Sinu tolmuimeja on ohus! Mida toob aasta 2020 küberturvalisuses?

1. detsember 2019 - 13:59 Autor: AM

Nutiseadmete maailmas läheb enda kaitsmine aina keerulisemaks ja ründajad aina targemaks. Samsungi mobiilidivisjoni juht Antti Aasma kirjeldab järgmise aasta mobiiliturvalisusega seotud trende ning annab nõu, kuidas end küberrünnakute eest kaitsta.

Aasma sõnul muutub mobiiltelefon järgmisel aastal maailmas kõige olulisemaks vahendiks, mille kaudu küberkurjategijad oma rünnakuid ellu viivad. Iga inimene peaks hoolikalt järele mõtlema, milliste seadmetega on tema mobiiltelefon ühendatud, kuna just nende nõrga turvalisuse tõttu pääsetakse ligi mobiilidele ja sealt edasi inimese väärtuslikele andmetele. Seega kui olete ostnud uue robottolmuimeja, nutikülmkapi või kasutate kodus nutikaid valgus- ja temperatuuriandureid, mida on võimalik mobiiliga juhtida, siis tasub üle vaadata, milliste vahenditega on need kaitstud.

“Kodused WiFi ruuterid on tavaliselt rahuldaval tasemel turvatud, ent võrku ühendatud seadmete kaudu võib küberpätt neile hõlpsasti ligipääsu saada ning siis juba omapead edasi toimetada. Seega tasub üle kontrollida, millised õigused on koduseadmetele antud ning kas neid annaks kuidagi paremini turvata,” soovitab Aasma.

“Võib tunduda kauge probleemina, ent turvamata võrkude ja seadmete otsinguil küberkurjategijaid liigub ringi aina rohkem ning järgmisel aastal suureneb oodatavate rünnakute arv kindlasti,” lisas Aasma.

Asjade internet muutub järk-järgult levinumaks igas kodus, aga samuti ka erinevates eluvaldkondades. 2020. aastal on oodata tarkade seadmete leviku kasvu meditsiinis. Seega avarduvad võimalused ajaga veelgi, ulatudes nutikodust kuni südamestimulaatorite, insuliinipumpade ja astmamonitorideni.

Õngitsemine jääb endiselt levinuimaks tegevuseks

2020. aastal jääb Aasma sõnul endiselt suurimaks küberrünnakute meetodiks õngitsemine ehk kavalate linkide, petukirjade ja muudetud sisu abil inimese manipuleerimine oma isiklike andmete, näiteks pangakonto paroolide, avaldamiseks. Kui andmed on kaaperdatud, nõutakse nende tagastamise eest lunaraha või asutakse andmeid ära kasutades kurja korda saatma.

“Igas sajas meilis on keskeltläbi üks taoline kiri, millega proovitakse inimese isiklikele andmetele ligi pääseda. Neid tuleks kindlasti ignoreerida ning mitte klikkida linkidele, milles ei olda sada protsenti kindlad,” rääkis Aasma. “Samuti peaks ettevaatlik olema äppidega ja selliste alla laaditavate failide käivitamisega, mis ei ole pärit ametlikest rakenduste poodidest.”

Tähelepanelik tuleb olla ka veebilehti külastades. Kui veebibrauseri aadressiribal kõige ees olev SSL-protokolli tähistav tabalukk on siiani tähendanud, et veebisait on turvaline, siis enam ei pruugi see nii olla. Aina rohkem levivad kalastusskeemid, kus veebilehel on ees kena rohelist värvi tabalukk ning eesliide https, kuid sait sisaldab pahavara, mis annab pättidele õiguse teie süsteemis tegutseda.

“Kõige parem nõuanne sellistel juhtudel on olla valvas ning kontrollida väga täpselt, millisele lehele läksite – kas aadress oli korrektselt sisestatud ning mida leht nõuab. Kui keegi hakkab ilma põhjuseta küsima teie salasõnu või krediitkaardi numbreid, on ilmselt juba tegu pettusega,” kommenteeris Aasma.

Üha levinumaks muutuvad ka iga inimese jaoks personaalselt disainitud rünnakud, mida on raskem läbi hammustada. Sotsiaalmeediast on

võimalik üsna lihtsalt järeldada, kas inimesele meeldivad kassid, suusatamine või eksootilised reisid. Juba selle teabe abil on võimalik lihtsalt genereerida kuritahtlikke ja meelitavaid lehekülgi, mänge või SMSe, milles leiduvale infole reageerimine ei pruugi lõppeda hästi.

Ohud varitsevad ka ettevõtteid ja valitsusi

Pahavaravastase tarkvara arendanud firma Malwarebytes uuring näitab, et lisaks üksikisikutele suunavad küberpätid aina enam tähelepanu organisatsioonidele ja seal on rünnakute kasv isegi suurem. Nende andmete kohaselt kasvas organisatsioonidele suunatud rünnakute arv 2019. aasta esimeses kvartalis võrreldes varasema aastaga kaks korda.

”Lisaks toob uuring välja, et kaitstud ei ole ka valitsusasutused. On selge, et kurjategijad on aru saanud, et suured rahad liiguvad ettevõtetes ja üksikisikutelt on võimalik vaid pisut andmeid või raha saada. Seetõttu on oluline mõelda turvalisele käitumisele aina enam ka ettevõtetes ja kasutada selleks spetsiaalselt mõeldud lahendusi. Näiteks Knox turvasüsteemi, mis hoiab telefonis olevaid tööandmeid eraldi turvatud kaustas,” selgitas Aasma.

- Uudised

- Kodumasinad
- Mobiiltelefonid
- Robotid
- Turvalisus