Az okostelefonos egészségügyi alkalmazások adatbiztonsága

DR. SPEER GÁBOR

Világszerte félmilliárdnyian használnak okostelefont, s közülük egyre többen egészségügyi alkalmazásokat is, egészségmegőrzési, vagy akár gyógyítási, diagnosztikus céllal. Vajon visszaélhet-e bárki avval, hogy a felhasználók nemcsak az egészségügyi eredmények feldolgozásában laikusok, hanem érzékeny adataik sorsának követésében sem mérik fel a buktatókat, hiszen céljuk a saját egészségük – és ez így van jól. A jelen közlemény célja viszont az egészségügyi alkalmazások használatakor keletkezett adatok biztonságára való figyelmeztetés.

Az USA-ban 2014-ben a felnőtt lakosság negyede töltött le legalább egy egészségügyi alkalmazást okostelefonjára, és az orvosok egyharmada ajánlott már betegének ilyen alkalmazást. Magyarországon az okostelefon-tulajdonosok 17%-a töltött már le egészségügyi vagy életmódot támogató alkalmazásokat, a krónikus betegek körében 18%, a nem betegek körében pedig 13% ez az arány (a Szinapszis Kft. felmérése szerint). A felmérésben részt vevők 36%-a hallott már egészségügyi vonatkozású mobilalkalmazásokról, ami jelentős növekedés (korábban 26% volt). Mind a krónikus betegek (38% *vs.* 26%), mind az okostelefonnal rendelkezők (49% *vs.* 36%) tájékozottsága javult ebben a kérdésben. A kutatásból az is kiderült, hogy az egészségügyi appok megítélése pozitív, a megkérdezettek kétharmada tartotta hasznosnak azokat. Akik pedig rendelkeznek letöltött egészségügyi vagy életmódi alkalmazással, 44%-ban napi szinten használják is azt.[1]

A felhasználók többségének azonban, pozitív hozzáállása mellett, nincs fogalma arról, hogy az applikáció (app) belső működése milyen, s nem tudja azt sem, hogy a személyes adatai, amiket felvisz, beír vagy rögzít az alkalmazás használatával – a telefonján keresztül –, hol és hogyan tárolódnak. Ez ebben a szektorban jelenleg kizárólag bizalmi kérdés. A felhasználók bíznak az appon keresztül megvalósuló szolgáltatás etikai alapjaiban, ugyanis jelenleg az egészségügyi alkalmazásokat kínáló applikációk sincsenek akkreditálva adatbiztonsági szempontokból (sem) – bár az adatok biztonságos kezelésére léteznek egészségügyi hatósági ajánlások.[2]

EGY BRIT FELMÉRÉS TANULSÁGAI

Az egyik online megjelenésű, lektorált orvosi folyóirat, a *BMC Medicine* 2015. szeptember 7-ei számában publikált közlemény[3] őszintén beszél arról, hogy az Egyesült Királyság egészségügyi hatósága (National Health Service, NHS) által akkreditált mobile health (mhealth, azaz okostelefonon működő egészségügyi) applikációk nem megfelelően kezelik az azokat letöltő és alkalmazó emberek személyes és egészségügyi adatait. Bár a szerzők csupán 79 mhealth alkalmazást vizsgáltak, ami elenyésző a világon elérhető teljes kínálathoz képest, de egyéb közlések is arra utalnak, hogy a kérdés világszerte aktuális. A probléma azért gyakori, mert jelenleg mindenki (a betegek és az orvosok is) az alkalmazások

DR. SPEER GÁBOR
PhD. Társalapító, Artmedus.
http://artmedus.com

használt vagy éppen hibáit tesztelik, mintegy ismerkednek a használatukkal, s nem az eszközök által tárolt és továbbított egészségügyi adatok biztonságával vannak elfoglalva. Még.

A munkacsoport tehát 79 egészségügyi, okostelefonra letölthető alkalmazást vizsgált. A vizsgált alkalmazások wellness vagy fitness alkalmazások voltak, illetve krónikus betegségek gondozásának támogatására voltak alkalmasak. Ezek közül 70 alkalmazás (89%) online szervizen keresztül továbbította a felhasználó által bevitt adatokat. Egyetlen app sem tárolta a személyes adatokat a felhasználó okostelefonjára (megjegyzésem: jóval biztonságosabb, ha nem a telefonon tárolódnak az adatok, feltéve hogy megfelelők az adatvédelemi feltételek). Az olyan alkalmazások kétharmada, amelyek az interneten keresztül küldenek személyes adatokat (pl. egy adatbázisba), nem használt titkosítást adatvédelmi célból, sőt az egészségügyi appok 20%-a semmilyen, a felhasználó adatait védeni hivatott titoktartási szabályzattal (privacy policy) nem rendelkezett. Volt négy olyan mobilalkalmazás is, amely titkosítási védelem nélkül használt a felhasználó azonosítására egyértelműen alkalmas adatokat. Bár egyetlen, titoktartási szabályzattal rendelkező app sem gyűjtött (tárolt) és továbbított olyan személyes adatot, amelyet a leírt szabályzata tiltott volna, de ezek közül 38 app (48%) nem tartalmazta titoktartási szabályzatában azoknak a személyes adatoknak a felsorolását, amelyeket használat során az adatbázisba küldenek, tárolnak. Érdekes, hogy az ingyenes appok háromnegyede, míg a fizetőseknek csak a 43%-a tüntetett fel titoktartási szabályzatot. Azok az appok, amelyek esetében a felhasználó adatait továbbították, csak 70%-ban közöltek titoktartási szabályzatot. Több androidos alkalmazás, mint ahány iOS app tartalmazott titoktartási szabályzatot.

A regisztrációhoz, vagyis az alkalmazás letöltéséhez az appok kétharmada a használó személy azonosítását könnyen lehetővé tevő információkat kért, pl. e-mail címet, vagy akár a teljes nevet. Az alkalmazások kisebb része volt olyan, melynek használóját nehezen lehetett azonosítani más által, mert csak a felhasználó nemét, életkorát vagy hollétét (pl. csak irányítószám) kérte. Az alkalmazások háromötöde érzékeny információt közvetített, tárolt: olyan információkat, mint az egészségügyi adatok, illetve a beteg által vezetett egészségügyi napló. A programok ötöde alkoholfogyasztással, dohányzással és szerfüggőséggel kapcsolatos információkra is rákérdezett, tárolta azokat, és néhányuk az etnikai hovatartozást, a képzettséget és a szexuális szokásokat is firtatta.

Az alkalmazások többsége egy vagy több ún. harmadik partner cégen keresztül is kommunikált, leginkább akkor, amikor pl. a felhasználót olyan egészségügyi információs oldalakra navigálta, melyekre a felhasználó igényt tartott. Az alkalmazások ötöde hirdetéseket is közvetített a felhasználónak. Ugyan egyetlen alkalmazás sem adta ki hirdetőknek vagy marketingcégnek a felhasználó adatait, de egyes hirdetők ún. sütiket (cookies) generálva ezekhez elvben hozzájuthattak. Tehát, az app használóiról a hirdetők számára azonosíthatatlanul kerültek csak ki információk, de egyéb technikai trükkökkel azonosítani lehetett a felhasználót, illetve az eszközét (mobiltelefonját). Ezért lehetséges az, hogy a felhasználó személyre szabott hirdetést kaphatott. Az emberek nagyon érzékenyek az egészségükkel kapcsolatos információk iránt, ezért a felhasználó keresése alapján célzott hirdetés gyakran talál célba (vevőre). Az appok 24%-a küldött másnak statisztikát a felhasználó szokásairól, beírt adatairól, anélkül hogy ezt közölte volna a felhasználóval vagy megkérdezte volna tőle a regisztrációkor (az alkalmazás letöltésekor).

VAN IGÉNY AZ ADATBIZTONSÁGRA

Az alkalmazások jó része tehát érzékeny információt tárolt, de a tárolás nem volt titkosított. Fontos tudni, hogy a felhasználókat az nyugtatja meg, hogy username/password kettőst vagy PIN kódot is kér az app, de ez önmagában egyáltalán nem jelenti azt, hogy a bevitt és tárolt adatokat nem lehet azonosítani a felhasználóval. Ez leginkább arra jó, hogy a telefonon keresztül más nem láthatja a beírt adatokat. Az appok nagy része online eszközzel kommunikált (és itt tárolta a felhasználó adatait), ezek harmada az alkalmazás fejlesztői/működtetői által kontrollált szerverrel. Azok az alkalmazások a legsérülékenyebbek, amelyek „felhő alapú" tárolással őrzik az adatokat, és a fejlesztés nem terjedt ki az adatvédelmi biztonságosságra. A szerzők arra jutottak, hogy a legtöbb alkalmazás nem is tett lépéseket a felhasználó személyes információinak megfelelően biztonságos tárolására.

Egyelőre ugyan nem tudunk arról, hogy a mobil health adatokkal akár az Európai Unióban, akár az USA-ban visszaéltek volna, de ismerve a korábbi és a jelenlegi közlések eredményeit, nem kizárható az adatok „hackelése", mert a lehetőség megvan rá.[4] A közleménnyel arra szeretném felhívni a figyelmet, hogy a probléma nem megoldhatatlan, hiszen a „bankolás" az interneten keresztül egyértelműen biztonságos, és hogy igény van az adatbiztonságra, az is evidencia. Ennek garanciáit az mhealth szektorban is meg kell teremteni. Addig azonban a felhasználóknak is ügyelniük kell erre, és fontosnak tartom ezt a szempontot a megfelelő alkalmazások kiválasztásában.

Levelezési cím:
gabor.speer@artmedus.com

Irodalom:

1. http://www.szinapszis.hu/kutatasi_eredmenyek/122

2. Cortez NG, Cohen IG, Kesselheim AS. FDA regulation of mobile health technologies. N Engl J Med 2014;371(4):372-9.

3. Huckvale K, Prieto JT, Tilney M, Benghozi PJ, Car J. Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med 2015;13:214.

4. Huckvale K, Car J. Implementation of mobile health tools. JAMA 2014;311(14):1447-8.