Pahavara tõttu võib nutitelefon hakata ise helistama ja sõnumeid saatma

9 aastat tagasi - 24.05.2017 Autor: AM

Kuigi Eestis pole nutitelefonide nakatumine pahavaraga massiline probleem, võiks seadmete kasutajad olla siiski teadlikud internetis varitsevatest ohtudest, näiteks sellest, et nutitelefon võib pahavara tõttu ise helistama või sõnumeid saatma hakata.

Nokia nutiturvalisuse raporti kohaselt üritati pahalaste poolt 2016. aasta esimeses pooles maailmas nakatada koguni 74% Androidi nutiseadmetest. Kui paljudel juhtudel see õnnestus, pole teada, kuid raporti hinnangul on maailmas nakatunud keskmiselt üks nutiseade 120-st. Kui seda raportit uskuda, võib Eestis igapäevaselt kasutuses olevast ligi miljonist nutiseadmest olla erineva pahavaraga nakatunud *ca* 8000 seadet. See on Paide linna jagu inimesi.

Selle aasta alguses avaldas Riigi Infosüsteemi Amet (RIA) küberturvalisuse teenistuse ehk CERT Eesti 2016. aasta kokkuvõtte. Eraldi juhitakse raportis tähelepanu mobiiliseadmete turvanõrkuste ja nuhkvara teemale. RIA teatel avaldas 2016. aasta novembris küberturvalisuse ettevõte Kryptowire teate Androidi mobiiliseadmete ADUPS turvaveast, mis seab ohtu väga paljude seadme kasutajate teabe konfidentsiaalsuse. Ettevõte tuvastas Androidi operatsioonisüsteemis pahavara, mis saadab kolmandate isikute serveritesse personaalset ja tundlikku kasutajainfot nagu kõnelogid ja lühisõnumite sisu. Mainitud haavatavusega seadmeid oli maailmas toonase hinnangu järgi pea 700 miljonit ning enam kui 200 riigis.

Turvaintsidentidega tegelev CERT Eesti tegi kindlaks, et ka Eestis oli arvukalt selliseid seadmeid, mis tihedalt suhtlevad kasutajatelt konfidentsiaalset teavet koguvate serveritega. Ainuüksi Kryptowire avaldatud artiklis mainitud BLU telefone on Eestis teadaolevalt kasutusel tuhandeid. Siiski ei ole probleem mitte telefoni tootjas, vaid operatsioonisüsteemi ADUPS konkreetses tootes (FOTA ehk Firmware on the Air). Operatsioonisüsteemi tootja oli eelmisel aastal nimetatud turvanõrkusest teadlik ning väljastas ka ADUPS FOTA järgmise versiooni, kus väidetavalt sai viga parandatud.

Telia Eesti turvaintsidentide valdkonnajuhi Aare Kirna sõnul on Eestis turvateadlikkuse tase kindlasti kõrgem kui maailmas keskmiselt, kuid sellest

hoolimata võib nutitelefoni kasutaja „komistada“ mõne pahavara otsa. „Tundmatute linkide avamine nutitelefonis on sama riskantne kui arvutis. Kui näiteks klikkida mõnel modifitseeritud lingil, võib telefon hakata pahavara tõttu kasutaja teadmata tegema kõnesid ja saatma SMS-e tasulistele välismaistele numbritele. See on korraliku väljamineku oht.“

Eraldi tasub tähelepanu juhtida laste ja noorte turvalisele netikäitumisele. Aeg-ajalt jõuavad ka avalikkuseni juhtumid, kus vanemad on kimpus üllatusarvetega, mis tekkinud lapse poolt kasutatud või ostetud tasulistest mängudest ning rakendustest.

„Selle vältimiseks on täna olemas turvalahendused – näiteks Telia SAFE, mis võimaldab blokeerida ebasoovitavat, tasulist ning eale mittevastavat sisu,“ tõi Kirna näite.

Telia Eesti lisaväärtusteenuste valdkonnajuht Maksim Melamed tõdes, et hetkel ongi üha enam hoogu sisse saamas trend, kus arvutite-sülearvutite kaitsmise kõrval pööratakse üha enam tähelepanu ka teiste nutiseadmete (telefonid, tahvelarvutid) turvamisele.

„Turbefirma F-Secure poolt loodud Telia SAFE turvalahendust kasutatakse täna kokku enam kui 13 500 seadmes, millest nutiseadmed moodustavad ligi 20%.“

- Uudised

- Androidiblog
- Mobiiltelefonid
- Turvalisus

Pilt

