Uksed lukus? Võrguseadmed ka? Netis koduseadmed võivad ettevaatamatusest luua koju ohtliku turvaaugu

28. Mai 2018 - 22:45 Autor: AM

Küberturvalisus on praegu olulisem kui kunagi varem ning sellepärast levib ka palju nõuandeid selles osas, kuidas enda arvutit, telefoni või kasutajaid erinevates teenustes edukalt kaitsta.
Samsung Eesti koduseadmete tootekoolitaja German Baranovi sõnul on meie kodudes palju internetiga ühendatud seadmeid, mis võivad teinekord kodu turvalisust tagades meelest minna. Seega on oluline teada, kuidas muuta turvaliseks ka teisi seadmeid lisaks telefonile. Näiteks internetiga ühendatud telerit, valgustit, turvakaamerat või tolmuimejat.

Oma ülevaadet

„Enne korraliku küberhügieeni läbiviimist kodus tuleb kõigepealt saada põhjalik ülevaade, millised seadmed on kodusesse internetivõrku ühendatud. Kuna täna on inimestel tihtipeale palju erinevaid seadmeid, siis on võimalik, et mõned seadmed võivad meelest ära minna," rääkis Baranov.

Hea viis kodusesse võrku ühendatud seadmetest ülevaate saamiseks on telefonirakendus Fing, mis on tasuta saadaval nii Androidi kui iOSi operatsioonisüsteemidele. Peale rakenduse allalaadimist tuleb telefon ühendada kodusesse WiFi võrku ning seejärel avada rakendus. Järgnevalt on kasutajal kohe näha ülevaade seadmetest, mis tema koduse võrguga on ühendatud.

Kaitse parooliga kõik seadmed

Üldiselt toimib internetiga ühendatud seadmete koju paigaldamine nii, et peale paika sättimist tuleb endale luua kasutaja, kuid kõik seadmed ei pruugi seda nõuda. Sellest tulenevalt on väga oluline, et kõik seadmed oleksid parooliga kaitstud. Kõige lihtsam viis seda tagada on uurida iga internetiga ühendatud seadme kasutusjuhendit ning selgitada, millised on konkreetse seadme puhul võimalusel selle kaitsmiseks.

„Üheks näiteks ohust, mis puudulike paroolide tõttu võib tekkida, on kodused WiFi-turvakaamerad, kus parool on hooletusest või teadmatusest muutmata jäänud. Sellised seadmed on kergeks saagiks küberpättidele ning olukorra muudab eriti ebameeldivaks see, et kasutajat on võimalik reaalajas video vahendusel jälgida," ütles Baranov.

Mitu kodust võrku

Hea viis internetti ühendatud seadmete turvalisuse tõstmiseks on luua neile eraldi WiFi võrk ning kaitsta see põhivõrgust erineva parooliga. Soovi korral võib kaaluda ka mitme võrgu loomist. Siis saab näiteks valgustid ja kaamerad ühendada ühte ning nutikõlarid ja teleka teise võrku.

Sellisel juhul ei lange kõik kodused seadmed rünnaku korral pätile saagiks. Siinkohal on range reegel, et iga võrgu parool peab olema erinev ning maksimaalselt keeruline. Neid võrke võib vaadata kui kasutajaid internetis – kui rakendad kõigi kasutajate puhul sama parooli, siis on ühe parooli arvamisel pätil koheselt ligipääs kõigile teistele kasutajatele. Kui paroolid on erinevad, siis vaid ühele.

Kaitse kõige olulisemaid seadmeid

Koduseadmete turvalisusele mõeldes on oluline meeles pidada ka seda, et üldiselt on nende puhul üks seade, mille kaudu kõiki teisi masinaid mugavalt kontrollida – telefon. Seega lisaks iga individuaalse seadme kaitsele tuleb turvata ka telefoni. Selleks on mitmeid erinevaid viise. Näiteks tasub vältida avalikke WiFi võrke, kuhu võib ühenduda ükskõik kes ning mille turvalisus ei pruugi olla tagatud. Samuti tasub alati ära teha kõik tarkvarauuendused, mida telefon kasutajale soovitab. Lisaks telefoni uuendustele tasub end hoida kursis ka teiste koduseadmete turvauuendustega ning need alati ära teha.

„Näiteks Samsungi telefonidel on selleks puhuks paigaldatud Knox turvasüsteem, mis lubab paigutada tundlikud failid telefonis spetsiaalsesse kausta, mida on vaja eriti turvalisena hoida. Samuti kasutab süsteem VPN-lahendust, mis turvab telefoni ebaturvaliste WiFi võrkude ja pahatahtliku koodi eest. Lisaks telefonidele on Knox turvasüsteem olemas ka näiteks käesoleva aasta QLED teleritel, kus süsteemi eesmärgiks on muuhulgas tuvastada pahatahtlikke rakendusi ning takistada andmevargust," selgitas Baranov.

Vali turvalised seadmed

Koduste seadmete valimise puhul tasub eelistada ettevõtteid, kes on tuntud eduka andmekaitse poolest. Seega enne iga seadme soetamist tasub teha kiire otsing seadme ning selle küberturvalisuse kohta.

„Silmipimestavalt odava hinnaga nutikad kodukaamerad või kõlarid välismaa internetipoodides võivad tunduda ahvatlevad, kuid tihtipeale võib odava hinna taga peituda asjaolu, et seadme arendamisel ei ole küberturbesse palju ressurssi panustatud," ütles Baranov.

- Uudised

- Andmeside
- Androidiblog
- Mobiiltelefonid
- Võrguseadmed