiadają podłączenie do Internetu, ale również często są zsynchronizowane z tabletami, bądź smartfonami użytkowników, przez które „nianie" są często obsługiwane. Z raportu senackiej Komisji Handlu, Nauki i Transportu (USA), wynika, że producenci zabawek rzadko dbają o bezpieczeństwo informacji dotyczących dzieci, zbierając jednocześnie ich podstawowe dane osobowe, zdjęcia, treść wiadomości pisemnych oraz głosowych, czy dane dotyczące lokalizacji. Analizie zostały poddane przypadki masowych wycieków danych z takich firm jak VTech, czy Fisher-Price[55]. Jak podkreśla Federalna Komisja Handlu (USA) wykradzione dane dzieci mogą być narzędziem w wyłudzeniach świadczeń socjalnych, otwieraniu kont bankowych, uzyskiwaniu pożyczek lub najmowaniu mieszkania[56].

Rozwijająca się automatyzacja nie pominęła budynków. Angielski termin „Smart Home" („Inteligentne Domy") to inaczej obiekty, które wysyłają dane do sieci, a jednocześnie potrafią je odbierać i przetwarzać. To „ekosystem", w którym przedmioty, sensory, czy urządzenia mogą się ze sobą komunikować, wymieniając dane za pośrednictwem łączności bezprzewodowej. Zebrane dane są przesyłane do chmury, gdzie następuje proces ich przetwarzania. Używając interfejsu (np. smartfon lub tablet), użytkownik może zdalnie korzystać z usług „Smart Home"[57]. Wszystkie urządzenia w takim systemie (podobnie jak komputer) posiadają indywidualny adres sieciowy, a oprócz możliwości obsługi przez interfejs, system posiada zdolność do autonomicznego wykonywania różnych operacji[58].

---

52 K. Zetter, *Man Sues Over Leaky Baby Monitor*, źródło: https://www.wired.com/2009/11/baby-monitor/ [dostęp: 02.2017 r.].

53 D. Gross, *Foul-mouthed hacker hijacks baby's monitor*, źródło: http://edition.cnn.com/2013/08/14/tech/web/hacked-baby-monitor/ [dostęp: 02.2017 r.].

54 *Hacker hijacks baby monitor*, FOX19, źródło: http://www.fox19.com/story/25310628/hacked-baby-monitor [dostęp: 02.2017 r.].

55 B. Nelson, *Children's Connected Toys: Data Security and Privacy Concerns*, źródło: https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf [dostęp: 09.2017 r.].

56 *7 Child Identity Theft*, Federal Trade Commission, źródło: https://www.consumer.ftc.gov/articles/0040-child-identity-theft [dostęp: 02.2017 r.].

57 B. Risteska Stojkoska, K. Trivodaliev, *A review of Internet of Things for Smart Home Challenges and solutions,* źródło: https://www.researchgate.net/publication/308975029_A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions [dostęp: 02.2017 r.], s. 5–6.

58 A. Ożadowicz, *Internet Rzeczy w systemach automatyki budynkowej*, źródło: https://www.researchgate.net/publication/269628658_Internet_Rzeczy_w_systemach_automatyki_budynkowej [dostęp: 02.2017 r.], s. 2–3.

Do najpopularniejszych rozwiązań w „Smart Home" należą systemy HVAC (ogrzewania, wentylacji i klimatyzacji), kontroli oświetlenia, systemy bezpieczeństwa i kontroli dostępu, systemy alarmowe, systemy przeciwpożarowe oraz systemy audiowizualne[59]. Urządzenia produkowane są z myślą o minimalizacji kosztów i poboru energii. Na tym skupiają się producenci, kosztem kwestii bezpieczeństwa. Biorąc pod uwagę ilość połączeń oraz zsynchronizowanych urządzeń „Internetu Rzeczy" w systemach automatyki domowej, łatwo wyobrazić sobie skalę szkód jaką mogą wywołać cyberprzestępcy mając dostęp do ogromnej ilości danych wrażliwych domowników i mnogość potencjalnych punktów dostępowych. W jednym z raportów firma Kaspersky podkreśla rosnący udział cyberataków na urządzenia „Internetu Rzeczy" poprzez router, za pośrednictwem którego urządzenia łączą się z siecią[60].

Mimo początkowej fazy rozwoju systemów automatyki domowej, nie brakuje przykładów na ich podatności w zakresie bezpieczeństwa. W 2013 roku dziennikarz K. Hill, podczas pracy nad artykułem, wpisała w wyszukiwarkę internetową frazę „Smart Home". Bez szczególnych umiejętności w zakresie informatyki ta czynność doprowadziła ją na stronę internetową firmy Insteon oferującej instalacje automatyki domowej, gdzie uzyskała dostęp do systemów kilku klientów firmy. Z poziomu strony internetowej Hill mogła kontrolować urządzenia (manipulować temperaturą w domu, a nawet otworzyć bramę garażową) w domach rodzin korzystających z usług Insteon oraz uzyskała dostęp do informacji na temat domowników. Afera, którą wywołała ta sytuacja, doprowadziła do odkrycia kolejnych nieprawidłowości w stosowanych przez firmę systemach[61]. Ofiarą przestępców może zostać niemal każde urządzenie w „Inteligentnym Domu", nie wykluczając z tego grona tostera podłączonego do sieci. Nie oznacza to, że haker za wszelką cenę chce przejąć kontrolę nad urządzeniem wykorzystywanym do przygotowywania posiłków, po prostu zaprogramowane przez niego złośliwe oprogramowanie automatycznie wyszukuje niezabezpieczone porty w całej sieci[62]. Być może toster nie jest kluczem pozwalającym przestępcy na fizyczne włamanie się do domu, ale synchronizacja wszystkich „rzeczy" może doprowadzić cyberprzestępcę do innych urządzeń, przetwarzających wrażliwe dane, bądź będących elementami systemu bezpieczeństwa[63]. Ataki na sprzęt AGD nie są jednak tak powszechne, jak te na sprzęt audiowizualny. Niepokojące stają się doniesienia o wrażliwości na cyberataki urządzeń takich jak „Apple Siri", „Google Home", czy „Amazon Echo". Są to zyskujący na popularności „asystenci" dowodzenia „Inteligentnych Domów", sterowane za pomocą komend głosowych. Możliwe jest zainfekowanie wirusem tych urzą-

---

59 N. Ul Mushtaq, *Smart Home*, źródło: http://cctvinstitute.co.uk/smart-home/ [dostęp: 02.2017 r.].

60 A. DeNisco, *Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise*, źródło: http://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/ [dostęp: 09.2017 r.].

61 K. Hill, *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet*, źródło: http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#49e204f546a5 [dostęp: 02.2017 r.].

62 A. McGill, *The Inevitability of Being Hacked*, źródło: https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/ [dostęp: 02.2017 r.].

63 A. Greenberg, *Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms*, źródło: https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/ [dostęp: 02.2017 r.].

dzeń w tradycyjny sposób, jednak chińscy i amerykańscy eksperci twierdzą, że za pomocą odtwarzania dźwięku o wysokiej częstotliwości (niesłyszalnych dla ludzkiego ucha) są w stanie przejąć kontrolę nad „asystentami”[64]. Mało prawdopodobne by taka praktyka stała się powszechna, jednak takie przykłady pokazują, że wystarczająco zmotywowany napastnik może uzyskać nieuprawniony dostęp do urządzenia, bądź danych w sposób niemożliwy do przewidzenia. Wiele urządzeń w „Smart Home” wykorzystuje łącze Bluetooth. We wrześniu 2017 roku firma Armis odkryła nowe narzędzie w rękach hakerów zagrażające urządzeniom mobilnym, komputerom oraz urządzeniom „Internetu Rzeczy”. Eksperci Armis określili jako najbardziej zagrożone wszystkie rodzaje telefonów, tabletów oraz urządzenia „ubierane”. Zagrożone są również urządzenia w systemach automatyki domowej oraz „elementy infrastruktury krytycznej”, takie jak samochody i urządzenia medyczne. Łączna liczba urządzeń potencjalnie podatnych na atak została obliczona na ponad 8 miliardów. Wiele z nich zostanie uodpornionych na atak poprzez aktualizację oprogramowania, lecz będą to głównie smartfony i komputery[65]. Nową podatność nazwano „BlueBorne”, nie jest to rodzaj złośliwego oprogramowania, a „wektor ataku”, który hakerzy wykorzystują dzięki wrażliwości urządzeń z włączoną łącznością Bluetooth. Uzyskując dostęp do jednego urządzenia, można z łatwością „włamać się” do kolejnego urządzenia z włączonym Bluetooth, nawet jeśli oba urządzenia nie zostały ze sobą wcześniej zsynchronizowane[66]. Wielu użytkowników smartfonów posiada aktywną łączność Bluetooth przez cały czas użytkowania urządzenia. Można sobie łatwo wyobrazić sytuację, w której właściciel restauracji postanowił skorzystać w swoim lokalu ze sprzętu grającego z technologią Bluetooth (takie urządzenia zyskują na popularności, podobnie jak bezprzewodowe zestawy słuchawkowe). Gdyby hakerowi udało się uzyskać dostęp do wspomnianego głośnika, mógłby on za jego pośrednictwem „włamać się” do smartfonów dużej części klientów restauracji. Podobnie, mógłby przejąć kontrolę nad wszystkimi tabletami, komputerami i innymi urządzeniami z tym standardem łączności, które znalazły się w zasięgu głośnika. Identyczny scenariusz mógłby mieć miejsce w każdym domu i to niekoniecznie tym „inteligentnym”. Już dzisiaj w wielu gospodarstwach domowych znajduje się kilkanaście urządzeń Bluetooth, a część z nich korzysta również z łączności internetowej[67].

Zagrożenia dla prywatności płyną nie tylko ze świata przestępczego, ale również od producentów. Przykładem jest autonomiczny odkurzacz firmy Roomba, którego producenci chwalą się, że urządzenie zbiera informacje na temat swojego otoczenia w trakcie pracy

64 *‘Dolphin’ attacks fool Amazon, Google voice assistants*, BBC, źródło: http://www.bbc.com/news/technology-41188557 [dostęp: 09.2017 r.].

65 B. Seri, G. Vishnepolsky, *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks*, źródło: http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf [dostęp: 09.2017 r.].

66 *The Attack Vector “BlueBorne” Exposes Almost Every Connected Device*, źródło: https://www.armis.com/blueborne/ [dostęp: 09.2017 r.].

67 M. Nowak, *Nasze lenistwo jeszcze odbije się czkawką. Blue Borne to spełnienie najczarniejszej wizji dla smart domów*, źródło: http://www.spidersweb.pl/2017/09/blueborn-bluetooth-bezpieczenstwo.html [dostęp: 09.2017 r.].

„mapując" przy okazji mieszkanie użytkownika, a zebrane dane, mają być sprzedawane producentom systemów automatyki domowej[68].

Podsumowanie

Jeden artykuł nie jest formatem wystarczającym do ukazania pełnej skali zagrożeń jakie prezentuje sobą „Internet Rzeczy" i związane z nim technologie. Ingerencja w życie człowieka urządzeń podłączonych do sieci będzie coraz większa, wraz z postępem technologicznym, rozwojem technologii „ubieranych", zautomatyzowanych i autonomicznych środków transportu, urządzeń medycznych podłączonych do sieci, czy rozwoju „Smart Cities". Na przestrzeni lat zdaje się podupadać mit o skuteczności oprogramowania antywirusowego, producenci przeznaczają nieznaczne środki finansowe na wzmocnienie cyberbezpieczeństwa, a przestępcy znaleźli w Internecie bezpieczną przystań, chroniącą od atrybucji potencjalnych działań. Gromadzone dane będą wykorzystywane nie tylko przez przestępców, ale również przez międzynarodowe korporacje oraz podmioty państwowe. Zakres oraz sposoby ich użycia będą ograniczone jedynie wyobraźnią i możliwościami technicznymi dysponenta danych. Tworzy to wiele potencjalnych niebezpieczeństw, których skutki trudno jest przewidzieć. Wyzwania w zakresie cyberbezpieczeństwa stoją nie tylko przed indywidualnymi użytkownikami, ale również przed korporacjami, służbami bezpieczeństwa, prawodawcami. „Internet Rzeczy" staje się integralną częścią życia, której zabezpieczenie jest kwestią nieodzowną do zapewnienia bezpieczeństwa jednostki, społeczeństw i państwa. Niezwykle ważna jest współpraca i spójność podejmowanych działań, bowiem każda niezgodność i brak synchronizacji, będzie tworzyć luki w systemie bezpieczeństwa. Ich stopniowym wypełnianiem powinni zająć się eksperci, jednak odpowiedzialność spoczywa również na użytkownikach. Dlatego na koniec warto przytoczyć cytat K. Mitnick'a: „Odkryłem, że łatwiej jest manipulować ludźmi niż technologią"[69].

Tytuł w języku angielskim:
INTERNET OF REAL THREATS

Bibliografia

Publikacje zwarte i artykuły naukowe

Brachman A., *Internet przedmiotów – raport*, Obserwatorium ICT, wrzesień 2013 r.

Goodman M., *Zbrodnie przyszłości: jak cyberprzestępcy, korporacje i państwa mogą użyć technologii przeciwko Tobie*, Gliwice 2016.

[68] R. Jones, *Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder*, źródło: http://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829 [dostęp: 09.2017 r.].

[69] *Kevin Mitnick Quotes*, źródło:https://www.brainyquote.com/quotes/quotes/k/kevinmitni613263.html [dostęp: 09.2017 r.].

Hołyst B., *Bezpieczeństwo gatunku ludzkiego*, t. 4, Warszawa 2016.

Kołodziej M., *Internet Rzeczy, nowe spojrzenie na ochronę prywatności*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2015*, Szczytno 2015.

Siwicki M., *Cyberprzestępczość*, Warszawa 2013.

Źródła internetowe

7 Child Identity Theft, Federal Trade Commission, źródło: https://www.consumer.ftc.gov/articles/0040-child-identity-theft [dostęp: 09.2017 r.].

Allen G.C., źródło: http://edition.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html [dostęp: 09.2017 r.].

BBC, *'Dolphin' attacks fool Amazon, Google voice assistants*, źródło: http://www.bbc.com/news/technology-41188557.

Chmura obliczeniowa, http://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/3086,pojecie.html.

DeNisco A., *Report: 2016 saw 8.5 million mobile malware attacks, ransomware and IoT threats on the rise*, źródło: http://www.techrepublic.com/article/report-2016-saw-8-5-million-mobile-malware-attacks-ransomware-and-iot-threats-on-the-rise/ [dostęp: 09.2017 r.].

Europol, *IOCTA – Internet Organised Crime Threat Assessment*, źródło: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 [dostęp: 09.2017 r.].

Europol, *SOCTA 2017 – Serious and Organized Crime Threat Assesments*, źródło: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017 [dostęp: 09.2017 r.].

European Police Chiefs Convention: The future of organised crime chellenges and recommended, Europol, źródło: https://www.europol.europa.eu/publications-documents/european-police-chiefs-convention-future-of-organised-crime-challenges-and-recommended [dostęp: 09.2017 r.].

Gibbs S., *Elon Musk leads 116 experts calling for outright ban of killer robots*, źródło: https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war.

Greenberg A., *Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms*, źródło: https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/.

Greenemeier L., *Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers*, źródło: https://www.scientificamerican.com/article/tracking-cyber-hackers/.

Gross D., *Foul-mouthed hacker hijacks baby's monitor*, http://edition.cnn.com/2013/08/14/tech/web/hacked-baby-monitor.

Hacker hijacks baby monitor, FOX19, źródło: http://www.fox19.com/story/25310628/hacked-baby-monitor.

Hall G., *Zuckerberg blasts Musk warnings against artificial intelligence as 'pretty irresponsible'*, źródło: https://www.bizjournals.com/sanjose/news/2017/07/24/elon-musk-artificial-intelligence-risk-zuckerberg.html [dostęp: 09.2017 r.].

Hołyst B., Pomykała J., *Cyberprzestępczość, ochrona informacji i kryptologia*, źródło: http://docplayer.pl/14827446-Artykuly-cyberprzestepczosc-ochrona-informacji-i-kryptologia-brunon-holyst-jacek-pomykala-streszczenie.html#show_full_text.

Honan M., *How Apple and Amazon security flaws let to my epic hacking*, źródło: https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.

Hill K., *When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet*, źródło: http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/#49e204f546a5.

ITU-T Y.4000/Y.2060 (06/2012) – Overview of the Internet of things, ITU, 15.06.2015, źródło: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

Johnsen A., *Investigation of privacy and security issues with smart toys*, źródło: https://fil.forbrukerradet.no/wp-content/uploads/2016/12/2016-11-technical-analysis-of-the-dolls-bouvet.pdf.

Jones R., *Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder*, źródło: http://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829.

Kelion L., *Parents urged to boycott VTech toys after hack*, źródło: http://www.bbc.com/news/technology-35532644.

Kemp S., *Digital 2017: Global Overview*, źródło: https://wearesocial.com/special-reports/digital-in-2017-global-overview.

Kevin Mitnick Quotes, źródło: https://www.brainyquote.com/quotes/quotes/k/kevinmitni613263.html [dostęp: 09.2017 r.].

KNF wydała rekomendację dot. bezpieczeństwa transakcji płatniczych w internecie, bankier.pl, 17.11.2015, źródło: http://www.bankier.pl/wiadomosc/KNF-wydala-rekomendacje-dot-bezpieczenstwa-transakcji-platniczych-w-internecie-3442312.html.

Kolenda P. (red.), Raport – *Internet Rzeczy w Polsce*, IAB Polska, źródło: http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf.

Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, *Innowacyjna gospodarka, analiza na zlecenie Ministerstwa Cyfryzacji*, źródło: https://mc.gov.pl/files/innowacyjna_cyfryzacja_0.pdf [dostęp: 09.2017 r.].

Kravets D., *School District Allegedly Snapped Thousands of Student Webcam Spy Pics*, źródło: https://www.wired.com/2010/04/webcamscanda/ [dostęp: 09.2017 r.].

Leistenschneider C., *Die Abhöranlage im Kinderzimmer*, źródło: http://www.saarbruecker-zeitung.de/sz-spezial/internet/art371089,6380949 [dostęp: 09.2017 r.].

McGill A., *The Inevitability of Being Hacked*, źródło: https://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/ [dostęp: 09.2017 r.].

Millions of children's data hacked after ‚biggest ever cyber attack' on toy firm, Telegraph, 25.12.2015, źródło: http://www.telegraph.co.uk/news/uknews/law-and-order/12051439/Millions-of-childrens-data-hacked-after-biggest-ever-cyber-attack-on-toy-firm.html [dostęp: 09.2017 r.].

Największa w historii luka w Androidzie. Twój telefon rozbroi zwykły MMS, źródło: http://tvn24bis.pl/tech,80/luka-w-androidzie-na-atak-hakerow-narazonych-jest-950-mln-smartfonow,563931.html [dostęp: 09.2017 r.].

National Cyber Security Centre, źródło: https://www.ncsc.gov.uk/articles/how-cyber-attacks-work.

Nelson B., *Children's Connected Toys: Data Security and Privacy Concerns*, źródło: https://www.billnelson.senate.gov/sites/default/files/12.14.16_Ranking_Member_Nelson_Report_on_Connected_Toys.pdf [dostęp: 09.2017 r.].

Nowak M., *Nasze lenistwo jeszcze odbije się czkawką. BlueBorne to spełnienie najczarniejszej wizji dla smart domów*, źródło: http://www.spidersweb.pl/2017/09/blueborn-bluetooth-bezpieczenstwo.html [dostęp: 09.2017 r.].

Olterman P., *German parents told to destroy doll that can spy on children*, źródło: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children [dostęp: 09.2017 r.].

Ożadowicz A., *Internet Rzeczy w systemach automatyki budynkowej*, źródło: https://www.researchgate.net/publication/269628658_Internet_Rzeczy_w_systemach_automatyki_budynkowej [dostęp: 09.2017 r.].

Prabucki R., *Kryptologia, a prawo – wybranezagadnienia: idea kryptowaluty i jej wpływu na ewolucję oszustw w internecie*, [w:] M. Zieliński (red.), *Przegląd Nauk Stosowanych*, Nr 10, źródło: http://pns.po.opole.pl/pns/PNS_10.pdf#page=106 [dostęp: 09.2017 r.].

Radoniewicz F., *Odpowiedzialność karna za przestępstwo hackingu*, Instytut Wymiaru Sprawiedliwości, Warszawa 2012, źródło: https://www.iws.org.pl/pliki/files/IWS_Radoniewicz_Odp%20za%20przest%20hackingu.pdf [dostęp: 09.2017 r.].

Riccio K., *Kevin Mitnick: 'People, Not Technology, Weakest Security Link'*, źródło: https://www.afcom.com/Public/Resource_Center/Articles/Kevin_Mitnick_People_Not_Technology_Weakest_Security_Link.aspx. [dostęp: 09.2017 r.].

Risteska Stojkoska B., Trivodaliev K., *A review of Internet of Things for Smart Home Challenges and solutions*, źródło: https://www.researchgate.net/publication/308975029A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions [dostęp: 09.2017 r.].

Rorot W., *Rzeczy Internetu Rzeczy*, źródło: http://2016.dariah.pl/wpcontent/uploads/sites/3/2016/04/Wiktor.Rorot_.pdf [dostęp: 09.2017 r.].

Rotella P., *Is Data The New Oil?*, źródło: https://www.forbes.com/sites/perryrotella/2012/04/02/is-data-the-new-oil/#41d038e57db3 [dostęp: 09.2017 r.].

Seri B., Vishnepolsky G., *The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks*, źródło: http://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper.pdf.

Simonite T., *The Antivirus Era is Over*, źródło: https://www.technologyrview.com/s/428166/the-antivirus-era-is-over/ [dostęp: 09.2017 r.].

Śmigielski T., *Hacker i cracker*, źródło: https://portal.uw.edu.pl/web/ado/hacker-i-cracker [dostęp: 09.2017 r.].

Swirski K., *Internet Rzeczy (Internet of Things), czyli trend, który zmieni nasz sposób kupowania i używania*, źródło: http://konradswirski.blog.tt.com.pl/internet-rzeczy-internet-of-things-czyli-trend-ktory-zmieni-nasz-sposob-kupowania-i-uzywania/ [dostęp: 09.2017 r.].

The Attack Vector "BlueBorne" Exposes Almost Every Connected Device, źródło: https://www.armis.com/blueborne/ [dostęp: 09.2017 r.].

The General Data Protection Regulation została zatwierdzona 24 maja 2016 roku i wejdzie w życie 25 maja 2018 roku, źródło: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679&from=en [dostęp: 09.2017 r.].

Top 7 Mobile Security Threats: Smart Phones, Tablets & Mobile Internet Devices – What the Future Has in Store, źródło: https://usa.kaspersky.com/internet-security-center/threats/mobile-device-security-threats#.WJ7UxlU1_IU [dostęp: 09.2017 r.].

Twitter, Snapchat, Internet Rzeczy. Dane konsumenta na wyciągnięcie ręki, źródło: http://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/1017004,twitter-snapchat-iot-czyli-dane-konsumenta-na-wyciagniecie-reki-20-00.html [dostęp: 09.2017 r.].

Ul Mushtaq N., *Smart Home*, źródło: http://cctvinstitute.co.uk/smart-home/ [dostęp: 09.2017 r.].

Walkowiak A., *Szpieg pod choinkę?*, źródło: https://panoptykon.org/wiadomosc/szpieg-pod-choinke [dostęp: 09.2017 r.].

Zetter K., *Man Sues Over Leaky Baby Monitor*, źródło: https://www.wired.com/2009/11/baby-monitor [dostęp: 09.2017 r.].