Ekspert hoiatab: mobiiltelefonides käib ohtlikult vilgas elu

7 aastat tagasi - 30.05.2019 Autor: Taavi Talve

Mobiilne mugavus ei tohiks muutuda ettevõtte äririskiks, ent just nii on see läinud. Kui arvutites olevate andmete kaitsmisega nähakse tulist vaeva, siis mobiilide näol jääb uks küberkuritegevusele sageli pärani avatuks. Oleks ekslik arvata, et kurjategijad selle võimaluse kasutamata jätavad, kirjutab Telia IT-teenuste juht Taavi Talve.

Rahvusvahelise statistikaportaali Statista andmetel kasvab nutitelefoni kasutajate arv 2019. aastal maailmas 2,5 miljardini. Eestis osteti ainuüksi mullu ligi 400 000 uut mobiiltelefoni, millest iseenesest mõistetavalt moodustasid lõviosa nutitelefonid. Selline kasv on omakorda toonud kaasa muutuse kübermaailma tumedamates nurgatagustes – statistika kinnitab, et rünnakud on muutunud targemaks ning mobiilid on saanud oluliseks sihtmärgiks, mille kaudu väärtuslike andmeteni pahatahtlikel eesmärkidel jõuda püütakse.

Tuues vaid paar näidet, siis mullu pälvis ülemaailmse tähelepanu pahavara AdultSwine, mis oli peidetud lastele mõeldud mängurakendustesse. Selliseid rakendusi kasutades avanesid suvalisel hetkel telefonides pornograafilise sisuga reklaamid ning anti kasutajatele märku, et nad laeksid alla viirusetõrje või jagaksid oma telefoninumbrit. Ainuüksi nimetatud pahavara jõuti nakatatud mängude kujul maailmas alla laadida ligi seitse miljonit korda. Septembrist meenub aga Suurbritannia lennufirmat British Airways tabanud ulatuslik andmevargus, mille käigus sattusid häkkerirünnakus ohtu ettevõtte mobiilirakendust kasutanud ligi 400 000 kliendi isiklikud- ja finantsandmed.

Selliseid näiteid võib viimasest aastast tuua tegelikult kümneid, kui mitte sadu. Julgen kinnitada, et eestlaslik lootus, et minuga midagi ei juhtu, pole enam ammu parim turvastrateegia. Kui inimene arvab, et teda pole küberrünnatud, siis pole ta lihtsalt piisavalt otsinud. Küberturvalisusega tegeleva ettevõtte Check Point mobiilse turvalisuse spetsialistid on aastaid uurinud üle maailma erinevate ettevõtete andmeid ning jõudsid juba 2017. aastal järelduseni, et igat ettevõtet rünnati mobiili kaudu aasta jooksul vähemalt korra. Infoturbega tegeleva Kaspersky Lab'i andmetel kasvas 2018. aastal mobiilse pahavara rünnakute arv aasta varasemaga võrreldes koguni kaks korda.

Kuivõrd suur osa inimesi kannab igapäevaselt taskus oleva nutiseadmega kaasas tohutut hulka isiklikke kui ka tööandja tundlikke andmeid, siis peaks töötajate mobiilide turvalisuse tagamine olema iga ettevõtja oluline prioriteet. Rääkimata inimestest endist, kes võiksid rohkem huvi ja muret tunda, mis nende taskus olevas seadmes päriselt toimub. Paraku toimub suure tõenäosusega tegelik muutus eestlaste ohutajus alles siis, kui näeme esimesi tõsiseid rünnakuid, mille tulemusel mõni kohalik ettevõte peab uksed sulgema, kannatajatele suuri summasid korvama või kui moraalset ning rahalist kahju kannavad tuhanded eestlased.

Kes seda aega käed rüpes ootama jääda ei taha, võiks esmalt veenduda selles, et:

- Telefonis kasutatav tarkvara oleks uuendatud ning sisse oleks lülitatud automaatsed turvauuendused.
- Rakendusi ehk äppe laetaks alla vaid ametlikest kanalitest (Google Play Store, Apple App Store ja Microsoft Store) ning rakenduste alla laadimisel tutvutakse ka arendaja lisainfo ning kasutajate varasema tagasisidega.
- Regulaarselt kontrollitakse rakenduste privaatsussätteid ning seda, millistele andmetele need telefonis ligi pääsevad.
- Telefonis olevate andmete kaitseks kasutataks minimaalselt klahvilukku, näo- või sõrmejälje tuvastust, aga veelgi olulisem, viirusetõrjet.
- Tundmatute kirjade, sõnumite, linkide ja manuste avamisest hoidutakse ka telefonides.
- Avalike WiFi-võrkude asemel kasutatakse turvalisi VPN-ühendusi, mis takistavad võõrastel andmetele ligipääsu.
- Telefoni seadete alt oleks kogu selle sisu krüpteeritud ning varundatud.

- Lahendused

- Androidiblog
- Mobiiltelefonid
- Turvalisus

Pilt


20:43
20:43
Th 2, 1 thg 1
Lịch
Đồng hồ
Thời tiết
Cài đặt
Ảnh
Cửa hàng Play
Google
Công cụ