Bezpieczna bransoletka?

25 lutego 2017

Jakiś czas temu sprawdzałam, jak nosidła (ang. wearables) radzą sobie z ochroną prywatności. Informacje, które udało mi się znaleźć, nie były zachęcające. Postanowiłam dać nosidłom kolejną szansę i przekonać się, czy z bezpieczeństwem zbieranych danych jest lepiej niż z jasnością warunków wykorzystywania takich urządzeń i z przestrzeganiem przez producentów zasad ochrony danych osobowych.

Nosidła monitorujące aktywność fizyczną stają się coraz popularniejsze. Wiele osób nawet nie zastanawia się, w jaki sposób informacje z bransoletki trafiają do aplikacji w telefonie ani czy dostęp do nich ma ktoś jeszcze. Przeprowadzone przez kanadyjską organizację pozarządową Open Effect badanie dotyczące bezpieczeństwa transmitowanych danych pokazuje, że większość tego typu urządzeń nie jest w dostateczny sposób zabezpieczona. Przeglądowi zostało poddane 8 nosideł oferowanych przez różne firmy: Apple Watch, Basis Peak, Fitbit Charge HR, Garmin Vivosmart, Jawbone UP 2, Mio Fuse, Withings Pulse O2 i Xiaomi Mi Band. W przypadku aż 7 z nich okazało się, że jeśli bransoletka nie została skonfigurowana z innym urządzeniem mobilnym (smartfonem, tabletem) i nie jest do niego podłączona, to można za jej

pośrednictwem śledzić lokalizację użytkownika. A że tego typu urządzenia nosi się praktycznie cały czas, to stworzenie mapy miejsc, w których często przebywa użytkownik, jest całkiem łatwe.

Dane dotyczące aktywności fizycznej, np. puls, mogą być ciekawą informacją na temat stanu naszego zdrowia. Zapewne jest to łakomy kąsek dla firm ubezpieczeniowych. Już teraz tego typu podmioty chcą wykorzystywać np. informacje z portali społecznościowych do określania stawek ubezpieczenia. A dzięki nosidłom mogą zyskać doskonałe narzędzie do sprawdzania, czy ubezpieczony żyje zdrowo. Bardzo łatwo wyobrazić sobie taką propozycję: noś naszą bransoletkę (zbierającą o tobie mnóstwo danych, łącznie z lokalizacją), by potwierdzać, że żyjesz zdrowo, a my na tej podstawie określimy dla ciebie preferencyjne stawki ubezpieczenia. Przy tym sięgniemy po algorytm, o którym nie dowiesz się zbyt wiele, bo to tajemnica naszego przedsiębiorstwa.

Abstrahując od tego, czy firmy ubezpieczeniowe powinny wykorzystywać takie urządzenia i czy będziemy godzić się na tego typu praktyki, trzeba pamiętać, że część urządzeń podatna jest na manipulację. Można więc stworzyć fałszywe informacje o tym, ile kroków przeszliśmy, ile kalorii spaliliśmy itp. A to może rodzić potencjalne problemy nie tylko dla ubezpieczycieli, ale także dla uczciwych użytkowników, którzy przez porównanie otrzymają gorsze warunki świadczenia usług. W przyszłości mogą się pojawić pomysły, by wykorzystywać smart urządzenia nie tylko do śledzenia tego, czy ktoś dba o zdrowie, ale także do celów dowodowych, np. w postępowaniach sądowych. Dlatego warto mieć świadomość, że dane wyciągnięte z fitness trackera mogą być nieprawdziwe.

Słabości w zabezpieczeniach wykazują nie tylko same bransoletki i zegarki: również część aplikacji obsługujących nosidła okazuje się podatna na włamanie. Ktoś obcy może zatem uzyskać nieautoryzowany dostęp do danych użytkownika – poczytać co nieco o jego lub jej stanie zdrowia,

przyzwyczajeniach i wyzwaniach, które podejmuje; zmieniać i usuwać zgromadzone dane.

Nosidła to jeden z przejawów Internetu rzeczy. Tak jak w przypadku innych tego typu urządzeń coraz częściej mierzyć będziemy się z konsekwencjami niedostatecznej dbałości o bezpieczeństwo. Jeśli nawet sami nie ucierpimy przez słabość zabezpieczeń zegarka lub bransoletki, to podłączając je do sieci, możemy umożliwiać ich wykorzystywanie jako botów w atakach DDoS.

Od wydania raportu z badania przeprowadzonego przez Kanadyjczyków minęło kilka miesięcy. Producenci smart bransoletek do śledzenia aktywności fizycznej mieli czas na poprawę zabezpieczeń. Mimo to nieszczególnie im dowierzam, dlatego większość dostępnych na rynku fitness trackerów otrzymuje u mnie kolejny minus. Z zakupem tego typu opaski poczekam, aż pod względem bezpieczeństwa staną się naprawdę „smart”.

Autorstwo: Anna Walkowiak
Zdjęcie: Unsplash (CC0)
Źródło: Panoptykon.org

BIBLIOGRAFIA

1. https://panoptykon.org/wiadomosc/nosidla-i-prywatnosc

2. https://openeffect.ca/reports/Every_Step_You_Fake.pdf

3. https://www.theguardian.com/technology/2016/nov/02/admiral-to-price-car-insurance-based-on-facebook-posts

4. http://www.makeuseof.com/tag/fitness-tracker-putting-security-risk/