# Internet zabawek

## Wsparcie dla rozwoju dziecka czy zagrożenie

Anna Rywczyńska
Przemysław Jaroszewski

NASK

# internet zabawek

## wsparcie dla rozwoju dziecka czy zagrożenie

NASK

# 1. Wstęp

Zabawki integrujące technologie nie są niczym nowym. Włączanie zaawansowanych funkcji technologicznych, w tym np. mikroprocesorów, które umożliwiają interaktywność podczas zabawy, ma już długą tradycję. Powszechnie znane są mówiące lalki czy też zdalnie sterowane samochody wyścigowe. Już w końcu zeszłego wieku powstawały zabawki typu robot-pies AIBO czy też tamagotchi. Jednakże pojawiające się w ostatnich latach interaktywne zabawki podłączone (*smart connected*), będące naturalną kontynuacją rozwoju dziedziny internetu rzeczy (*Internet of Things – IoT*), mogą wprowadzić rewolucję do dziecięcego świata zabawek. Komunikatywni towarzysze, zapewniając dziecku atrakcyjny sposób spędzania czasu, wspierając edukację i naukę technologii, wnoszą również sporą porcję wyzwań, głównie w kontekście prywatności, ochrony danych, ale również w aspekcie społecznym. Zabawki bazujące na infrastrukturze internetu i technologiach mobilnych potencjalnie podatne są bowiem na wszystkie zagrożenia związane z cyberprzestępczością, jak również niosą ze sobą nowe wyzwania związane z rozwojem poznawczym dzieci.

**Internet zabawek to jedna z prężniej rozwijających się dziedzin gospodarki. Jak podaje raport Juniper Research[1], łączna liczba przesyłek handlowych z zabawkami typu smart w 2017 roku, to odpowiednio w mln:**

**118,2 Ameryka**
**52,5 Europa**
**53,3 reszta świata**
**W Chinach przewiduje się wzrost średnio o 47 proc. rocznie do 2022 roku, co będzie stanowiło 18-procentowy udział w globalnym rynku przesyłek inteligentnych zabawek.**

1 Juniper Research, *Smart Toys: Market Summary* 2017.

Problematyka bezpieczeństwa internetu rzeczy (inaczej: internetu przedmiotów) początkowo obecna była jedynie w środowiskach związanych z bezpieczeństwem systemów teleinformatycznych. Właśnie za przyczyną internetu zabawek zaistniała w środowiskach zajmujących się bezpieczeństwem dzieci online. W grudniu 2016 roku FOSI (Family Online Safety Institute) opublikował dokument *Kids and the Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots*, w którym wstępnie badany jest krajobraz świata inteligentnych zabawek pod kątem bezpieczeństwa oraz pod kątem podstaw do zastosowania praw ujętych w COPPA (Children's Online Privacy Protection Act) w odniesieniu do producentów zabawek oraz dostawców implementowanej w nich technologii. W raporcie tym zaprezentowana została również wstępna typologia interaktywnych zabawek dzieląca je na trzy kategorie:

- **smart toys** – zabawki zawierające elementy „sztucznej inteligencji", tj. uczenia się, przetwarzania informacji od dziecka itp., lecz wykonujące wszystkie analizy lokalnie, bez przesyłania danych do zewnętrznego serwisu;
- **connected toys** – zabawki przesyłające dane (np. zdjęcia, pliki dźwiękowe) do zewnętrznego serwisu, lecz nieposiadające elementów „sztucznej inteligencji";
- **connected smart toys** – zabawki łączące cechy obu grup, wykorzystujące zasoby zewnętrznego serwisu, do którego przesyłane są zbierane przez urządzenie dane, do zaawansowanej komunikacji z użytkownikiem.

W lipcu 2017 roku Centrum ds. Przestępstw w Internecie FBI wydało specjalne ostrzeżenie. Jego celem jest zachęcenie konsumentów do zastanowienia się nad bezpieczeństwem cybernetycznym, zanim wprowadzi się inteligentne, interaktywne zabawki podłączone do internetu do swoich domów. W przypadku zabawek smart na odpowiedź czeka wiele pytań, w tym: jak wygląda bezpieczeństwo danych – często wrażliwych – zbieranych przez urządzenia, co się z nimi dzieje? Jak są chronione? Kto może wejść w ich posiadanie? Czego potrzeba, by kontrolę nad nimi przejęła osoba postronna? Mając na uwadze potencjalne zagrożenia mogące wyniknąć z posiadanie inteligentnej zabawki, wydaje się ważne, żeby osoba zainteresowana jej kupnem mogła swoją decyzję podjąć jak najbardziej świadomie, w czym – mamy nadzieję – pomocny będzie niniejszy poradnik. Jego zawartość powstała w ramach projektu realizowanego w Państwowym Instytucie Badawczym NASK „Internet zabawek – wsparcie dla rozwoju dziecka czy zagrożenie".

**Projekt objął:**

- pilotażowe badania jakościowe w postaci wywiadów dotyczących zróżnicowanych postaw i praktyk właściwych dla osób o różnych poziomach kapitałów (ekonomicznego, kulturowego), związanych z używaniem urządzeń cyfrowych należących do kategorii internetu rzeczy (IoT) ze szczególnym uwzględnieniem inteligentnych, podłączonych zabawek;
- badania ilościowe sprawdzające poziom rozpowszechnienia inteligentnych zabawek oraz stan wiedzy dotyczącej ich bezpieczeństwa;
- przeprowadzenie testów wybranych produktów pod kątem podatności na cyberzagrożenia oraz zaimplementowanych zabezpieczeń producenckich
  - w tym opis informacji dotyczących prywatności i bezpieczeństwa przekazywanych przez producenta przed zakupem oraz wewnątrz opakowania
  - w warstwie technicznej: rodzaj transmitowanych danych i miejsce ich składowania oraz przetwarzania, sposób ochrony (np. szyfrowanie) i poprawność jej implementacji, a także dostępność i skuteczność ochrony przed treściami niepożądanymi.

Przygotowane opracowanie ma za zadanie zaznajomić potencjalnych nabywców z problematyką dotyczącą inteligentnych zabawek. Prezentowane definicje terminów i zjawisk, opisy funkcjonalności oraz rekomendacje mają ułatwić bezpieczne korzystanie z technologii IoT w domach, w tym z interaktywnych podłączonych zabawek.

# 2. Dzieci – pierwsi odbiorcy nowych technologii

Technologia cyfrowa jest dziś nieodłącznym elementem codzienności i towarzyszy prawie każdej czynności zarówno zawodowej, jak i prywatnej. Służy do robienia zakupów, dokonywania płatności, rezerwowania urlopów, komunikacji oraz utrzymywania kontaktów ze znajomymi, jest elementem pracy czy też pozyskiwania wiedzy i informacji. Dzieci dorastają w otoczeniu technologii cyfrowej praktycznie od urodzenia, a średnia wieku, kiedy zaczynają samodzielnie korzystać z sieci, to 9–10 lat. Ponad 93 proc. polskich nastolatków jest w zasadzie cały czas online[2], a dostęp do szerokopasmowego internetu posiada prawie 80 proc. gospodarstw domowych[3]. W ostatnich latach zauważa się dynamiczny wzrost wykorzystywania przez dzieci i młodzież technologii mobilnych: tablety oraz smartfony coraz częściej zastępują komputery stacjonarne. Ponad 30 proc. młodzieży jest praktycznie cały czas online za pośrednictwem telefonów komórkowych[4]. Rozwijają się media społecznościowe (*social media*) bardzo mocno osadzone w sferze internetu mobilnego, robotyka (*robotics*), rzeczywistość wirtualna/rozszerzona VR/AR (*Virtual Reality/Augmented Reality*) – najszybciej rozwijająca się w sferze rozrywki, ale mająca też coraz więcej zastosowań w edukacji, czy też AI (*Artificial Intelligence*) – sztuczna inteligencja, która w przewidywaniach ma zrewolucjonizować między innymi świat przemysłu. Coraz powszechniejsze są również rozwiązania z dziedziny internetu rzeczy – (*Internet of Things* – IoT) – rozwiązania pozwalającego na gromadzenie, przetwarzanie i wymienianie danych pomiędzy przedmiotami za pośrednictwem sieci komputerowej.

Zjawisko rewolucji cyfrowej rozpatrywane jest więc zarówno w aspekcie społecznym, jak również edukacyjnym i ekonomicznym, a od zrównoważonego rozwoju społeczeństwa informacyjnego uzależnia się wręcz koniunkturę światowej gospodarki. Kompleksowe i uważne podejście do synergizacji technologii z innymi sferami życia oraz rozwijanie kompetencji cyfrowych w oparciu o solidne podstawy edukacyjne może

2 Badanie *Nastolatki 3.0*, NASK, grudzień 2016.
3 Raport GUS: *Społeczeństwo informacyjne w Polsce w 2017 roku*, s. 4.
4 Badanie *Nastolatki 3.0*, ibidem, s. 5.

prowadzić do wyrównywania szans i poziomów życia w społeczeństwie. Wychodząc z tych założeń, za niezwykle ważne uznajemy więc świadome wprowadzanie technologii do życia dzieci – tak aby wzrastając w otoczeniu urządzeń cyfrowych, potrafiły wykorzystać je do zaspokajania swoich potrzeb rozwojowych i społecznych. Z rozwojem globalnej sieci związane są bowiem nie tylko szanse, ale również wyzwania dotyczące bezpieczeństwa użytkowników. Sieć dająca ogromną przestrzeń relacjom i wymianie informacji może także narazić użytkowników na wiele zagrożeń, związanych między innymi z utratą prywatności, narażeniem na niebezpieczne kontakty, szkodliwe treści – w tym również treści nawołujące do zachowań ryzykownych oraz rozpowszechniające fałszywe informacje (tzw. *fake news*). Zagrożenia związane z internetem obejmują również problematykę dysfunkcyjnego korzystania z sieci, i prowadzącego między innymi do uzależnienia od internetu. Nawet odpowiednio dobrane treści internetowe mogą mieć negatywny wpływ na rozwój dzieci, jeśli są wprowadzone do ich świata na wcześnie i zbyt intensywnie. Dziecko, którego doświadczenia poznawcze są ograniczane do urządzeń ekranowych, zastępujących kontakt z ludźmi, wspólną zabawę, odbieranie świata wszystkimi zmysłami, jest narażone nawet na zaburzenia w rozwoju struktur neuronowych w mózgu. Wyniki badań[5] są jednak alarmujące: ponad 40 proc. rocznych i dwuletnich dzieci w Polsce korzysta z tabletów lub smartfonów, a wśród nich niemal co trzecie korzysta z urządzeń mobilnych codziennie lub prawie codziennie. W kontekście zaleceń Światowej Organizacji Zdrowia, aby dzieciom w wieku poniżej dwóch lat nie udostępniać urządzeń ekranowych, wyraźnie widać, że cyfrowy świat pojawia się w życiu dzieci w sposób rewolucyjny i w procesie tym często brakuje świadomego zarządzania ze strony rodziców.

Przygotowany poradnik dotyczy nowego zjawiska w kontekście bezpieczeństwa dzieci w internecie, jakim są zabawki interaktywne podłączane do sieci i wykorzystujące „systemy uczące się". Problematykę tę można roboczo podzielić na dwa główne obszary:


5 *Korzystanie z urządzeń mobilnych przez małe dzieci w Polsce*, Millward Brown Poland dla FDN, 2015.

Podzbiór łączący te zagadnienia to obszar związany z prywatnością. Może ona być obiektem działań cyberprzestępców, którzy na bazie zapisanych w zabawkach danych mogą stworzyć fałszywą tożsamość i wykorzystywać ją do celów nielegalnych. Z drugiej strony, zabawki zapisując podejmowane z dzieckiem interakcje i udostępniając je rodzicom lub innym osobom korzystającym z aplikacji, odkrywają treść rozmów bądź zapis obrazu bez wiedzy bezpośrednich użytkowników, czyli dzieci bawiących się zabawką. Perspektywę związaną z wkraczaniem rodzica w sferę prywatności dziecka poruszył podczas konferencji Internet Governance Forum w 2016 roku światowy ekspert w tej dziedzinie John Carr. W swoim wystąpieniu wskazał na możliwy wpływ zabawek podłączonych na relacje w rodzinie poprzez wykorzystywanie zabawek jako substytutów realnego uczestnictwa w życiu dziecka. Problem ten podkreśla również profesor Sherry Turkle w książce *Alone together*[6].

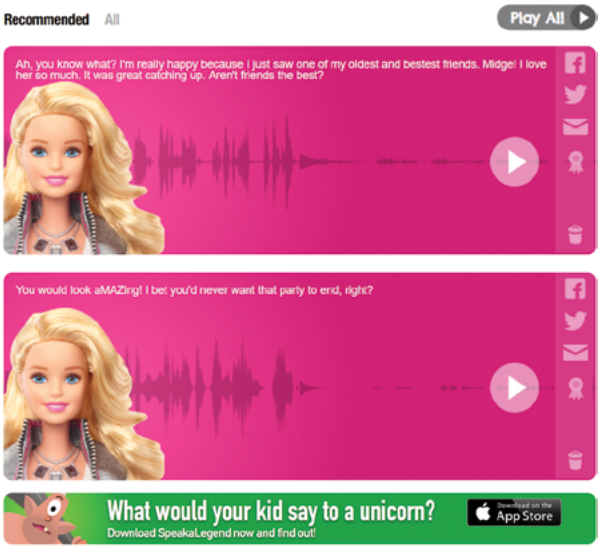
Przy okazji warto zwrócić uwagę na dodatkowy aspekt dotyczący prywatności dzieci, a związany z rozwojem internetu rzeczy – tzw. technologię ubieralną (*wearables*) – czyli ubrania oraz akcesoria zawierające w sobie komputer oraz zaawansowane technologie elektroniczne[7]. Wielu ekspertów uważa[8], że rozwiązania, które pozornie mają podnosić bezpieczeństwo dziecka mogą w konsekwencji ograniczyć prywatność dzieci i wolność osobistą, jednocześnie zachęcając je do akceptowania nadzoru. Z jednej strony naturalne jest, że rodzice chcą wykorzystać każdą możliwość aby chronić, swoje dzieci, ale zbyt rozwinięta inwigilacja, świadomość stałego monitoringu ze strony rodziców i nauczycieli może mieć bardzo duży wpływ na zachowanie i rozwój młodych ludzi.

**Pamiętajmy, że dzieci mają prawo do prywatności. Potrzebują prywatnych przestrzeni, aby móc bawić się i rozwijać bez odczuwania, że są stale obserwowane.**

zdj. Fotolia.com

6 Turkle Sherry, *Alone Together*, Basic Books 2011.
7 https://pl.wikipedia.org/wiki/Wearables.
8 https://www.theguardian.com/sustainable-business/2016/feb/05/big-mother-gps-tracking-technology-threat-privacy-childhood.

Bardzo ciekawą perspektywę dotyczącą prywatności w interakcji dzieci z inteligentnymi zabawkami oraz podejścia rodziców do możliwości odsłuchiwania i monitorowania rozmów dzieci dały badania pilotażowe przeprowadzone przez ekspertów z Uniwersytetu Waszyngtona „Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys". W ramach badań przeprowadzono osiem wywiadów z rodzicami i dziećmi (w wieku 6–10 lat), podczas których demonstrowano im działanie Hello Barbie i CogniToy Dino. Ciekawe były spostrzeżenia rodziców dotyczące sensowności nagrywania rozmów dzieci z zabawkami – zastanawiali się, do czego to może im służyć. Przychodziło im na myśl, że w ten sposób mogliby poznać jakieś problemy dziecka, o których nie chce powiedzieć bezpośrednio, wyłapać wyrazy, których nie chcą, żeby używało. Ale z drugiej strony, rodzice zaczynali wyobrażać sobie, jak czuliby się, gdyby ktoś ich nagrał bez ich wiedzy. Panel dla rodziców towarzyszący Hello Barbie daje nawet możliwość opublikowania nagranej rozmowy dziecka na portalu społecznościowym... I to wszystko w sytuacji, kiedy dzieci w większości wypadków kompletnie nie zdają




Rys. 1 Panel rodzica – po prawej stronie ikonki umożliwiające szybkie publikowanie w sieciach społecznościowych

sobie sprawy z nagrywania ich rozmów z cyfrowym przyjacielem. Większość dzieci biorących udział w wywiadach nie wiedziała, że rodzice mają dostęp do ich rozmów z Barbie, jedno z nich, kiedy dowiedziało się, że lalka zapamiętuje rozmowy, przestraszyło się. Jedną z rekomendacji płynących z tych badań była propozycja, żeby dzieci mogły z poziomu zabawki odsłuchać swoje nagrania. Wszyscy byli zgodni, że producenci i rodzice muszą poinformować dziecko o wszystkich funkcjonalnościach zabawek.

Aspekty związane z problematyką społeczną dotyczą między innymi wpływu, jaki zabawki inteligentne mogą mieć na umiejętność budowania przez dzieci autentycznych relacji międzyludzkich opartych między innymi na empatii, wrażliwości, responsywności, uważności, samopoznaniu, wzajemności, zainteresowaniu[9] oraz na rozwój poznawczy dzieci. Niezwykle ciekawą perspektywę do tych rozważań wniosły badania[10] oparte na eksperymencie, w którym wzięło udział dziewięćdziesięcioro dzieci w wieku 9–12 oraz 15 lat. W badaniu wykorzystany był japoński robot Robovie. Większość dzieci biorących udział w eksperymencie uznawała robota za byt społeczny, z którym można się zaprzyjaźnić, powierzyć mu sekrety, który ma własną inteligencję. 33 proc. dzieci dałoby mu prawa wyborcze, a 54 proc.uznało, że to nie w porządku zamykać robota w pudełku, jeśli on tego nie chce. Dzieci w wieku 9–12 wykazywały dużo wyższą tendencję personalizacji robotów niż piętnastolatkowie.

Badania wskazały na silną tendencję budowania przez dzieci relacji emocjonalnej z inteligentnymi urządzeniami i obdarzania ich dużym zaufaniem. Stąd tak wielkie zagrożenie, że dziecko może potencjalnie wejść w interakcję z kimś, kto przejmie urządzenie, wykorzystując tak powszechne rozwiązania jak choćby Bluetooth, że do osób niepożądanych trafią sekrety, które dziecko dzieli z cyfrowym przyjacielem, bądź że będzie narażone na działanie ukrytych reklam zaimplementowanych w urządzeniu (np. lalka Cayla nawiązuje w interakcji z dzieckiem do znanych na rynku przekąsek i słodyczy). Dlatego bardzo istotna jest uważność ze strony rodziców we wprowadzaniu zabawek smart do świata dziecka, dbanie o równowagę w jego aktywnościach społecznych oraz ochrona dziecięcej prywatności.

9 Budwig N., Turiel E., Zelazo P. D., *New Perspectives on Human Development*, Cambridge University Press, 2017.
10 Ibid, Kahn Peter H., Jr, Shen S., *NOC, NOC, who's there? A new ontological category (NOC) for social robots*, rodział 7, s. 106 – 123.

**Najważniejsza równowaga**

zdj. Fotolia.com

**Potencjalne konsekwencje dla rozwoju poznawczego[11]:**

☞ wspieranie uczenia się:
- wiedza spersonalizowana dla dziecka
- nieustannie aktualizowana przez samouczącą się nauczycielkę/nauczyciela

ale

☞ ryzyko bańki edukacyjnej:
- fragmentacja wiedzy, zagubienie w obfitości, uczenie się algorytmiczne
- ryzyko działań ukrytego marketingu na dziecko

**Potencjalne konsekwencje dla rozwoju tożsamości:**

- wpływ na postrzeganie relacji w kontakcie ludzko-ludzkim, przy kontekście człowiek – robot (Shanyang 2006)[12]
- rozszerzenie siebie: zabawki inteligentne jako nowa kategoria ontologiczna (Kahn i in. 2013)
- zmiany w postrzeganiu prywatności
- roboty/zabawki inteligentne jako urządzenia nadzorujące

**Potencjalne konsekwencje dla rozwoju relacji:**

**rekompensata za niezadowalające relacje w świecie rzeczywistym (np. Kahn i in. 2013),**
**funkcjonalna dywersyfikacja relacji,**
**nauczanie dziecka relacji w zależności mistrz-sługa (np. Kahn i in. 2013),**
**utrata autentyczności relacji (Turkle 2007).**

11 Amsterdam School of Communication Research/AscorR.
12 Shanyang Zhao, *Humanoid social robots as a medium of communication*, „New Media & Society", 2006.

# 3. O internecie rzeczy

Tak zwany internet rzeczy (*Internet of Things*) to pewien koncept, polegający na wyposażaniu przedmiotów w mechanizmy umożliwiające komunikację z innymi przedmiotami bądź systemami. Pozwala to na zdalne zbieranie danych z takich urządzeń, a często także na kontrolę nad nimi w ograniczonym lub pełnym zakresie.

Definicja ta jest bardzo ogólna, co wprowadza przynajmniej kilka problemów w posługiwaniu się nią i w konsekwencji w każdej dyskusji nad tym zjawiskiem. Przede wszystkim, spektrum „przedmiotów" włączanych w internet rzeczy jest bardzo szerokie. Z jednej strony mamy mechanizmy stosowane w systemach przemysłowych: roboty, inteligentne mierniki czy przełączniki. Na drugim biegunie – gadżety i urządzenia dla indywidualnych konsumentów: zegarki, telewizory, pralki czy wreszcie zabawki.

zdj. Fotolia.com

Elementami internetu rzeczy stają się także pojazdy (łączone w systemy zarządzania flotą), sygnalizacje świetlne, budynki i ich poszczególne podsystemy, jak alarmy czy klimatyzacja… Każda z tych grup urządzeń jest zupełnie inna. Dla systemów przemysłowych priorytetem będzie niezakłócone działanie – awaria bloku elektrowni czy oczyszczalni ścieków może mieć przecież poważne konsekwencje. Dla producentów telewizorów czy zabawek istotniejsza będzie możliwość szybkiego wprowadzenia na rynek nowych funkcji, wzbudzających zainteresowanie kupujących i pozwalających budować przewagę nad konkurencją.

Bardzo różnorodne są także rozwiązania technologiczne stosowane przez producentów inteligentnych urządzeń – od architektur i platform sprzętowych, przez systemy operacyjne, po protokoły komunikacji radiowej i sposoby przechowywania oraz transmisji danych. Dla przykładu, wiele rozwiązań konsumenckich wykorzystuje do wstępnej konfiguracji – najczęściej z użyciem smartfonu – Bluetooth Low Energy, WiFi Direct lub NFC, a przy normalnym działaniu „tradycyjne" WiFi.

Wreszcie, granica internetu rzeczy jest raczej umowna i płynna. Dobrym przykładem są tu smartfony. W zasadzie należałoby je zaliczyć do grupy urządzeń IoT (jako *nomen omen* „inteligentne telefony"). Z drugiej strony, są to rozwiązania na tyle dojrzałe i wyposażone w tak dużą moc obliczeniową, że nauczyliśmy się je traktować jako nową klasę przenośnych komputerów, w których korzystanie z sieci GSM do rozmów głosowych i wysyłania wiadomości jest jedynie jedną z funkcji.

W konsekwencji traktowanie internetu rzeczy jako całości ma bardzo ograniczone zastosowanie, w szczególności jeśli mówimy o jego problemach technicznych. Mimo to poniżej pokusiliśmy się o zestawienie najważniejszych klas problemów wspólnych dla urządzeń inteligentnych podłączanych do sieci.

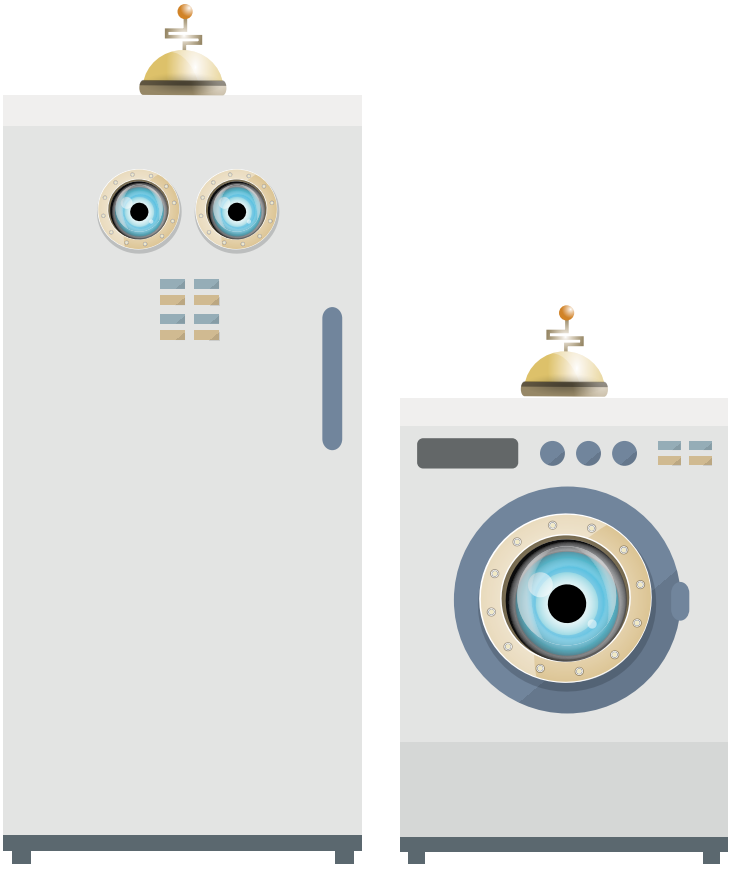
***Ograniczone zasoby przy produkcji*** – przy projektowaniu urządzeń IoT koniecznością jest zazwyczaj zadbanie o ich niewielkie rozmiary i energooszczędność. Może to skutkować kompromisem pomiędzy bezpieczeństwem (np. stosowaniem kosztownych obliczeniowo silnych algorytmów kryptograficznych) a implementacją dodatkowych funkcji. Z punktu widzenia producenta istotnym zasobem jest także czas – opóźnienie wprowadzenia nowego modelu produktu może wiązać się z utratą części rynku. Pokusą może być więc ograniczenie testów, w tym pod kątem bezpieczeństwa.

***Wykorzystywanie gotowych komponentów*** – elementy takie jak karty sieciowe, moduły BLE, kamery itd. są często wykorzystywane w wielu podobnych urządzeniach różnych producentów. Podobnie jest z bibliotekami programistycznymi łączonymi z oprogramowaniem urządzeń. W przypadku niektórych tanich urządzeń inteligentnych produkty różnych marek potrafią różnić się w zasadzie wyłącznie obudową i elementami wizualnymi interfejsu użytkownika. Co za tym idzie, znalezienie podatności w jednym z typowych elementów ma konsekwencje dla wielu produktów.

***Konieczność aktualizacji oprogramowania*** – naprawienie każdego błędu w oprogramowaniu urządzenia wiąże się z koniecznością wydania jego nowszej wersji przez producenta, a następnie pobrania jej i zainstalowania na urządzeniu. Producent – jeśli w ogóle przewidział możliwość aktualizacji – może zaproponować automatyczny lub ręczny proces aktualizacji. Przy drugim rozwiązaniu użytkownik musi samodzielnie sprawdzać dostępność poprawek oraz zadbać o ich instalację. W każdym przypadku producent stoi przed wyzwaniem zapewnienia mechanizmu bezpiecznego dostarczenia poprawki – tak,

by użytkownik mógł zweryfikować, że pochodzi ona z zaufanego źródła i nie została zmodyfikowana. Nie mniej istotnym problemem jest to, że dostępność ewentualnych aktualizacji oprogramowania po zakupie produktu jest uzależniona od tego, jak długo producent będzie ten produkt wspierał. Jeśli uzna on wsparcie za nieopłacalne, może się okazać, że zostaliśmy z produktem, który nigdy nie zostanie naprawiony.

Warto zauważyć, że problemy te dotyczą w zasadzie wszystkich urządzeń „inteligentnych" – niezależnie od tego, czy są one podłączane do sieci (a więc są elementem IoT), czy nie.



zdj. Fotolia.com

# 4. Postrzeganie i rozpowszechnienie w Polsce urządzeń typu smart – badania ilościowe i jakościowe

Do 2020 roku na świecie ma funkcjonować blisko 25 miliardów urządzeń należących do internetu rzeczy[13], a do 2025 roku, zdaniem ekspertów, ponad 70 proc. gospodarstw domowych na świecie będzie wyposażone w urządzenia typu smart[14]. Internet rzeczy definiowany jako kolejny etap cyfrowej rewolucji informacyjnej wkracza w każdą dziedzinę życia codziennego i przemysłu.

zdj. Fotolia.com

**O internecie rzeczy mówimy w kontekście m.in. inteligentnej gospodarki, inteligentnego miasta, inteligentnego transportu, inteligentnego zdrowia czy też inteligentnego domu.**

Ta dynamicznie rozwijająca się gałąź technologii jest również coraz powszechniejsza w Polsce. Chcąc określić aktualne rozpowszechnienie inteligentnych urządzeń w polskich gospodarstwach domowych – ze szczególnym uwzględnieniem rozpowszechnienia i wiedzy na temat internetu zabawek – przeprowadzono w połowie 2017 roku badania ilościowe oraz badania jakościowe, które pozwoliły stworzyć pełniejszy obraz tego, jak postrzegana jest technologia IoT i w jakich miejscach występuje.

13 https://www.gartner.com/newsroom/id/2905717.
14 https://www.forbes.com/sites/forbestechcouncil/2017/06/06/best-smart-home-devices-and-how-iot-is-changing-the-way-we-live/#578e929b43bd.

## BADANIA ILOŚCIOWE

**Badanie przeprowadzone na panelu Ariadna na ogólnopolskiej próbie polskich internautów liczącej N=1051 osób. Kwoty dobrane wg reprezentacji w populacji w wieku 18 lat i więcej dla płci, wieku i wielkości miejscowości. Termin realizacji: 8 – 11 września 2017 roku Metoda: CAWI;**

**oraz**

**Badanie przeprowadzone na panelu Ariadna na ogólnopolskiej próbie internautów liczącej N=1047 osób. Kwoty dobrane wg reprezentacji w populacji w wieku 18 lat i więcej dla płci, wieku i wielkości miejscowości. Termin realizacji: 15 – 18 września 2017 roku Metoda: CAWI.**

## BADANIA JAKOŚCIOWE

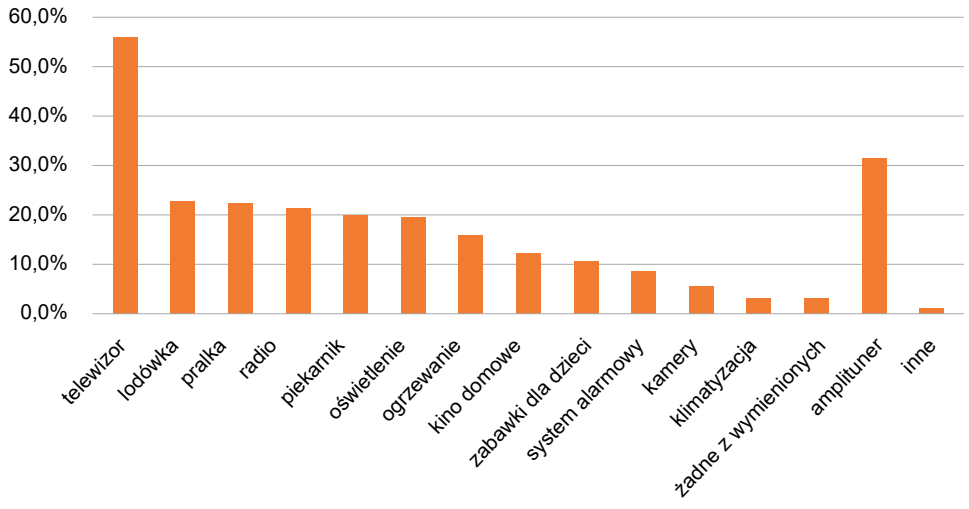
**Badania przeprowadzone metodą wywiadu pogłębionego (IDI) w okresie od lipca do września 2017 roku. Rozmowy odbywały się w miejscach zamieszkania respondentów lub ich czasowego pobytu. Było to szczególnie ważne dla umożliwienia przeprowadzenia badań obserwujących, skonfrontowania otrzymywanych informacji z sytuacją towarzyszącą rozmowie, wzięcia pod uwagę informacji dotyczących rozpowszechnienia i wykorzystywania urządzeń elektronicznych w urządzeniu mieszkania, występowania urządzeń w zasięgu wzroku podczas rozmowy etc. Przeprowadzono 24 wywiady z rodzinami wybranymi według wytycznych matrycy zakładającej zróżnicowanie wedle miejsca zamieszkania, wykształcenia, liczby dzieci oraz liczby opiekunów w rodzinie (oboje rodzice/samotny rodzic).**

## Czy moja lodówka jest smart?

Badania ilościowe przeprowadzone były dwukrotnie. Pierwsze badanie wykazało duży problem ze zdefiniowaniem przez respondentów urządzeń należących do internetu rzeczy. Wydaje się, że kampanie marketingowe oraz retoryka opisująca urządzenia jako „inteligentne", mając na uwadze jedynie bardziej rozbudowane funkcje (np. nowe funkcje urządzeń AGD), sprawiają, że posiadacze tego typu produktów uważają, że są to przedmioty należące do internetu rzeczy.

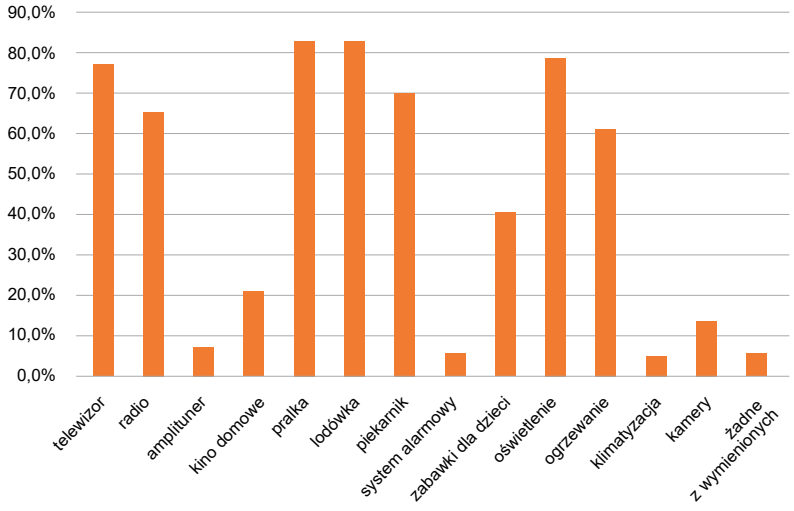
Przykładem tego jest poniższy wykres prezentujący odpowiedzi na pierwsze pytanie zadane w pierwszej edycji badań.

Które z poniższych urządzeń znajduje się w Twoim gospodarstwie domowym i ma połączenie z internetem lub może być podłączone do internetu, czyli jest urządzeniem typu smart?

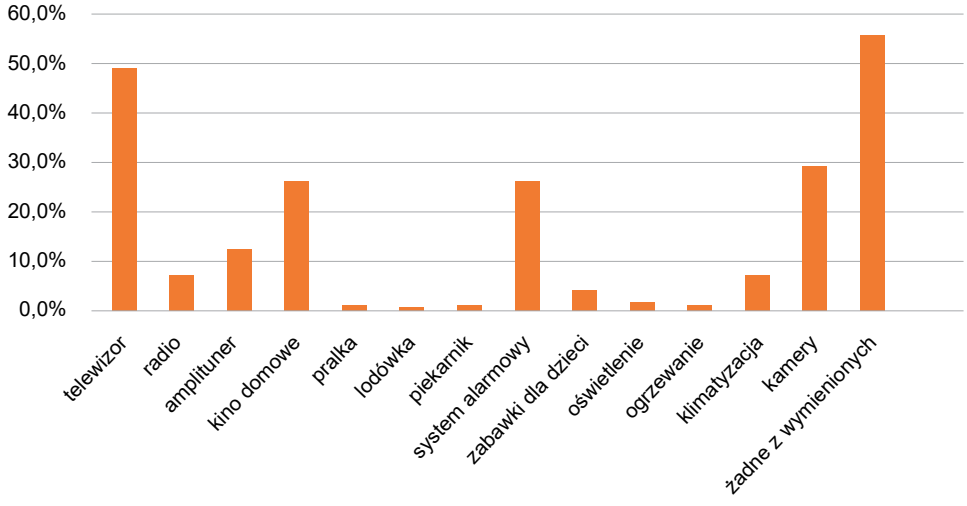


Uzyskane odpowiedzi i wysokie wskaźniki posiadania urządzeń typu smart wymogły powtórne badanie, w którym dokonano podziału pierwszego pytania na dwa uzupełniające się.

Które z poniższych urządzeń znajduje się w Twoim gospodarstwie domowym?




Które z tych urządzeń w Twoim gospodarstwie domowym są podłączone do internetu?



Jak można zaobserwować, po zadaniu pytania odnoszącego się bezpośrednio do podłączenia urządzenia do internetu, uzyskane zostały dane wskazujące na dużo niższe rozpowszechnienie urządzeń IoT w gospodarstwach domowych, niż wynikało to z pierwszego panelu. Analizując te dane, trzeba jednak mieć na uwadze również ewentualność, którą zasygnalizowały badania jakościowe, że występuje też sytuacja, w której respondenci posiadają urządzenie typu smart (głównie smart tv), ale nie podłączają go do internetu, wykorzystując jedynie jako tradycyjny telewizor. W kilku przypadkach na ścianie w mieszkaniu rozmówców wisiał najnowocześniejszy model telewizora typu smart, niepodłączony do sieci.

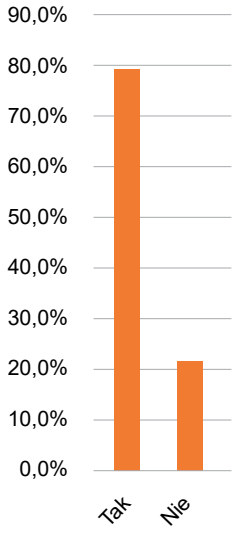
Badanie sprawdzające rozpowszechnienieurządzeń IoT wykazało ponadto, że najczęstszymi posiadaczamismart tv (najpowszechniejszegow polskich domach urządzenia smart)są osoby w grupie wiekowej 45–55 lat, zamieszkujące małe i średniemiasta. Mieszkańcy średniej wielkościmiast (20–99 tys. mieszkańców), w wieku 25–44 lat, są również najczęstszymi posiadaczami inteligentnych systemów alarmowych. Zabawki inteligentne są na razie rzadkością, a ich posiadacze to najczęściej osoby z wyższym wykształceniem, w wieku 35–45 lat, zamieszkujące duże miasta.

Wywiady z rodzinami potwierdziły fakt, że bardzo często osoby mające urządzenie smart nie mają świadomości, co to oznacza. Nie widać również korelacji wynikającej z posiadania jakiegoś urządzenia smart z wiedzą o innych urządzeniach z dziedziny IoT.

## Kto kupuje i kto decyduje

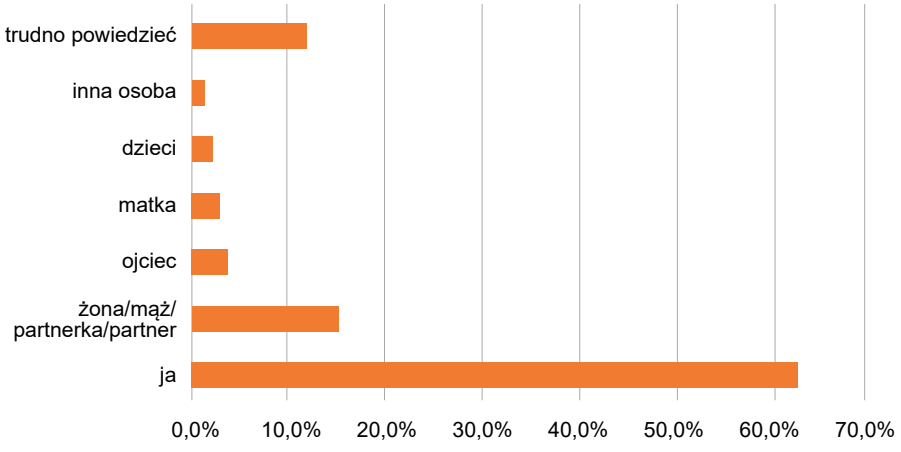
Zabawki są zakupem dokonywanym przez praktycznie wszystkie grupy społeczne, w każdym wieku. Kupowanie zabawek zadeklarowało prawie 80 proc. respondentów, z czego ponad 95 proc. osób w wieku 25–34 lat.

Czy kupujesz swoim dzieciom zabawki?

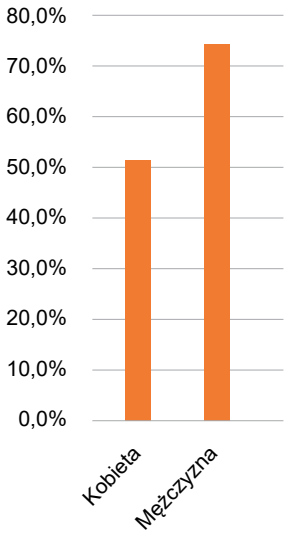


Nieco częściej zabawki kupują kobiety (80,3 proc.) w stosunku do mężczyzn (76,4 proc.), jednakże może to zmienić się w odniesieniu do zabawek cyfrowych, ponieważ mężczyźni o wiele częściej uważają swój głos za decydujący podczas kupowania urządzeń elektronicznych. Badania ilościowe potwierdzają obserwacje płynące z badań jakościowych. W większości przypadków jako osoba decydująca o zakupie urządzeń cyfrowych wskazywany jest ojciec. Jego doradcy i motywatorzy to w większości przypadków dzieci. Kobiety wskazują na siebie jako na osoby decydujące tylko w przypadku wywiadów z samotnymi matkami. Pojawiają się też sytuacje sporne – rodzice nie zgadzają się co do poczucia decyzyjności – ostatecznym argumentem w dyskusji jest wówczas informacja, kto był płatnikiem.

Kto w Twoim gospodarstwie domowym ma decydujący głos przy zakupie urządzeń elektronicznych?



Ja decyduję.

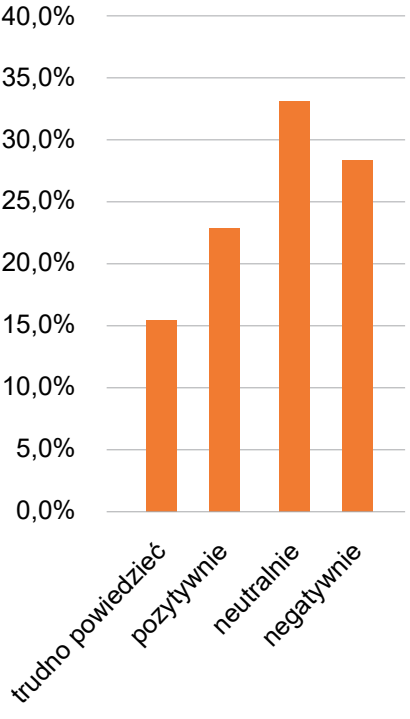



78 proc. mężczyzn twierdzi, że to oni podejmują decyzję o zakupie sprzętu elektronicznego, o sobie myśli tak 54,7 proc. kobiet (mężczyźni tylko w 5,4 proc. stwierdzili, że decyduje żona/partnerka).

Zadaniem badania było też sprawdzenie, jak postrzegany jest rozwój rynku zabawek inteligentnych. Najbardziej pozytywnie do rozwoju IoT nastawiona jest społeczność dużych miast – 10 proc. więcej odpowiedzi „pozytywnie" niż średnia odpowiedź na pytanie: Jak oceniasz fakt, że coraz więcej zabawek ma możliwość podłączenia do internetu? Procentowo przeważa podejście neutralne i pozytywne, chociaż prawie 30 proc. wyraża dużo obaw.

## Jak oceniamy rozwój technologii IoT w kontekście dzieci

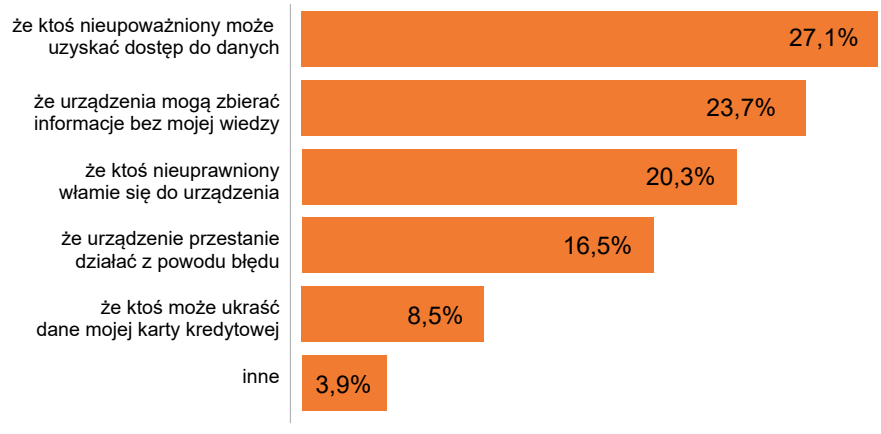
Jak oceniasz fakt, że coraz więcej zabawek dla dzieci ma możliwość podłączenia do internetu i zdalnego zarządzania przez aplikacje na smartfonie, tablecie lub komputerze?



Na poniższym wykresie widać, że najbardziej boimy się niedozwolonego dostępu do naszych danych. Co ciekawe, najmniejsze ryzyko respondenci wiązali z bezpośrednią utratą pieniędzy, np. z przejęciem konta bądź danych do karty.

Badania jakościowe również zasygnalizowały raczej neutralne podejście do rozwoju technologii internetowych w kontekście zabawek, natomiast prawie wszystkim wypowiedziom towarzyszyły pewne wątpliwości. Najczęściej rodzice zwracali uwagę na problematykę ochrony prywatności dziecka, ryzyko dostępu do danych osobowych, obawiali się, że zabawka może dostarczać dziecku fałszywych emocji oraz że dziecko może być narażone na niebezpieczne kontakty. Osoby nastawione pozytywnie do zabawek smart mają nadzieję, że wpłyną one korzystnie na rozwój dziecka, zwłaszcza w kontekście edukacyjnym oraz wyrażają przekonanie, że to naturalna konsekwencja cyfrowej rewolucji. Tym niemniej również mają obawy, głównie dotyczące ryzyka nadużywania przez dzieci urządzeń cyfrowych oraz internetu jako „zabijacza czasu" dla młodych ludzi. Ocena negatywna zabawek smart wiązała się głównie z obawami o inwigilację, utratę prywatności oraz zabijanie kreatywności u dzieci. Zarówno w badaniach jakościowych, jak i w ilościowych widać, że obawy o straty finansowe, czyli potencjalne przechwycenie danych kont, loginów, haseł, nie jest wymieniane jako główne ryzyko kojarzone z urządzeniami IoT.

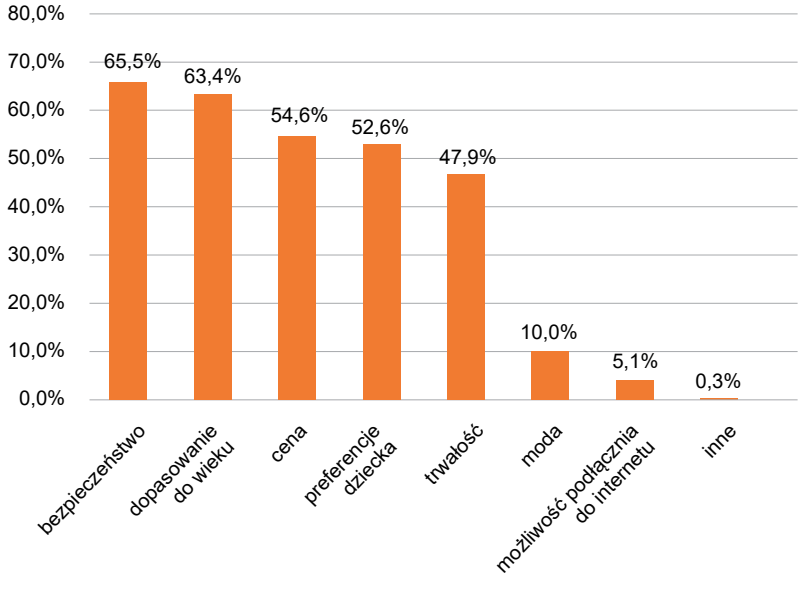
Co najbardziej Cię niepokoi w urządzeniach podłączonych do internetu?



Celem badania było również określenie, jakie cechy są najważniejsze dla rodziców przy wyborze zabawki. Pytanie dawało możliwość wielokrotnego wyboru. Jak widać na wykresie, dla większości ankietowanych (65,5 proc.) najważniejsze jest bezpieczeństwo oraz dopasowanie do wieku (63,4 proc.). Na kolejnych miejscach plasowane są cena oraz preferencje dziecka. Prawie 50 proc. badanych kieruje się przy zakupie również trwałością – warto więc w kontekście inteligentnych zabawek zwracać uwagę na ten aspekt, ponieważ producenci nie zawsze gwarantują dłuższy czas funkcjonowania zabawki.

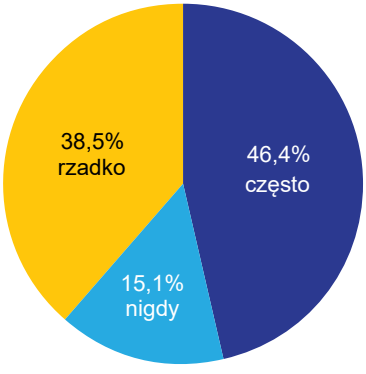
Powstaje pytanie, na ile uważność dotycząca bezpieczeństwa obejmuje też fizycznye aspekty zabawek – ryzyko połknięcia przez małe dzieci, brak odpowiednich atestów, a na ile będzie koncentrowała się na kwestiach związanych z bezpieczeństwem internetowym. Bazując bowiem na odpowiedziach na pytanie odnośnie do częstotliwości prowadzenia z dzieckiem rozmów o bezpie-

Jakie cechy zabawki są dla Ciebie najważniejsze podczas podejmowania decyzji o ich zakupie?



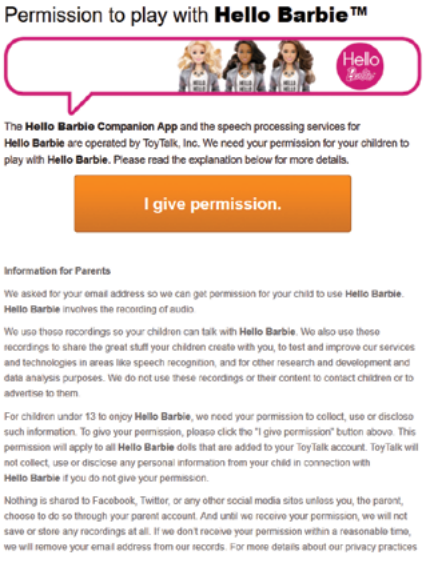
czeństwie w sieci, można stwierdzić, że tematyka ta jest wciąż w wielu domach nieobecna (15,1 proc.) bądź rzadka (38,5 proc.). Częste rozmowy z dziećmi na temat bezpieczeństwa online liczniej deklarują kobiety (51,3 proc.) w stosunku do mężczyzn (39,1 proc.) natomiast one znacznie rzadziej decydują oraz inicjują zakup urządzeń cyfrowych. Rodzice podczas wywiadów bardzo często tłumaczyli fakt nieprowadzenia z dziećmi rozmów o bezpieczeństwie w sieci przekonaniem, że dzieci wiedzą więcej, że rodzice nie nadążają za technologią. Przyznawali też, że nie potrafią takich rozmów prowadzić, że trzeba znać tematykę i dopasować zakres rozmowy do wieku dzieci, ale jednocześnie większość rozmówców właśnie rodziców widziała jako tych, którzy bardziej niż szkoła powinni odpowiadać za edukację i ochronę dziecka przed zagrożeniami online. Wydaje się bardzo ciekawe, że im respondent mniej wiedział na temat technologii i cyfrowych aktywności dzieci, tym większą widział swoją odpowiedzialność i rolę, natomiast osoby będące dobrze zaznajomione ze światem cyfrowym i same będące aktywnymi użytkownikami sieci wskazywały na szkołę jako tę, która powinna wieść prym w kształtowaniu kompetencji cyfrowych, tłumacząc, że widzą po sobie, iż rodzice często nie nadążają za technologią. Trochę wedle słynnej maksymy „wiem, że nic nie wiem" – im bardziej poznajemy tajniki internetu, tym większą mamy świadomość potencjalnych wyzwań towarzyszących poznawaniu wirtualnego świata.

Jak często rozmawiasz ze swoim dzieckiem lub dziećmi na temat bezpieczeństwa korzystania z internetu oraz zagrożeń z nim związanych?




Alarmującą prawidłowością, która dała się zaobserwować podczas rozmów z rodzinami, jest fakt całkowitego pomijania regulaminów dotyczących urządzeń, które kupujemy. Większość respondentów zgodnie odpowiadała, że kupując urządzenia cyfrowe, ściągając aplikacje, korzystając portali społecznościowych bądź z innych serwisów internetowych, nie zapoznaje się z ich regulaminami ani z polityką prywatności. Czytanie regulaminów potwierdzamy tylko w przypadkach, kiedy mamy obawę bądź świadomość, że z daną usługą online mogą się wiązać jakieś

płatności, a i to nie jest regułą. Dlatego też wszyscy rodzice wyrażali potrzebę jak najwyraźniejszego informowania o wszystkich funkcjonalnościach oraz polityce prywatności zabawek smart już na samych opakowaniach albo wręcz na samej zabawce. Przy okazji warto wspomnieć, że dane te potwierdzają wnioski z cytowanych wcześniej badań przeprowadzonych przez Uniwersytet Waszyngtona – wszyscy rodzice, którzy brali udział w wywiadach, na panelu rodziców towarzyszącym lalce Hello Barbie naciskali ikonkę zgody na używanie lalki przez dziecko bez chwili zastanowienia i bez zapoznania się z polityką prywatności.




Rys. 2 Zgoda rodziców na zabawę dziecka z Hello Barbie

Respondenci chcieliby, aby producenci czuli się odpowiedzialni za odpowiednie informowanie potencjalnych klientów i ochronę ich danych potrzebnych do funkcjonowania urządzeń. Rodzice też bardzo cenią sobie wszystkie wydawnictwa poradnikowe, które mogłyby im pomóc zadbać o bezpieczeństwo dzieci w świecie mediów cyfrowych.

Wyniki badań wyraźnie wskazują na potrzebę działań informacyjnych dotyczących specyfiki, funkcjonowania oraz wyzwań związanych z rozwojem internetu rzeczy. Zadaniem niniejszego poradnika jest więc przede wszystkim przybliżenie kwestii technologicznych inteligentnych urządzeń cyfrowych, zaprezentowanie potencjalnych zagrożeń wynikających ze specyfiki zabawek smart bazujących na infrastrukturze internetu oraz dotarcie do rodziców i opiekunów z poradami odnośnie do świadomego wprowadzania technologii IoT w życie dziecka, począwszy od dokonywania przemyślanego zakupu, a później konsekwentnego dbania o bezpieczeństwo dziecka w kontekście ochrony jego prywatności oraz rozwoju społecznego.

# 5. Inteligentne zabawki pod lupą – testy i analiza problematyki

Tak jak zaznaczyliśmy wcześniej, w niniejszym poradniku skupiamy się przede wszystkim na inteligentnych zabawkach łączących się z internetem (*smart connected*). Połączenie to oznacza zazwyczaj pewien rodzaj interakcji z usługami dostępnymi na serwerach producenta bądź współpracującej z nim firmy trzeciej. W przypadku każdej zabawki szczegóły tej interakcji mogą wyglądać zupełnie inaczej. Zazwyczaj jednak większość zebranych z otoczenia informacji przesyłana jest do obróbki na serwer w stanie surowym. Dzięki temu, że analiza odbywa się poza urządzeniem, sama zabawka nie potrzebuje dużej mocy obliczeniowej. Jak jednak łatwo się zorientować, ten model może potencjalnie zagrażać naszej prywatności.

Aby sprawdzić w praktyce, jak wygląda bezpieczeństwo korzystania z takich zabawek, wcieliliśmy się w rolę konsumentów i kupiliśmy do testu cztery zabawki z kategorii *smart connected*.

**Hello Barbie** – Lalka reklamowana jako wyposażona w możliwość interaktywnej rozmowy i rozpoznawanie głosu. Wyposażona jest w mikrofon, z którego wypowiedzi dziecka wysyła do serwera w chmurze. Aplikacja serwera stara się rozpoznać słowa kluczowe typu „tak”, „nie”, tematy rozmowy i „odpowiada” jedną z kilku tysięcy zadanych formułek. Polecana jest dla dzieci w wieku 6–15 lat.


Rys. 3 Hello Barbie

**Barbie Hello Dreamhouse** – Inteligentny domek dla lalek. Wykorzystuje mechanizmy podobne jak Hello Barbie, aby polecenia głosowe zamieniać na aktywowanie różnych funkcji (np. włączanie muzyki, zapalanie światła). Zabawka polecana przez producenta dla dzieci w wieku od 3 do 10 lat.

Rys. 4 Barbie Hello Dreamhouse

**Fisher Price Smart Toy Monkey** – wykorzystuje mikrofon, kamerę i akcelerometr do interaktywnej zabawy, reagując na słowa kluczowe, karty aktywności (rozpoznawane przez kamerę) czy aktywność ruchową (np. podrzucenie). Polecany przez producenta dla dzieci w wieku od 3 do 8 lat.



Rys 5. FisherPrice Smart Toy Monkey

**Dinozaur CogniToys** – przesyła do serwera zapis głosu użytkownika, aplikacja serwera w chmurze zasilana jest bazą wiedzy i systemem IBM Watson, który generuje odpowiedzi w formie naturalnej konwersacji, podając dane encyklopedyczne, opowiadając dowcipy, śpiewając itd. Polecany dla dzieci powyżej 5 roku życia.


Rys. 6 Dinozaur CogniToys

Zanim w szczegółach omówimy możliwe problemy, przybliżmy sposób działania zabawek *smart connected*. Dla wszystkich zabawek, które testowaliśmy, daje się rozróżnić kilka etapów, istotnych z punktu widzenia zrozumienia istoty ich działania.

1. **Rejestracja** w serwisie producenta/dostawcy usług – przed rozpoczęciem korzystania z zabawki jesteśmy zwykle proszeni o założenie profilu użytkownika. Zakres danych podawanych na tym etapie bywa różny – jest to co najmniej adres e-mail, ale możemy być także proszeni np. o imię i wiek dziecka. Dane profilu zapisane są na serwerze producenta.

2. **Konfiguracja** urządzenia odbywa się zwykle za pomocą smartfonu. Podczas tego procesu będziemy musieli podać co najmniej dane sieci bezprzewodowej (nazwa i hasło), które będą wykorzystywane przez zabawkę do nawiązywania połączenia w przyszłości. Informacje te zapisane zostają w pamięci zabawki, choć może się zdarzyć, że będą później wysyłane do producenta (co najmniej jedna z badanych przez nas zabawek przesyłała

na zewnątrz nazwę sieci bezprzewodowej, z której korzystała). Konkretna zabawka zostaje w ten sposób powiązana z profilem użytkownika.

3. **Zabawa** odbywa się po każdorazowym włączeniu zabawki w cyklu:
**zbieranie danych** od użytkownika – zabawka rejestruje dźwięk, obraz lub np. wskazania akcelerometru i przesyła je do serwera (czasami wstępnie obrobione);
**przetworzenie** danych na serwerze – w zależności od zabawki może być przeprowadzana np. analiza symbolu graficznego bądź pełne rozpoznawanie mowy. Oprogramowanie na serwerze generuje informację zwrotną (np. odpowiedź głosową, uruchomienie zaprogramowanego działania zabawki, wersję skryptu opowiadanej historyjki) i przesyła ją do zabawki. Tu jest więc zaszyta „inteligencja" zabawki;
**prezentacja wyniku** – odtworzenie odpowiedzi głosowej, muzyczki, wykonanie czynności itp.

zdj. Fotolia.com

## Kupujemy inteligentną zabawkę

Żadna z testowanych przez nas zabawek nie była dostępna na polskim rynku. Zakupów dokonaliśmy więc w amerykańskim sklepie internetowym. Co ważne, wszystkie zabawki do skonfigurowania wymagają aplikacji na smartfon, która także może być niedostępna dla polskich użytkowników. Na szczęście sprzedawca informuje o tym w czytelny sposób w opisie zabawki – poniżej ostatni wiersz dotyczący aplikacji towarzyszącej Hello Barbie.

- Chat with Barbie for a whole new way to play!
- Hello Barbie doll uses WiFi and speech recognition technology to engage in two-way dialogue
- Use is simple with functionality built into her belt buckle -- press to start the conversation and release to hear Hello Barbie doll respond
- Doll must be placed in charger for initial set-up. Refer to the product description before use.
- This is a US only product. The Hello Barbie companion app can only be found in US app stores.

Rys. 7 Fragment aplikacji Hello Barbie

Z opisów zabawek można dowiedzieć się, że są one interaktywne, inteligentne, a także że wymagają połączenia z internetem (a więc są *smart connected*). Nie jest jednak łatwo wywnioskować, na czym dokładnie polega ich „inteligencja", ani jakie dane są przez nie wykorzystywane. Niektóre z opisów odsyłają drobnym drukiem do polityki prywatności na stronie producenta. Kupujemy więc trochę kota w worku.

**Custom Conversation, Safe Play**

Parents and guardians are in control of their child's data and can manage this data through the ToyTalk account at anytime. For more information visit our official website or call our customer care.

Parents must also set up a ToyTalk account and connect to use the conversational features. Hello Barbie doll can remember up to three different WiFi locations and does not require a smart device after WiFi configuration. Hello Barbie doll is compatible with iPhone 5, iPhone 5c, iPhone 5s, iPhone 6 Plus, iPhone 6, iPad Air, iPad Air 2, iPad 4th generation, IPad mini 2, iPad mini 3; must have iOS 8 or above. Android mobile devices must have Android OS 4.0.3 or above. Use of Hello Barbie involves recording of voice data; see ToyTalk's privacy policy at our official website.

Rys. 8 Fragment dotyczący kwestii prywatności w zabawce Hello Barbie

Po rozpakowaniu paczek dochodzimy do wniosku, że mimo wszystko przy zakupach online byliśmy w lepszej sytuacji niż konsument, który chciałby się zdecydować na zakup po zobaczeniu zabawki w sklepie. Na opakowaniach nie ma prawie żadnych informacji o tym, jak dokładnie działa zabawka, nie mówiąc o szczegółach użytych rozwiązań technicznych.

Na jakie pytania warto naszym zdaniem szukać odpowiedzi przed dokonaniem zakupu?

- **Jak dokładnie działa zabawka?** Na to pytanie możemy poszukać odpowiedzi u sprzedawcy, prosząc o demonstrację. Możemy także poszukać opisów testów zabawki w internecie, filmów demonstracyjnych itp. Warto pamiętać, że opis „inteligentnej" zabawki i rozumienie niektórych terminów (np. „interaktywna rozmowa") może być inne u osób odpowiedzialnych za marketing produktu, a inne w naszych oczekiwaniach.
- **Jakie dane zbiera zabawka? Gdzie są przechowywane? Kto ma do nich dostęp?** Te informacje powinniśmy znaleźć w opisie polityki prywatności na stronie producenta. Na pudełku lub w instrukcji (często dostępnej do pobrania ze strony) może znajdować się dokładny odnośnik do dokumentu lub przynajmniej adres głównej strony producenta. W ostateczności, możemy poszukać na niej działu wsparcia technicznego i tam zapytać o te informacje.
- **Jak są chronione dane przesyłane pomiędzy zabawką a serwerem producenta?** W każdym przypadku powinniśmy oczekiwać, że dane te będą szyfrowane. Nie zawsze jednak tak się dzieje. Poza tym samo

szyfrowanie nie jest jeszcze gwarancją, że nikt nie może danych przechwycić. Niestety, na próżno szukać dokładnych informacji w jakiejkolwiek dokumentacji dostarczanej z zabawką. Warto skierować pytanie do działu wsparcia technicznego producenta, a także poszukać w internecie testów konkretnej zabawki. Być może ktoś pokazał już, że nie jest ona bezpieczna? A może wręcz przeciwnie?

- **W jaki sposób aktualizowane jest oprogramowanie?**
  Wszystkie testowane przez nas zabawki automatycznie poszukiwały aktualizacji po każdym włączeniu. Informacji o tym nie znaleźliśmy jednak w instrukcji. Warto więc pytać o to dział wsparcia technicznego przed zakupem.
- **Jak długo wspierany będzie produkt?**
  Producent może w dowolnym momencie przestać dostarczać aktualizacje, co oznacza, że ewentualne błędy nie zostaną naprawione. Co gorsza, sam serwer odpowiadający za „inteligencję" zabawki może zostać wyłączony, co sprawi, że stanie się ona niemal bezużyteczna. W przypadku jednej z zabawek informacja ta znajduje się w materiałach sprzedażowych. Łatwo jednak ją przeoczyć. Nie znaleźliśmy jej też na pudełku!

**Customize Barbie® Hello Dreamhouse™ with Your Own Sounds!**

Using the Barbie® Hello Dreamhouse™ Companion app, it's easy to change the sounds in each play space. Pick a sound for any of 15 locations throughout the house or record your own. To go back to the original sounds, it's as easy as saying "Use the original sounds." The Hello Dreamhouse™ Companion app has three main features. How-to videos guide parents through house assembly; the Wi-Fi Setup takes parents through the process for connecting Hello Dreamhouse™ to a Wi-Fi network for voice activation; and Customize Play allows kids to personalize their experience. The use of Hello Dreamhouse™ involves the recording of voice data. Parents are required to create a ToyTalk account and consent to use of Hello Dreamhouse™ by following the in-app instructions. We reserve the right to terminate the app and speech recognition services after 4/1/2019. This product is English speaking only. Product does not ship to the Province of Quebec.

Rys. 9 Informacja na temat aktualizacji zabawki

Jeśli uda się zebrać wszystkie, a przynajmniej satysfakcjonującą większość, odpowiedzi, należy na spokojnie zastanowić się, czy chcemy dokonać świadomego zakupu, biorąc pod uwagę wszelkie ryzyko.

## Mamy zabawkę

Niektóre zabawki w bardzo ograniczony sposób ujawniają dane użytkownika na zewnątrz. W ich przypadku możemy jedynie obawiać się, że ktoś mógł zmodyfikować oprogramowanie tak, by kamera, mikrofon czy czujnik ruchu rejestrowały więcej niż zakładał producent (czy zabawka pochodzi z drugiej ręki? Czy ufamy sprzedawcy?). Inne zabawki wysyłają do producenta kompletny zapis rozmów dziecka z lalką, a na serwerze oprócz nagrań przechowują także ich transkrypcje, które mogą być wykorzystywane do analiz maszynowych.

W takim scenariuszu wyjątkowo istotne jest odpowiednie szyfrowanie danych podczas transmisji, a także ochrona przed niepowołanym dostępem przez osoby trzecie. Innymi słowy, musimy mieć zaufanie do dostawcy treści i jego kompetencji technicznych.

zdj. Fotolia.com

Warto zwrócić uwagę, że wszystkie zabawki, z którymi mieliśmy do czynienia, są adresowane do klienta anglojęzycznego. Jest to bardzo istotne w szczególności w zakresie funkcji rozpoznawania mowy. W naszych testach algorytmy często nie radziły sobie poprawnie z tym zadaniem (nawet podczas „rozmowy" z *native speakerem*). Może to być tym większym powodem do frustracji u dziecka, którego wymowa jest siłą rzeczy mniej wyraźna, a język mniej poprawny.

Pierwszą czynnością, którą musieliśmy wykonać przed korzystaniem z każdej z zabawek było zainstalowanie i uruchomienie dedykowanej aplikacji na smartfonie. Przy pierwszym uruchomieniu konieczne jest założenie konta w serwisie producenta. Na tym etapie musimy zaakceptować warunki użytkowania zabawki, w tym politykę prywatności. Choć najczęściej tego rodzaju komunikaty pomijane są szybkim „Dalej", w tym przypadku zalecamy dokładne zapoznanie się z dokumentami. Opisują one, jakie dane są zbierane, a także komu i w jakim celu mogą być udostępniane. W skrajnych przypadkach producent deklarował chęć przekazywania wszelkich danych (w tym nagrań rozmów dziecka z zabawką) firmom trzecim niemal bez żadnych ograniczeń. W dalszej części poradnika można znaleźć obszerną analizę tego tematu.

Zainstalowana aplikacja służy do wstępnego skonfigurowania zabawki, w szczególności do ustawienia danych dostępowych do sieci bezprzewodowej oraz skojarzenia zabawki z kontem użytkownika. Do połączenia z zabawką wykorzystywany jest najczęściej protokół WiFi Direct bądź Bluetooth. W obu przypadkach połączenie odbywa się bez autoryzacji po stronie zabawki, nie wymaga też znajomości unikatowego PIN-u czy hasła. Zalecamy w związku z tym konfigurowanie zabawki i łączenie się z nią w miejscu, gdzie nie ma ryzyka przejęcia połączenia przez postronną osobę

o złych intencjach. Należy wspomnieć, że z aplikacji zmuszeni będziemy korzystać przy większości zabawek wyłącznie podczas zmiany ustawień (np. dodawania nowej sieci bezprzewodowej). Raz skonfigurowana zabawka będzie działać samodzielnie, o ile znajduje się w zasięgu sieci, która została zapamiętana.

Miejsce korzystania z zabawki ma znaczenie właśnie z powodu „pamiętanych" przez nią sieci bezprzewodowych. Zabawka podłączy się bowiem z każdą siecią WiFi, która będzie posiadała identyczną konfigurację (nazwa, protokół zabezpieczeń, hasło) – nawet jeśli jej dysponentem jest np. złośliwy sąsiad. Każda osoba kontrolująca urządzenie WiFi, z którym łączy się zabawka, może z kolei przejąć komunikację między nią i serwerem dostawcy, potencjalnie podsłuchując ją lub modyfikując. Analogiczne ryzyko występuje przy świadomym korzystaniu z publicznych sieci, gdy nie wiemy, kto nimi administruje lub czy nie zostały przejęte.

Aby chronić prywatność użytkownika oraz zagwarantować, że dane wymieniane są z właściwym serwerem, producenci mogą stosować kryptografię, choćby korzystając z popularnych protokołów SSL/TLS. Podczas testów sprawdziliśmy, czy tak jest w rzeczywistości. Większość zabawek zdała test bez zarzutu, nie tylko szyfrując ruch, ale także weryfikując, czy druga strona faktycznie należy do producenta i odmawiając komunikacji z podstawionym przez nas serwerem. Tak było również w przypadku lalki Hello Barbie, którą w 2013 roku ogłoszono podatną na taki rodzaj ataku. Oznacza to, że producenci najwyraźniej naprawili problem i dokonali odpowiedniej aktualizacji oprogramowania lalki. Niestety, w jednej z zabawek szyfrowanie okazało się bardzo słabe i dotyczyło wyłącznie części ruchu (rozmów głosowych), a nie całej komunikacji z serwerem. Możliwe było w szczególności zainstalowanie spreparowanej aktualizacji. Z drugiej strony, odpowiednio wykorzystywane i odpowiednio silne szyfrowanie sprawia, że nie ma możliwości sprawdzenia, jakie dane zbierane są przez zabawkę wyłącznie na podstawie analizy ruchu między nią i serwerem.

Wszystkie testowane przez nas zabawki posiadają mechanizm automatycznej aktualizacji. Po podłączeniu do sieci WiFi sprawdzają na serwerze producenta informacje o dostępności nowszej wersji oprogramowania i pobierają ją oraz instalują w razie potrzeby. Jak wspomnieliśmy wyżej, niezwykle ważne jest, aby odpowiednie mechanizmy kryptograficzne gwarantowały, że aktualizacja jest faktycznie programem zaufanym, pochodzącym z wiarygodnego źródła. Skutkiem zainstalowania zmodyfikowanego oprogramowania

może być w zasadzie dowolne wykorzystanie urządzeń peryferyjnych, w które wyposażona jest zabawka (a więc przede wszystkim mikrofonu czy kamery) i dowolne wykorzystanie zebranych przez nie danych.

Warto podkreślić, że wszystkie testowane przez nas zabawki zbierają dane wyłącznie w wyniku świadomej interakcji użytkownika (zwykle naciśnięcie konkretnego przycisku). To dobra wiadomość, ponieważ oznacza, że nie są cały czas „na nasłuchu" i nie wysyłają danych producentowi, gdy sobie tego nie życzymy lub w ogóle nie zdajemy sobie z tego sprawy.

Zadaliśmy sobie także pytanie, czy „inteligencję" zabawek można wykorzystać przeciwko dziecku, np. ucząc je agresywnych czy wulgarnych zachowań. W przypadku większości zabawek odpowiedź okazała się prosta ze względu na ich ograniczoną zdolność interakcji i brak możliwości wygenerowania komunikatów spoza z góry założonego zestawu skryptów (nawet jeśli, jak w przypadku Hello Barbie, skrypt zawiera ponad 8000 fraz). W przypadku CogniToys Dino potencjał wydawał się większy, ponieważ wykorzystuje on system IBM Watson i generuje odpowiedzi w oparciu o bardzo rozbudowaną (i prawdopodobnie stale poszerzaną) bazę wiedzy. Producent zadbał jednak o odpowiednie filtry treści, zarówno ograniczając dostęp do treści niepożądanych, jak i odpowiednio reagując na próby „niestosownego zachowania" testujących.

## Bezpieczeństwo fizyczne zabawki

Innym sposobem „zaatakowania" zabawki inteligentnej jest fizyczny dostęp do zaszytych w niej układów i próba odzyskania lub zmiany danych i oprogramowania. Wśród takich danych zapisanych w zabawce znajdują się zapamiętane nazwy i hasła do sieci WiFi czy dane konta użytkownika. Zmodyfikowane mogą być z kolei – poza oprogramowaniem – choćby komunikaty dźwiękowe dostępne bez połączenia z siecią (np. witające dziecko czy informujące o błędach).


zdj. Fotolia.com

„Inteligentne” zabawki są niczym innym jak urządzeniami elektronicznymi przystosowanymi do komunikowania się ze światem za pośrednictwem wbudowanych sensorów (np. mikrofonu, kamery), jak również z internetem za pośrednictwem standardowych interfejsów sieciowych (np. WiFi, bluetooth).

Jednym z aspektów dotyczących szeroko pojętego bezpieczeństwa „inteligentnych” zabawek jest możliwość uzyskania fizycznego dostępu do elementów odpowiedzialnych za komunikację lub przechowywanie danych. Jest to ogromnie ważne w sytuacji, gdy taka zabawka pochodzi z rynku wtórnego, kiedy dojdzie do jej zgubienia lub kradzieży, czego konsekwencją może być możliwość odczytania wrażliwych danych przechowywanych na urządzeniu albo modyfikacja oprogramowania w sposób, który pozbawi użytkownika kontroli nad zabawką. Wchodzą tu w grę kolejno: odczytanie np. poświadczeń do domowej sieci bezprzewodowej i modyfikacja zachowania zabawki, która wpłynie negatywnie na bawiące się nią dziecko. Możliwe jest również umieszczenie w urządzeniu dodatkowych funkcji pozwalających np. na podsłuchiwanie dziecka podczas zabawy albo domowników w zasięgu wbudowanej kamery czy mikrofonu.

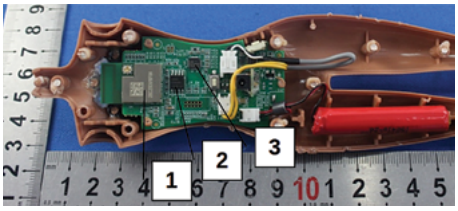
**Hello Barbie**

Pozornie niczym się nie różni od innych lalek tego producenta, jednak wyposażona jest w stację dokującą i ładowarkę (patrz rysunek 10).

Rys. 10 Hello Barbie razem z akcesoriami

Po rozebraniu i otwarciu lalki możemy dostrzec płytkę drukowaną i zidentyfikować wszystkie elementy funkcjonalne (patrz rysunek 11):

1. moduł sieci bezprzewodowej – AzureWave AWCU300E 802.11 b/g/n,
2. pamięć przechowująca oprogramowanie i wszystkie dane - Gigadevice GD25Q16 16Mbit SPI Flash,
3. moduł audio odpowiedzialny za przetwarzanie sygnałów z mikrofonu i odtwarzanie dźwięków – Nuvoton NAU8810 24bit.



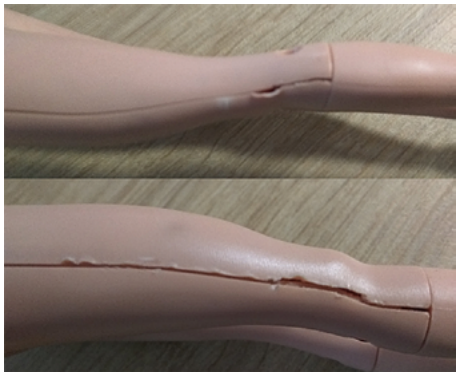
Rys. 11 Hello Barbie po rozebraniu.

W sytuacji gdyby osoby trzecie weszły w posiadanie zabawki, najbardziej narażonym elementem jest pamięć urządzenia, ponieważ pozwala ona na odczyt całej swojej zawartości. Podczas analizy wykazano, że aby odczytać całą zawartość pamięci, należy wylutować element i za pomocą czytnika odtworzyć jej zawartość. Podczas analizy zawartości pamięci okazało się, że została ona podzielona na sekcje ze względu na obszary funkcjonalne.

- Sekcja 1 zawiera tzw. boot loader pozwalający na uruchomienie oprogramowania sterującego zabawką.
- Sekcja 2 zawiera konfigurację urządzenia z poświadczeniami do sieci bezprzewodowej. Warto tu zaznaczyć, że odczytanie tych danych nie było możliwe ponieważ są przechowywane w postaci zaszyfrowanej.
- Sekcja 3 to oprogramowanie sterujące lalką.
- Sekcja 4 to oprogramowanie sterujące modułem WiFi.
- Sekcja 5 zawiera wszystkie pliki dźwiękowe pozwalające zabawce na podstawową komunikację z dzieckiem i rodzicem, które konfiguruje lalkę do dostępu do sieci bezprzewodowej.

W takiej sytuacji nie mamy łatwego dostępu do wrażliwych danych zapisanych w pamięci lalki. Pozostaje trudna, uciążliwa i wymagająca specjalistycznej wiedzy modyfikacja oprogramowania lub plików dźwiękowych znajdujących się w pamięci.

Należy niezwykle ostrożnie podchodzić do nabywania takiej zabawki na rynku wtórnym. Jeśli już się decydujemy na taki zakup, to koniecznie trzeba sprawdzić, czy zabawka była wcześniej otwierana. W przypadku lalki Hello Barbie większość prób ingerencji powinna pozostawić jakieś ślady. Najłatwiej można to sprawdzić poprzez dokładne obejrzenie szczelin, w których stykają się dwie części

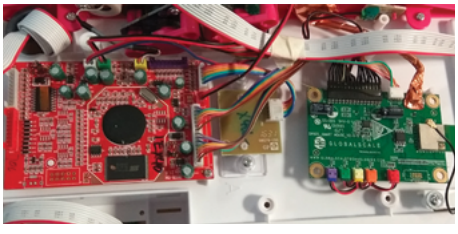

Rys. 12 Ślady po otwarciu Hello Barbie

lalki. Ponieważ lalka jest w dużej mierze sklejona wewnątrz, dostęp do wnętrza wymaga użycia siły, co z reguły pozostawia ślady na krawędziach (patrz rysunek 3).

Rysunki 10, 11 i 12 pochodzą ze stron: https://fccid.io/PIYDKF74-15A5W, http://somersetrecon.com/s/HelloBarbieSecurityAnalysis.pdf.

**Dream House**

Inteligentny domek dla lalek tego samego producenta co lalka Hello Barbie. Po otwarciu ukazują nam się dwie płytki drukowane, a na uwagę zasługuje zielona (patrz rysunek 13). Na pierwszy rzut oka wygląda podobnie do układu z lalki Hello Barbie.

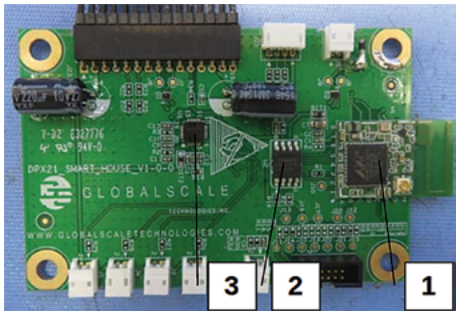


Rys. 13 Jednostka centralna Dream House po otwarciu

Na płytce można zidentyfikować takie same bloki funkcjonalne jak w przypadku Hello Barbie. Na rysunku 14 zostały wskazane poszczególne moduły:

1. moduł sieci bezprzewodowej,
2. pamięć przechowująca oprogramowanie i wszystkie dane – Winbond W25Q128FV,
3. moduł audio odpowiedzialny za przetwarzanie sygnałów z mikrofonu i odtwarzanie dźwięków.

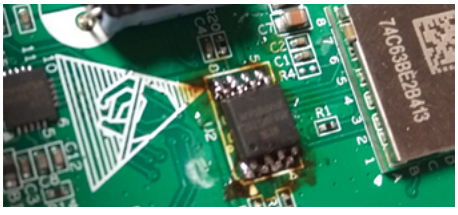
Ułożenie elementów na płytce sugeruje, że jest to taki sam układ jak Hello Barbie tylko z inną (większą) pamięcią. Po wylutowaniu kości pamięci i odczytaniu jej zawartości okazało się, że jest to dokładnie taki sam układ pod względem wykorzystywanych funkcji. Większa pamięć została wprowadzona ze względu na większy rozmiar plików z dźwiękami. Druga płytka natomiast odpowiedzialna jest za sterowanie poszczególnymi elementami domku, jednak nie realizuje komunikacji z siecią.




Rys. 14 Moduł komunikacyjny Dream House

W odróżnieniu od lalki domek pozwala na dostęp do układów elektronicznych dzięki wygodnym do odkręcenia wkrętom, co nie pozostawia śladów manipulacji. W związku z tym, jeśli zdecydujemy się na nabycie

takiej zabawki z niezaufanego źródła nie ma możliwości zweryfikowania, czy zostały dokonane jakieś modyfikacje. W takiej sytuacji pozostaje jedynie rozkręcenie zabawki i sprawdzenie, czy kość pamięci została wylutowana i wlutowana z powrotem. Zwykle powinny zostać jakieś ślady w okolicy nóżek kości (patrz rysunek 15) jednak można tego dokonać również bardzo starannie i nie pozostawić większych śladów ingerencji.




Rys. 15 Przykład śladów po manipulacji przy kości pamięci

Zdjęcia Dream House (rys. 13, 14, 15) pochodzą ze strony: https://fccid.io/PIYDPX-21-16A5W.

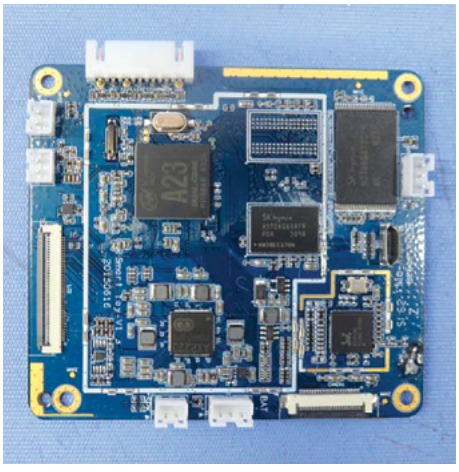
### Fisher Price Smart Toy

Najbardziej zaawansowana technologicznie zabawka poddana analizie. Z zewnątrz jest to przyjemny pluszowy miś panda lub małpka (patrz rysunek 16), w środku natomiast jest to układ elektroniczny przypominający funkcjonalnie i technologicznie smartfon. W celu podłączenia się do urządzenia konieczne jest rozprucie futra z tyłu na odcinku od ogona po podstawę głowy (patrz rysunek 17) oraz przecięcie jednej opaski zaciskowej. Po tym można przejść do wydostania obudowy urządzenia i swobodnego odkręcenia pokrywy. Zabawka jest kontrolowana przez systemem operacyjny z rodziny Android. Umieszczenie na płytce portu USB (patrz rysunek 18) pozwala na interakcję z urządzeniem w takim samym zakresie jak w przypadku smartfona. Pozwala na dostęp do plików i procesów, instalację własnych aplikacji, odczytywanie wszystkich danych z urządzenia. Najlepiej można

Rys. 16 Smart Toy w wariancie małpka

Rys. 17 Smart Toy po rozpruciu

zobrazować zagrożenie poprzez przygotowanie aplikacji instalowanej w środowisku Android i wykorzystanie jej do podsłuchu, wykorzystując wbudowane w pluszaka kamerę i mikrofon.



Rys. 18 Płyta główna Smart Toy z zaznaczonym portem USB.

Inteligentna zabawka od Fisher Price pozwala na duży zakres manipulacji w jej oprogramowaniu po uzyskaniu fizycznego dostępu. Jedyny ślad ingerencji, jaki pozostanie, to ślad ponownego szycia futra na plecach pluszaka. Można to jednak zrobić bardzo starannie, a wówczas – aby znaleźć ślad ingerencji – potrzebne będą bardzo wnikliwe oględziny.

Zdjęcia Smart Toy (Rys. 16, 17, 18) pochodzą ze strony: https://fccid.io/CCT-DNV31-15.

# 6. Okiem ekspertów prawa

Duża część dostępnych dziś na rynku zabawek inteligentnych produkowana jest przez podmioty mające siedzibę na terenie USA, w oparciu o tamtejsze regulacje prawne dotyczące prywatności i ochrony danych osobowych. Również zabawki wybrane do testów w ramach przygotowywania tego poradnika zakupione zostały w Stanach Zjednoczonych. Z tego względu nie korespondują one w pełnym zakresie z regulacjami obowiązującymi na terenie Unii Europejskiej, w tym w Polsce. Poziom ochrony danych osobowych oraz prywatności na terenie USA jest co do zasady niższy niż w Unii Europejskiej, zarówno na gruncie aktualnego stanu prawnego, jak i mając na uwadze unijną reformę systemu ochrony danych osobowych, która wejdzie w życie w maju 2018 roku.

Bazując na analizach przeprowadzonych przez Kancelarię Prawną Everberg, przedstawiamy najważniejsze potencjalne ryzyka związane z korzystaniem z inteligentnych zabawek, wynikające z polityki bezpieczeństwa producentów i ich regulaminów ochrony prywatności użytkowników.

**Zakres danych zbieranych przez producentów zabawek / oprogramowania**

Interaktywne zabawki oferowane przez wskazanych producentów automatycznie zapisują i przesyłają różnego rodzaju dane osobowe dotyczące dziecka, które z nich korzysta. Producenci wskazują, że zabawki te mogą zbierać między innymi dane o zainteresowaniach dziecka, rzeczach które lubi lub których nie lubi, a także inne dane dotyczące edukacji. Oznacza to, że **producent zabawki przechowuje i przetwarza (między innymi analizuje również w zautomatyzowany sposób) dane pozyskane podczas interakcji z zabawką.**

Należy zwrócić uwagę, że pomimo określenia, jakiego typu dane są automatycznie zbierane, nie jest to w żadnym wypadku katalog zamknięty, a więc producent nie ogranicza w jakikolwiek sposób zakresu danych, które może pozyskiwać i przetwarzać na skutek interakcji dziecka z zabawką. W dodatku pojęcia, które opisują ten otwarty katalog zbieranych danych, są na tyle niedookreślone,

że producent jest *de facto* uprawniony do zbierania wszelkiego rodzaju informacji pozyskanych podczas korzystania przez dziecko z danej zabawki.

Niektóre zabawki zapisują również nagrania dźwiękowe pozyskane w trakcie interakcji dziecka z zabawką. Nagrania te są następnie przetwarzane (analizowane, tłumaczone, poddawane badaniom) przez producenta oraz podmioty działające na jego zlecenie. Zakres czynności wykonywanych na pozyskanych w ten sposób nagraniach dźwiękowych jest w zasadzie nieograniczony. Co prawda producent wskazuje, że nagrania dźwiękowe ani ich zawartość nie będą wykorzystywane do kontaktu z dziećmi, jednak należy zwrócić uwagę, że skoro producent ograniczył możliwość wykorzystywania pozyskiwanych przez siebie danych jedynie w zakresie kontaktu z dziećmi, to uznać należy, że będzie on przetwarzał pozyskane za pomocą nagrań dźwiękowych dane do wszystkich innych celów. Przykładowo może on zbierać i przetwarzać dane pozyskane na skutek nagrania rozmów domowników mieszkających wraz z dzieckiem korzystającym z zabawki.

**Dostęp rodziców do zbieranych przez producenta danych**

W polityce CogniToy Dino producent wskazał, że rodzic ma dostęp do większości danych zbieranych przez producenta na skutek interakcji dziecka z zabawką, nie tłumacząc, jakie dane nie są dostępne dla rodzica i dlaczego. Zgodnie z regulacjami obowiązującymi w Polsce (art. 32 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych), każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych. Porównując zatem zakres uprawnień rodzica, który dysponuje danymi swojego dziecka wynikający z analizowanej polityki bezpieczeństwa z zakresem uprawnień wynikającym z przepisów obowiązujących

zdj. Fotolia.com

na terenie Polski, ochrona osoby, której dane dotyczą (oraz rodzica dysponującego danymi swojego dziecka), jest zdecydowanie mniejsza na gruncie polityki CogniToy Dino. W tym kontekście pojawia się **ryzyko związane z możliwością przetwarzania przez producenta zabawki danych osobowych bez wiedzy i zgody osoby, której dane dotyczą (lub rodzica dziecka, którego dane dotyczą).**

**Niedoskonałość systemu Privacy – Shield**

Polityka bezpieczeństwa Hello Barbie wskazuje, że producent posiada certyfikat związany z porozumieniem „EU-U.S. Privacy Shield Frameworks". Założeniem tego programu certyfikacji jest zrównanie poziomu ochrony danych osobowych przetwarzanych przez podmioty mające siedzibę w USA (podmioty wpisane na listę certyfikowanych podmiotów), z poziomem ochrony danych obowiązującym w Unii Europejskiej i Szwajcarii.

Wskazać należy, że pomimo posiadania certyfikatu podmioty mające siedzibę na terenie USA nie zapewniają ochrony tak daleko idącej, jak wymaga tego ustawodawstwo europejskie. Przykładowo, producenci zabawek mogą przekazywać dane osobowe do krajów trzecich, które nie zapewniają odpowiedniego poziomu ochrony (o czym mowa szerzej poniżej).

**Przekazywanie danych do państw trzecich**

Na gruncie przepisów o ochronie danych osobowych obowiązujących na terenie Unii Europejskiej, przekazywanie danych osobowych poza Europejski Obszar Gospodarczy jest dozwolone jedynie, gdy dane państwo zapewnia odpowiedni stopień ochrony danych osobowych. Dzięki takiemu rozwiązaniu dane osobowe są, co do zasady, chronione przed skutkami ich ewentualnego transferu do państwa, w którym regulacje w tym zakresie nie zapewniają takiego poziomu bezpieczeństwa jak reżim obowiązujący w EOG.

Producenci zabawek zastrzegają sobie często prawo przekazywania danych poza terytorium USA, nie precyzując, do jakich krajów dane mogą być transferowane. W konsekwencji powstaje ryzyko przekazywania pozyskanych przez producenta danych osobowych do kraju trzeciego, w którym standardy ochrony danych są na niskim poziomie lub w ogóle ich nie ma. Stanowi to istotne zagrożenie dla zachowania danych w poufności. Przykładowo należy wskazać, że jeśli dane trafią do kraju, w którym dopuszczalne jest handlowanie bazami danych bez żadnych ograniczeń, osoba, której dane dotyczą, nie będzie miała jakichkolwiek narzędzi umożliwiających jej kontrolę, jakie podmioty przetwarzają dane, jakimi

danymi dysponują ani w jakich celach je przetwarzają. **W konsekwencji osoba taka pozbawiona będzie również jednego z podstawowych praw przysługujących jej na terenie Unii Europejskiej – prawa do kontroli przetwarzania danych, które jej dotyczą.**

**Udostępnianie danych organom ścigania i administracji**

Analizowane polityki bezpieczeństwa przewidują możliwość przekazywania danych osobowych do organów ścigania i organów administracji USA. Możliwość ta jest zastrzeżona na rzecz producenta właściwie bez żadnych ograniczeń, gdyż jednym z warunków takiego udostępnienia danych jest własne przekonanie producenta o konieczności ich przekazania. W konsekwencji producent jest uprawniony do przekazywania danych organom państwowym (prokuraturze, policji, innym służbom) w każdej sytuacji.

Takie ukształtowanie uprawnień producenta jest w istocie umożliwieniem organom państwowym prowadzenia inwigilacji obywateli na szeroką skalę, bez jakiejkolwiek kontroli sądowej w tym zakresie. Stanowi to istotną odmienność w stosunku do reżimu panującego co do zasady w Unii Europejskiej, gdzie przekazywanie danych osobowych organom państwowym jest ograniczone do szczególnych sytuacji i poddane jest badaniu przez sąd między innymi co do zasadności ich udostępnienia.

Jak ostatnio podkreślał John Carr[15], być może regulacja RODO zapewni wystarczającą podstawę prawną, która ustali wymogi polityki bezpieczeństwa producentów. Wydaje się, że w najbliższej przyszłości powinno pojawić się, w przypadku zabawek interaktywnych, coś na wzór systemu oznakowania CE, aby rodzice i dzieci mieli łatwy sposób na przekonanie się, że to, co mogą kupić lub czego mogą użyć, spełnia pewne podstawowe standardy ochrony ich prywatności.

zdj. Fotolia.com

15 https://johnc1912.wordpress.com/2017/07/19/more-warnings-about-the-internet-of-toys/.

## Wnioski

**Producenci zabawek interaktywnych, których polityka bezpieczeństwa została poddana analizie, nie zapewniają ochrony danych osobowych na poziomie wymaganym przez przepisy obowiązujące w Unii Europejskiej, w tym w Polsce.**

- **Zakres danych osobowych zbieranych i przetwarzanych przez producentów zabawek jest niedookreślony, w konsekwencji czego producenci mogą przetwarzać co do zasady wszelkie dane pozyskane w trakcie interakcji z zabawką.**
- **Niektóre urządzenia przechwytują dźwięk, a nagrania pozyskane w ten sposób mogą być przetwarzane przez producentów bez żadnych ograniczeń, co może uniemożliwić lub istotnie ograniczyć prawo osoby, której dane dotyczą (lub rodzica dziecka, którego dane dotyczą), do kontroli zakresu przetwarzanych danych (jedno z podstawowych praw w reżimie prawa ochrony danych na terenie UE).**
- **Producenci nie gwarantują jednoznacznie możliwości dostępu do przetwarzanych danych przez osobę, której dane dotyczą (lub rodzica dziecka, którego dane dotyczą), co w istotny sposób może ograniczać możliwość kontroli zakresu przetwarzanych danych (jedno z podstawowych praw w reżimie prawa ochrony danych na terenie UE).**
- **Posiadanie przez producenta certyfikatu przyznanego w ramach programu „EU-U.S. Privacy Shield Frameworks" nie oznacza spełniania przez takiego producenta wszystkich wymogów dotyczących przetwarzania danych osobowych wynikających z prawa obowiązującego na terenie UE.**
- **Istotnym zagrożeniem dla skutecznej ochrony danych osobowych przetwarzanych przez producentów zabawek jest możliwość przekazywania zbieranych przez nich danych do krajów, w których ochrona w tym zakresie jest na niskim poziomie lub w ogóle jej nie ma.**
- **Możliwość udostępniania danych osobowych organom państwowym (w tym przypadku USA) – np. policji, prokuraturze, innym służbom – bez żadnej kontroli sądowej, stanowi istotną odmienność od zasad obowiązujących na terenie RP w tym zakresie i może wiązać się z bezpodstawną inwigilacją przeprowadzoną przez organy amerykańskiej administracji.**

## porady W pigułce

**Kilka porad przed kupieniem zabawki *smart connected***

- Zastanów się, czy wziąłeś pod uwagę wszystkie zagrożenia związane z zakupem danej zabawki i czy są one uzasadnione jej „inteligentnymi" funkcjami. Być może tradycyjna zabawka będzie bezpieczniejszym wyborem?
- Nie kupuj inteligentnej zabawki pod wpływem impulsu podczas wizyty w sklepie. Wielu istotnych informacji nie znajdziesz na pudełku ani nie uzyskasz od sprzedawcy.
- Poczytaj opinie o zabawce, poszukaj filmów. Spróbuj przekonać się, czy jej działanie jest zgodne z Twoim wyobrażeniem.
- Poszukaj informacji na temat ewentualnych problemów z bezpieczeństwem zabawki – artykułów, technicznych opisów błędów.
- Bądź szczególnie ostrożny w stosunku do zabawek, które dopiero pojawiły się na rynku. Jest duża szansa, że producent wypuścił je przed ukończeniem wszystkich testów i za jakiś czas dostępne będą ich poprawione wersje.
- Nie kupuj zabawek z rynku wtórnego, jeśli nie masz pełnego zaufania do sprzedającego i nie znasz ich pochodzenia. Zabawka mogła zostać zmodyfikowana – np. by wysyłać dane nie tylko do producenta.
- Kupując zabawkę, dopasuj ją dobrze do wieku dziecka.

## porady W pigułce

### Po zakupie

- Konfigurując zabawkę z użyciem smartfonu (także np. dodając nową sieć WiFi), upewnij się, że jesteś w bezpiecznym miejscu, gdzie nikt niepowołany nie podłączy się do zabawki zamiast Ciebie.
- Zapoznaj się dokładnie z polityką prywatności przed jej zaakceptowaniem. Czy wiesz, jakie dane będą przechowywane, gdzie i przez kogo?
- Tworząc konto online, stwórz hasło inne od używanych wcześniej i upewnij się, że jest odpowiednio silne – ma minimum 10 znaków i zawiera znaki również spoza podstawowego alfabetu (np. cyfry, znaki interpunkcyjne).
- Podawaj tylko tyle rzeczywistych informacji o sobie/dziecku, ile jest niezbędne do poprawnego działania zabawki.
- Pamiętaj, aby zabawkę łączyć tylko z zaufanymi sieciami WiFi. Nie wystarczy, że sieć jest szyfrowana – czy na pewno wiesz, kto zarządza jej punktem dostępowym?
- Przeglądaj regularnie konto, na którym zbierane są dane z zabawki. Na bieżąco usuwaj niepotrzebne dłużej treści.
- Nie wchodź na konto, korzystając z odnośników otrzymanych mailem czy komunikatorem, aby nie paść ofiarą wyłudzenia danych dostępowych. Loguj się samodzielnie, wpisując adres strony lub dodając go do zakładek.
- Upewnij się, że zabawka jest wyłączona, gdy nie jest używana.
- Dbaj o równowagę pomiędzy zabawą z rówieśnikami a czasem spędzonym w towarzystwie zabawek cyfrowych czy też urządzeń ekranowych.
- Pamiętaj, że wiedza zaimplementowana w zabawkach jest często wyselekcjonowana i limitowana, a tematyka prowadzenia interakcji często ograniczona wizją producenta.
- Pamiętaj, że Twoje dziecko może być też adresatem ukrytego marketingu.

## porady W pigułce

**Przed pozbyciem się zabawki**

- Pamiętaj o usunięciu danych z zabawki przez tzw. przywrócenie urządzenia do stanu fabrycznego. Informacje, jak to zrobić, powinny znajdować się w instrukcji.
- Jeśli nie planujesz już używać takiej samej zabawki, rozważ usunięcie konta w serwisie producenta.

Spis treści:

O autorach:

**Anna Rywczyńska**
Koordynatorka Polskiego Centrum Programu Safer Internet oraz kierowniczka Zespołu Projektów Społecznych w NASK PIB. Ekspertka w dziedzinie bezpiecznego korzystania przez dzieci i młodzież z internetu i nowych mediów. Współtwórczyni międzynarodowej konferencji „Bezpieczeństwo dzieci i młodzieży w internecie". Autorka i współautorka publikacji oraz narzędzi edukacyjnych, członkini międzynarodowych grup roboczych między innymi w ramach agencji ENISA oraz organizacji ECSO.

**Przemysław Jaroszewski**
Kieruje zespołem CERT Polska, działającym w NASK BIP. Programista i psycholog społeczny. Ma kilkanaście lat doświadczenia w bezpieczeństwie teleinformatycznym, a w swojej karierze zaangażowany był w wiele krajowych i międzynarodowych projektów związanych ze współpracą zespołów reagujących oraz wymianą danych. Współautor materiałów szkoleniowych oraz trener w programach dla zespołów reagujących, między innymi TRANSITS i ENISA CERT Exercises.

Współpraca ekspercka:

**Mikołaj Kopeć**
Konsultant bezpieczeństwa IT w NASK BIP, z wieloletnim doświadczeniem. Specjalizuje się w bezpieczeństwie infrastruktury teleinformatycznej i aplikacyjnej. Entuzjasta systemów wbudowanych, OT i IoT oraz aspektów bezpieczeństwa związanych z nimi. Uczestniczył w wielu projektach z obszaru audytu bezpieczeństwa, oceny podatności infrastruktury i systemów oraz testów penetracyjnych dla firm i instytucji z sektora finansowego, publicznego, nowych technologii. Jest absolwentem wydziału cybernetyki Wojskowej Akademii Technicznej, ze specjalizacją sieci teleinformatyczne.

**Realizacja badań ilościowych**
**– Ogólnopolski Panel Badawczy Ariadna**

ariadna
ogólnopolski panel badawczy

**Przeprowadzenie analizy prawnej**
**Kancelaria Everberg**

EVERBERG
ONE STEP AHEAD

Perspektywa międzynarodowa:

**Chris Pinchen, „Agencja Prywatności”**

Rodzice powinni mieć świadomość, że zabawki IoT są w większości wytwarzane przez producentów zabawek, a nie przez firmy technologiczne. Może to oznaczać, że cała część IoT zajmuje drugie miejsce, a firmy produkujące zabawki nie mają żadnego doświadczenia w zakresie bezpieczeństwa cyfrowego.

Rodzice powinni również zwrócić uwagę na to, czy zastosowana w zabawkach technologia będzie podtrzymywana lub też czy za uaktualnienia nie będą musieli dodatkowo płacić. Jeśli zabawka ma oprogramowanie lub sprzęt, który przestanie być wspierany, czy będzie nadal funkcjonować? Należy pamiętać, że firma produkująca zabawki jest zainteresowana sprzedażą zabawek i może zlecać technologię, prowadzenie baz danych i gromadzenie danych stronom trzecim – czy te „strony trzecie” mają doświadczenie i dobrą renomę w tej dziedzinie? Jakie są ich obowiązki w odniesieniu do prywatności i ochrony danych? Czy można uzyskać te informacje? A także, co z regulacjami prawnymi – gdzie są zapisane dane, na jakich obszarach i wedle jakich obowiązujących przepisów?

**Barbara Buchegger, kierowniczka projektów pedagogicznych, Austriackie Centrum Safer Internet**

Zabawki podłączone wchodzą do pokoi i życia naszych dzieci od najmłodszych lat. Od lalek, robotów, samochodów, do „smartwatchy” lub okularów: często trudno wykryć, jakie dane są zbierane, jak bezpieczne jest połączenie… Nie zawsze potrafimy radzić sobie z tymi nowymi, cyfrowymi asystentami. Dlatego też rodzice potrzebują wskazówek i informacji na temat możliwości, jakie dają zabawki, ale też zagrożeń, jakie mogą ze sobą nieść. Dotyczy to nadzoru i prywatności z jednej strony, ale także ryzyka polegającego między innymi na tym, że dzieci zbytnio polegają na rodzicach lub innych dorosłych, ponieważ „oni tak czy inaczej zawsze wiedzą, co robię”. Niezależnie jednak od potencjalnych zagrożeń cyfrowe, interaktywne zabawki oferują nieznane jeszcze i może nawet niewyobrażalne możliwości uczenia się i dostępu do informacji.

Autorzy: Anna Rywczyńska, Przemysław Jaroszewski
Korekta: Katarzyna Wilczek
Projekt okładki i skład: Aneta Witecka



NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa
www.nask.pl
Wydanie I
Warszawa 2018
ISBN 978-83-65448-05-7

NASK

NASK jest Państwowym Instytutem Badawczym nadzorowanym przez Ministerstwo Cyfryzacji. Prowadzi badania w zakresie rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Kluczowym polem aktywności NASK są działania związane z zapewnieniem bezpieczeństwa internetu.

Reagowaniem na zdarzenia naruszające bezpieczeństwo sieci w Polsce i koordynacją działań w tym obszarze zajmuje się pion NC Cyber, w którego skład wchodzi zespół CERT Polska. NASK prowadzi także rejestr domeny pl. Ważną rolę pełni działalność edukacyjna i popularyzacja idei społeczeństwa informacyjnego. W Akademii NASK realizowane są projekty społeczne oraz unikatowe szkolenia dla firm i instytucji ze szczególnym uwzględnieniem tematyki bezpieczeństwa ICT. Od lat prowadzony jest program Komisji Europejskiej Safer Internet, promujący bezpieczne korzystanie z nowych technologii i internetu wśród dzieci i młodzieży.

W NASK realizowane są również systematyczne badania społeczne w obszarze bezpieczeństwa internetu oraz edukacji cyfrowej, a wśród nich cykliczne ogólnopolskie badania młodych użytkowników sieci zatytułowane „Nastolatki 3.0”. Rolę konsultacyjną w tym obszarze pełni Naukowe Kolegium Ekspertów ds. Rozwoju Technologii Informacyjno-Komunikacyjnych w Edukacji, które tworzą uznani naukowcy i specjaliści w dziedzinie edukacji oraz wykorzystania nowych technologii w nauczaniu.

NASK prowadzi portal e-learningowy IT Szkoła (www.it-szkola.edu.pl) skierowany do uczniów szkół ponadgimnazjalnych i nauczycieli, pomagający w podnoszeniu poziomu kompetencji cyfrowych poprzez wykłady on-line i certyfikowane kursy.

W ramach Instytutu funkcjonuje Dyżurnet.pl, jedyny w Polsce punkt kontaktowy, który przyjmuje zgłoszenia dotyczące nielegalnych i niebezpiecznych treści w internecie, przede wszystkim związanych z materiałami przedstawiającymi seksualne wykorzystywanie dzieci. NASK PIB na mocy ustawy pełni rolę operatora Ogólnopolskiej Sieci Edukacyjnej – programu, którego celem jest podłączenie wszystkich szkół w Polsce do szybkiego i bezpiecznego internetu.

NASK Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa
tel. 22 380 82 00, fax 22 380 82 01, nask@nask.pl
www.nask.pl