Ekspert: mobiiltelefonide turvalisuses on toimunud revolutsiooniline areng

12. oktoober 2020 - 10:16 Autor: Vitali Donskoi

Äristatistika platvormi Statista andmetel leiti ainuüksi selle aasta esimeses kvartalis mobiilseadmetest umbes 1,2 miljonit pahavara paketti. Seadmete turvalisuse tagamine on täna prioriteediks kõigile mobiiltelefonide tootjatele, sest nii nagu areneb nutiseadmete tehnoloogia ja selle kasutamise võimalused, muutuvad üha targemaks ka need, kes telefonides leiduvaid isikuandmeid kurjasti ära soovivad kasutada.

Kui paarkümmend aastat tagasi kaitses andmeid mobiiltelefonides ainult SIM-kaardi PIN-kood ning telefoni tootjast olenev klahvistike kombinatsioon, siis tänaseks on isikuandmete kaitsmiseks kasutusel väga erinevad meetodid nagu biomeetrilised lukud, erinevad autentimise viisid ja rakendusepoe turvasüsteemid. Ent seejuures on oluline ka iga inimese vastutus ja teadlikkus enda isikuandmete kaitsmisel.

Üks kood kehtis kõigile

2000ndate alguses kasutusel olnud mobiilide lukustussüsteeme, kus telefoni avamiseks tuli olenevalt tootjast vajutada kõigile teadaolevaid klahvikombinatsioone, on raske nimetada telefoni või andmete kaitsmiseks. Lukustamise ja avamise klahvikombinatsioon oli siis vajalik vaid juhuslike klahvivajutuste ehk kogemata väljaminevate kõnede või ilma tähenduseta tekstisõnumite vältimiseks.

Ainus mõistlik telefoni turvaelement sel ajal oli SIM-kaardi PIN-kood, mida tuli sisestada iga kord, kui telefon sisse lülitati. Seega ei kujutanud kadunud või tühjaks saanud seade koos täiendavalt blokeeritud kaardiga tavaliselt isikuandmetele ohtu. Samas tuleb meeles pidada, et tol ajal oli inimestel telefonides oluliselt vähem teavet – telefoninumbrid, tekstsõnumid ja kõnelogi, kuid muud isiklikku infot seadmetes polnud.

Lukustuskuva tõstis andmete kaitsmise uuele tasemele

Koos nutitelefonide tulekuga said populaarseks turvalisust tõstvad ekraanilukud, mis olenevalt tootjast seisnes näiteks personaalses PIN-koodis või sõrmega ekraanil koodimustri libistamises. Iga kasutaja lõi lukustamise kombinatsiooni ise vastavalt enda loogikale, kuid kuna neid kombinatsioone oli siiski võimalik ära arvata või jälitada, polnud endiselt tegemist väga turvalise lahendusega.

Tehnoloogia arenedes tekkis kasutajal võimalus kaitsta oma telefoni biomeetriliste andmete, näiteks sõrmejälgede või näotuvastuse abil. See oli oluline samm edasi isikuandmete turvalisuses, sest biomeetriliste andmelukkude ilmumisega telefonidesse sissehäkkimise võimalus sisuliselt kadus. Siin on heaks näiteks Huawei telefonid, mille puhul võeti lisaks kasutusele ka eraldi seadme mälu, kuhu hakati salvestama kasutaja biomeetrilisi andmeid.

Tänu sellele ei saanud telefoni ilma kasutaja teadmata sisse häkkida, seda muuta ega varastada.

Rakendusepoed – uus turvaauk nutitelefonide kasutajatele

Nutitelefonidega kaasnenud rakendusepoodide kasutusele võtmine ja nende üha kasvav populaarsus tõi kaasa uue turvariski. Tänu sellele tekkis võimalus telefoniomaniku andmetele ligipääsemiseks mitte ainult ekraani avades, vaid ka sisemiste süsteemide ja kaugjuhtimise teel.

Tänapäevaste standardite järgi ei olnud esimestel rakendusepoodidel peaaegu ühtegi turvaelementi. Seetõttu oli suur oht pahatahtlike rakenduste allalaadimiseks, seadme nakatamiseks või häkkeritele tahtmatult juurdepääsu andmiseks isikuandmetele ja muudele tundlikele andmetele.

IT-ettevõtte Cisco poolt hiljuti läbiviidud uuring näitas, et 84% inimestest tunneb erilist muret oma andmete turvalisuse pärast ning nad soovivad suuremat kontrolli oma teabehalduse üle. Nii rakendusepoodide arendajate kui ka tarbijate jaoks on poodide turvalisusest saanud esmane prioriteet.

Näiteks Huawei AppGallery rakenduste poe ehitamisel on loodud neljatasandiline turvaprotsess. Kõigepealt tuvastatakse ja kontrollitakse arendajate identiteeti, seejärel analüüsitakse, kas rakendused on loodud pahatahtlike toimingute tegemiseks. Siis tehakse privaatsusanalüüs ja kontrollitakse, millistele andmetele rakendused juurdepääsu vajavad, ning lõpuks testivad meie spetsialistid kõiki poe tooteid käsitsi. Nii saame olla kindlad, et kasutajad laevad AppGallery poest alla ainult turvalisi rakendusi. Ainuüksi eelmisel aastal lükkas AppGallery tagasi umbes 37% rakendustest, kuna need ei vastanud turvanõuetele.

Turvalisuse eest vastutab ka iga kasutaja ise

Suhtlusvõrgustike ja Interneti ajastul, kui kasutajatel on telefonis kogu enda kohta käiv teave, pole vähem oluline kasutajate enda teadlikkus ja vastutus. Seetõttu töötatakse välja spetsiaalseid turvasüsteeme, mis võimaldaksid tarbijatel oma teavet kaitsta.

Lisaks juba laialdaselt kasutatavatele biomeetriliste andmetega turbelahendustele on üks kasulikumaid vahendeid täna kaheastmeline autentimine (2FA). Protsessi esimese sammuna tuleb sisestada kasutajale teadaolevad andmed, näiteks kasutajanimi ja parool, seejärel genereeritakse teise etapina kasutajale juhuslik ühekordne kood. Isegi kui petturid arvavad ära esimese sammu andmed, välistab kolmandate osapoolte juurdepääsu teabele teine □□samm, kus juhusliku sisselogimiskoodi saab sätestada ja enda kontole juurdepääsu võimaldada ainult kontoomanik ise.

Statista andmetel oli 2018. aastal globaalse küberturvalisuse kui teenuse turu väärtus 5,9 miljardi eurot, 2023. aastaks ulatub see nende hinnangul juba enam kui 210 miljardi euroni. Selline kasv tõestab ilmekalt teema olulisust ja näitab, et tegemist on valdkonnaga, kuhu globaalselt aina enam panustatakse. Tarbijate teadlikkus õigete valikute tegemisel on siin aga võtmetähtsusega.

VITALI DONSKOI
Huawei Mobile Service äriarenduse juht

- Lahendused
- Turvalisus