

Interaktywne zabawki zagrożeniem dla prywatności

6 grudnia 2017

Przed zakupem interaktywnej zabawki dla dziecka, która łączy się z internetem, trzeba koniecznie sprawdzić jej producenta, politykę prywatności i bezpieczeństwa – przestrzegło w tym roku FBI. Taka niepozorna zabawka może zostać szybko i łatwo zhakowana albo – dzięki wbudowanym kamerom i mikrofonom – posłużyć jako urządzenie szpiegowskie, które będzie podsłuchiwać otoczenie dziecka. Nowoczesne, elektroniczne zabawki rejestrują i gromadzą też duże ilości informacji, które mogą zostać wykradzione albo użyte w niewłaściwy sposób.



– W przypadku zabawek, które mają urządzenia rejestrujące, mikrofon czy kamerę, najpoważniejszym zagrożeniem jest to, że są one podłączone do internetu i komunikują się z infrastrukturą producenta. Decydując się na zakup tego typu elektroniki dla dzieci, trzeba wiedzieć, że istnieje potencjalne ryzyko ujawnienia tych informacji – przestrzega w rozmowie z agencją informacyjną Newseria Biznes Marcin Pielaszek, ekspert Wyższej Szkoły Bankowej we Wrocławiu.

Elektroniczne, interaktywne zabawki dla dzieci cieszą się

ogromną popularnością, a ich sprzedaż rośnie zwłaszcza w okresie przedświątecznym. Są wyposażone w kamery, czujniki czy mikrofony, systemy komunikacji bluetooth i wi-fi. Dzięki połączeniu z internetem można je podłączyć do tabletu czy smartfona i sterować za pomocą aplikacji. Dziecko może rozmawiać z taką zabawką i zadawać jej pytania, a aplikacja zmienia tekst mówiony w pisany i udziela odpowiedzi na podstawie informacji znalezionych w sieci.

– Takie zabawki naśladują naturalną postać, rozpoznają mowę dzieci, które często przekazują im swoje tajemnice, opowiadają o swoim życiu, mówią, do jakiej chodzą szkoły, gdzie mieszkają i jak nazywają się rodzice. Wszystkie te informacje spływają na serwer producenta, tam są analizowane i przetwarzane, tak żeby zabawka naturalnie rozmawiała z dzieckiem, na przykład naśladując mowę bajkowej postaci. Dziecko jest bezbronne i będzie szczerze mówić do tej zabawki różne rzeczy, które znajdują się w infrastrukturze producenta – mówi Marcin Pieleśzek.

Ekspert radzi, żeby przed zakupem elektronicznej, interaktywnej zabawki w prezencie dla dziecka dokładnie sprawdzić jej producenta, zapoznać się z polityką prywatności i bezpieczeństwa. Dobrze jest też zasięgnąć opinii znajomych, przeczytać opinie na internetowych forach albo serwisy poświęcone bezpieczeństwu teleinformatycznemu, gdzie można znaleźć przykłady dotyczące konkretnych zabawek i marek.

– Jeżeli decydujemy się kupić dziecku zabawkę, która rejestruje dźwięk, obraz i przesyła te dane do internetu, możemy zmniejszyć ryzyko, decydując się na zakup od sprawdzonego, znanego producenta. Pewne ryzyko i tak zawsze pozostaje. Informacje, które zostały w bazach danych producenta tej zabawki, powinny być odpowiednio chronione, ale one już z naszego domu wyszły i nie ma stuprocentowej gwarancji, że tak rzeczywiście będzie – mówi Marcin Pieleśzek.

Nowoczesne, elektroniczne zabawki rejestrują i gromadzą duże

ilości informacji, które mogą zostać wykradzione albo użyte w niewłaściwy sposób. Z drugiej strony ze względu na słabe zabezpieczenia albo wręcz ich brak mogą szybko i łatwo zostać zhakowane.

– Niebezpieczeństwo tkwi nie tylko w tym, że informacje są przekazywane do internetu czy producenta zabawki, bo inne osoby też mogą uzyskać do niej dostęp. Na filmikach w znanym serwisie wideo można zobaczyć, jak hakuje się taką zabawkę, która zaczyna na przykład mówić brzydkie słowa. Na zasadzie eksperymentu pokazano, jak uzyskać dostęp do takiej zabawki i że może to zrobić przykładowo sąsiad zza ściany. Oczywiście nie wszystkie urządzenia i nie wszyscy producenci są na to podatni – mówi Marcin Pieleśzek.

W lipcu tego roku oficjalnie ostrzeżenie przed zabawkami, które łączą się z internetem, wydało FBI. Amerykańskie biuro śledcze przestrzegło, że mogą one naruszać prywatność dziecka i zagrażać jego bezpieczeństwu albo śledzić otoczenie dziecka i codzienne życie całej rodziny, a później przekazywać takie informacje cyberprzestępcom. FBI zaleca, żeby wybierać te zabawki, które łączą się z internetem przez protokoły szyfrujące zabezpieczone silnym hasłem i zwracać uwagę na to, czy producent często aktualizuje oprogramowanie dotyczące zabezpieczeń.

Wiosną tego roku w mediach głośno było o interwencji niemieckiego urzędu regulacyjnego (Bundesnetzagentur), który nakazał wycofać ze sprzedaży interaktywne lalki Cayla, które – za pośrednictwem Bluetooth – mogły służyć jako urządzenia szpiegowskie, podsłuchiwać otoczenie dziecka czy transmitować reklamy (zabawka reklamuje inne marki, wspominając o nich podczas rozmowy z dzieckiem).

Zdjęcie: [vborodinova](#) (CC0)

Źródło: [Newseria.pl](#)