Noua din zece aplicatii medicale si de fitness colecteaza mai multe date decât ar fi nevoie (studiu)

Majoritatea aplicatiilor medicale si de fitness din Google Play (88%) colecteaza mai multe date decât este nevoie, reiese dintr-un studiu publicat, recent, de Optus Macquarie University Cyber Security Hub din Sydney, citat de blogul din România al producatorului de securitate cibernetica, Eset.

"Principalele tipuri de date colectate de aplicatiile mHealth includ informatii de contact, locatia utilizatorului si mai multi identificatori de dispozitiv. O parte dintre acesti identificatori (ne referim în mod specific la identitatea internationala a echipamentelor mobile - IMEI, un identificator unic utilizat pentru amprentarea telefoanelor mobile; controlul accesului media - MAC, un identificator unic al interfetei de retea în dispozitivul utilizatorului si identitatea internationala a abonatului mobil, un numar unic care identifica în mod unic fiecare utilizator al unei retele celulare) sunt unici si persistenti, adica sunt imuabili si nu pot fi schimbati sau înlocuiti. De asemenea, pot fi utilizati de terti pentru a urmari utilizatorii din retele si aplicatii", se arata în studiul citat de Eset.

În acelasi context s-a evidentiat faptul ca doua din trei aplicatii colecteaza identificatori MAC si cookie-uri, o treime colecteaza adresele de e-mail ale utilizatorilor si aproximativ un sfert dintre aplicatii ar putea presupune locatia curenta a utilizatorului pe baza antenei la care sunt conectati.

Cu toate acestea, transmiterea datelor a fost înregistrata la doar aproximativ 4% dintre aplicatiile mHealth testate, cele mai comune tipuri de date transmise cuprinzând numele si locatiile utilizatorilor.

Potrivit sursei citate, desi modul în care aplicatiile mHealth colecteaza si partajeaza datele utilizatorilor ar putea fi considerate de rutina, raspunderea despre aceste practici nu a fost deloc transparenta. Astfel, aproape un sfert dintre transmiterile de date ale utilizatorilor, în special datele referitoare la parole si date de localizare, au fost observate având loc printr-o conexiune HTTP necriptata nesecurizata. În plus, circa o treime dintre aceste aplicatii nu au oferit niciun fel de politica de confidentialitate care detaliaza modul în care sunt tratate datele.

De asemenea, un sfert din totalul aplicatiilor analizate au gestionat datele într-un mod în care au fost încalcate politicile de confidentialitate.

"Acest lucru ar putea însemna probleme pentru companiile suspectate ca ar fi încalcat reglementarile privind confidentialitatea, cum ar fi Regulamentul general al Uniunii Europene privind protectia datelor (GDPR), care impune ca utilizatorii sa fie informati în mod clar despre modul în care sunt tratate datele lor. Aplicatiile mobile devin rapid surse de informatii si instrumente de sprijin pentru luarea deciziilor atât pentru clinicieni, cât si pentru pacienti. Astfel de riscuri de confidentialitate ar trebui sa fie comunicate pacientilor si ar putea face parte din consimtamântul privind utilizarea aplicatiilor. Credem ca ar trebui sa se tina seama de raportul între beneficiile si riscurile aplicatiilor mHealth pentru orice discutie tehnica si politica în jurul serviciilor furnizate de astfel de aplicatii", se mentioneaza în cercetarea de specialitate.

Studiul intitulat "Mobile health and privacy: cross sectional study" a fost publicat de British Medical Journal si a analizat 8.000 de aplicatii clasificate drept "medicale" si 13.000 de aplicatii care se încadreaza în categoria "sanatate si fitness". Documentul a inclus aproape toate aplicatiile mHealth accesibile în Google Play Store, în Australia.

Eset a fost fondata în anul 1992 în Bratislava (Slovacia) si se situeaza în topul companiilor care ofera servicii de detectie si analiza a continutul malware, fiind prezenta în peste 180 de tari.