CERT-EE juht küberturvalisuse ohtudest: tulevikus on ilmselt keeruline leida koduseadet, mis poleks internetti ühendatud

1. aprill 2019 - 13:22 Autor: AM

Riigi Infosüsteemi Ameti küberintsidentide käsitlemise osakonna CERT-EE juht Tõnu Tammer rääkis möödunud neljapäeval toimunud Samsungi küberkaitseseminaril, et internetti ühendatud seadmete arvu aina suurema kasvu tõttu tekib kübermaailma ka rohkem ohte, millega tuleb tegeleda.

„Praegu elab maailmas üle 7 miljardi inimese ja internetti ühendatud seadmeid on nende inimeste kasutuses ligikaudu 23 miljardit. See teeb keskmiselt kolm seadet inimese kohta. Vaadates tulevikku, siis on näha, et nende seadmete arv aina kasvab ning võib eeldada, et 5 aasta pärast on neid seadmed veel 3 korda rohkem. Kuna aga praeguse seisuga nende vidinate küberkaitsele kohati eriti ei mõelda, siis tekib seadmete arvu kasvuga ka aina rohkem kohti, mille kaudu küberpätid võivad kasutaja koduvõrku pääseda," rääkis Tammer.

Olukorra näitlikustamiseks tõi Tammer paralleeli 20. sajandi algusega, kus inimesel oli poodi minnes mikserit valides kaks valikut – käsitsi ja elektril toimiv mikser. Tänapäeval on aga sisuliselt võimatu leida mikserit, mis ei töötaks elektriga. Tulevikus leiab ilmselt aset sama muutus internetti ühendatud seadmetega, kus keeruline on leida koduseadet, mis poleks internetti ühendatud.

Lisaks tekib tohutu seadmete arvu tõttu ka suur nõudlus küberkaitse valdkonnas tegelevate töötajate järele ning hinnanguliselt on 2021. aastaks globaalselt täitmata 3,5 miljonit küberkaitsega seotud ametikohta.

Osana lahendusest näeb Tammer praktikat, kus tootjad panustaksid aktiivsemalt turvauuenduste tegemisse seadmetes. „Näiteks selle asemel, et anda kasutajale valik, kas teha tarkvarauuendus või mitte, võiks tal olla valik, et uuendus on vaja teha ning kasutaja saab ise valida, millal järgneva 24 tunni jooksul ta seda teha soovib," selgitas Tammer.

Lisaks tõi Tammer esitluses välja, et inimesed võivad teinekord olla tarkvarauuenduste vastu, kuna see võib kaasa tuua uue vea süsteemis. Samas ei tohiks Tammeri sõnul jääda vaid seetõttu turvauuendus tegemata, kuna vaatamata võimalikule veale on tarkvaras lapitud need turvaaugud, millest küberpahalased juba teadlikud on.

„Jah, vastab tõele, et uue tarkvara paigaldamisel võib sellega kaasneda vigu või isegi turvaauke, kuid nende turvaaukude jaoks ei ole pahalased veel ründeviisi välja töötanud, seega on kasutaja uue tarkvaraga ikkagi turvalisemas seisus, kui vana tarkvara kasutades,“ ütles ta.

Tegijad
Uudised
Turvalisus