Ettevaatust, pooled mobiilirakendused võivad sinu privaatseid andmeid himustada

9 aastat tagasi - 14.08.2017 Autor: AM

Euroopa Majandusuuringute Keskus uuris Google Play rakenduste poest alla laetud faile. Uuringust selgus, et 136 rakendusest pooli sai installida ainult pärast seda, kui telefoni omanik on lubanud juurdepääsu enda tundlikule teabele. 14 äppi olid problemaatilised mobiilirakendused eraelu ja isikuandmete kaitse seisukohast.

Tänapäevased nutitelefonid suudavad pea kõike, sest iga toimingu jaoks on olemas oma mobiilirakendused. Mängud, vöötkoodiskännerid, videokõned, ilmaennustus, transport, fototöötlus, keeleõpe – katmata valdkondi leidub väga vähe. Ühtlasi on tähelepanuväärne, et suurem osa nendest põnevatest rakendustest on tasuta. See peaks panema mõtlema, kuidas arendaja suudab neid üldse rahastada.

Tele2 tootedirektori Katrin Aroni sõnul ei ole mingi saladus, et reklaamil on tasuta rakendustes suur osa, kuigi mõned arendajad pakuvad ka reklaamivabu tasulisi versioone.

„Tekib küsimus, kuidas on lugu rakendustega, mis reklaami ei kasuta. Sel juhul on rahavoog varjatud ja hõlmab suure tõenäosusega isikuandmete müüki," rääkis Aron, kelle sõnul on ka isikuandmete müük seotud reklaamiga ja alati ei ole tegu tavalise hüpikreklaamiga.

„Nimi, telefoninumber ja aadress koos on ettevõtete jaoks väga väärtuslikud, sest osa neist on valmis suure andmehulga eest tohutuid summasid välja käima. Kui kasutaja profiil on moodustunud pikema aja jooksul, sisaldades otsingupäringuid Google'is, oste Amazonist ja broneeringuid reisisaitidel, on nutikate algoritmide abil võimalik inimese tegevust ennustada ja talle sobivat reklaami näidata. Seda tüüpi reklaam on väga edukas," selgitas Aron.

„Muidugi tekib küsimus, kuidas üldse selliseid isikustatud andmeid kogutakse. Kui jutt on nutitelefonidest, siis ei kogu ettevõtted andmeid ebaseaduslike vahenditega, näiteks häkkimise või pahavara abil. Tegelikult anname ise rakenduse arendajatele loa meie isikuandmetele juurde pääseda," lisas Aron.

Loe, kuidas inimesed tasuta äppidega oma isikuandmetele juurdepääsu võimaldavad.

- **Installimisõigus**

Kui minna Google Play või Apple Store’i rakenduste poodi ja mõni rakendus alla laadida, siis küsib äpp nii nutiseadmele kui ka andmete ligipääsule õigusi. Enne ei saa rakendust isegi installida. Näiteks kui laadida alla fotorakendus, tuleb lubada sellel oma kaamerat kasutada. Sama kehtib satelliitnavigatsioonirakenduste kohta, mis vajavad juurdepääsu nutiseadme GPS-i signaalile. Aga mis siis, kui laadida alla äratuskellarakendus, mis küsib luba saada juurdepääs fotodele, kaamerale ja mikrofonile? Kas on loogiline, et tasuta mängurakendus tahab juurdepääsu tekstidele ja kontaktiloendile? See peaks olema hoiatussignaal, mis annab märku, et allalaetav rakendus kasutab isikuandmeid, mis ei ole funktsiooni seisukohast üldse vajalikud. Nende õigustega saab rakenduse välja töötanud ettevõte saata need andmed rakenduse töötamise ajal oma serveritesse. Sellisel juhul tuleb sätted ja tingimused üle vaadata, enamasti võib sealt leida sellekohase väite.

- **Ligipääsuõigused**

Mitmesugused mobiilirakendused nõuavad ligipääsuõigusi, aga nende lubamine võib kaasa tuua oma andmete ja privaatsuse suuremal või vähemal määral loovutamise. Siin on välja toodud rakenduste kõige levinumad isikuandmete taotlused ja nende tähendused.

Telefon. Selle õigusega saavad rakendused helistada ja kõnesid vastu võtta. Mõne rakenduse puhul, nagu Skype, on see arusaadav. Aga kui sellist juurdepääsu küsib rakendus, millel ei ole telefonikõnedega mingit pistmist, peaks see muutma ettevaatlikuks.

SMS. See võimaldab rakendusel saata tekstsõnumeid. Pahatahtlikud rakendused võivad SMS-i kaudu tellimusi teha ja telefoniarveid suurendada. See õigus, nagu ka juurdepääs telefonile, tuleks anda rakendusele ainult sel juhul, kui äpp ja selle allikas on tõesti usaldusväärsed.

Fotod, meediumid, mälukaart. Kui anda rakendusele need õigused, pääseb see juurde seadme mälule ja saab andmeid lugeda, muuta ning kustutada. See on vajalik pilvtalletuse või failide ühiskasutuse rakendustele, nagu Google Drive või Evernote, aga üldiselt küsivad paljud mobiilirakendused seda õigust selleks, et telefoni seadeid enda tarbeks salvestada. Internetipääs on samuti vajalik vaid veebi või pilvtalletusruumi failide üleslaadimiseks, mitte teiste rakenduste jaoks.

Kontaktid. See lubab rakendusel pääseda juurde seadmesse salvestatud kontaktandmetele. Sellised rakendused, nagu WhatsApp või Skype, aadressiraamatud ja sotsiaalmeediavõrgustikud vajavad seda juurdepääsu, aga muude rakenduste jaoks on see üldjuhul tarbetu.

Seadme ja rakenduste ajalugu. Selle õiguse abil saab rakendus reaalajas jälgida nutitelefoni kasutustoiminguid. See võib-olla vajalik, et programmiviga ja veateateid arendajatele saata.

Asukoht. Sellised navigeerimis- ja asukohapõhised rakendused, nagu Google Maps ning Uber vajavad oma teenuste osutamiseks juurdepääsu teie GPS-i asukohale. Saadetud andmetest saab moodustada liikumisprofiile, mis näitavad täpselt, kus te konkreetsel hetkel olete olnud. Kui järele mõelda, teeb see veidi kõhedaks. Kindlasti ei vaja asukohaluba kõik mobiilirakendused.

Identiteet. See võimaldab rakendustel tuvastada, millised kasutajakontod on seadmes olemas ja kuidas need on ühendatud. Selle õigusega rakendustel on lubatud lugeda ja muuta inimese kontaktikaarti, mis tavaliselt hõlmab telefoninumbrit ja pilti.

Kaamera, mikrofon. Ehkki see on nõutav enamiku sotsiaalmeediarakenduste, näiteks Snapchati ja Instagrami puhul, ei ole see kindlasti vajalik kõigi rakenduste puhul. Tuleks kindlasti järele mõelda, mida installida – kahjurrakendused võivad kasutada neid õigusi, et salaja luurata.

„Väga tähtis on lugeda enne rakenduse installimist, milliseid volitusi ja õigusi täpselt küsitakse. Kui need tunduvad ülemäärastena, tuleks valida muu rakendus. Pärast installimist saab installitud rakenduste küsitud õigusi vaadata rakenduste haldurist, näiteks kui kasutate WhatsAppi, siis vaadake selle pikka õiguste loendit," ütles Aron. Ta lisas, et igal juhul tasub olla ettevaatlik ja jälgida, et rakendus pärineks ametlikust rakenduste poest, nagu Google Play või iTunes.

- Uudised

- Androidiblog
- Mobiiltelefonid
- Tarkvara
- Turvalisus

Pilt


iTunes Store
Yelp
Instagram
Phoster
Facebook
Twitter