Miks on koju vaja tervelt kolme WiFi-võrku?

4 kuud tagasi - 07.07.2026 Autor: AM

Pealtnäha süütu soodne tehnikavidin võib avada küberpättidele kodu digitaalse esiukse. Telia küberturbe lahenduste arhitekti Kristjan Aljase sõnul kipuvad inimesed nutividinate puhul vaatama eelkõige hinnasilti, jättes odava tootega kaasnevad riskid tagaplaanile.

„Paljud nutiseadmed on tehtud võimalikult lihtsasti kasutatavaks, kuid turvafunktsioonid on sageli täiesti puudu, sest kaitsemeetmed muudavad kasutamise keeruliseks ja vähendavad müüki," räägib ta.

Mida see praktikas tähendab?

Näiteks võib koduvõrku ühendatud väline kõvaketas paisata sinu isiklikud fotod automaatselt kättesaadavaks igale teisele samas võrgus olevale seadmele.

Veelgi kõhedam on mõelda, et soodsast turvakaamerast võib sinu kodul või suvilal silma peal hoida lisaks sulle endale ka keegi kolmas, kes seda infot kurjasti ära kasutab.

Laste külalised ja küberrünnakute *zombie*d

Küberrünnakute statistika maalib üha murelikuma pildi: paljud koduarvutid on omaniku teadmata nakatunud ja muudetud osaks suuremast küberrünnakute võrgustikust. Selline nakatumine toimub aga hirmutavalt lihtsalt just läbi ühise WiFi-võrgu, kuhu on ühendatud kõik kodu kaitseta nutiseadmed ja mida kasutavad ka külalised.

Ühise, kõikehõlmava WiFi parooli jagamine on nagu kortermaja välisukse koodi kleepimine teadetetahvlile. Aljas toob siinkohal välja väga elulise näite: „On tavaline, et kortermajas käivad lapsed üksteisel külas ja jagavad WiFi paroole sõpradega, mis tähendab, et sinu WiFi-le võib lõpuks olla ligipääs poolel majal. Tegelikult ei tohiks koduseid WiFi andmeid niimoodi maailmaga jagada. Isegi mitte koju kutsutud tehnikule."

Lahendus: jaga oma koduvõrk kolmeks

Kuidas siis kaitsta oma väärtuslikke faile, tööarvutit ja privaatsust? Lahendus ei peitu nutiseadmete ära viskamises, vaid nende isoleerimises.

Küberhügieeni kuldreegel näeb ette, et kodus võiks olla loodud kolm eraldi WiFi-võrku.

1. **Põhivõrk:** sinu ja su pere arvutite, tööseadmete ning nutitelefonide jaoks (kus liiguvad pangaparoolid ja tööfailid).
2. **Nutivõrk (IoT)**: eraldi võrk nutipirnidele, robottolmuimejatele, kaameratele ja nutiteleritele.
3. **Külaliste võrk**: eraldatud võrk külalistele ja sõpradele, mis annab neile küll internetiühenduse, kuid ei lase piiluda sinu kodusesse sisevõrku.

„Kolm eri võrku tagab, et töö- ja isiklikud andmed on kaitstud isegi siis, kui mõni nutiseade nakatub või keegi üritab võrgus olevatele seadmetele ligi pääseda," selgitab Aljas ja tuletab meelde lisareeglit: seadmeid tuleb pidevalt uuendada. Tarkvarauuendused on nagu digitaalsed vaktsiinid, mis muudavad seadmed turvalisemaks ja panevad need tihti ka sujuvamalt tööle.

Kuidas seda tehniliselt teha?

Selleks on ekspertide hinnangul kaks peamist teed. Üks variant on ehitada süsteem füüsiliselt eraldi seadmetest – ühendades teenusepakkuja ruuteri külge eraldi WiFi-ruuterid, mis on seadistatud toimima iseseisvate võrkudena. Siin on kriitilise tähtsusega jälgida, et need käsitleksid algset ruuterit puhtalt välisvõrguna ning moodustaksid tõepoolest üksteisest isoleeritud saared.

Teine, oluliselt tänapäevasem lähenemine nõuab aga lihtsalt pisut nutikamat riistvara.

„Lihtsam ja sageli ka praktilisem lahendus on kasutada ruuterit, mis toetab mitme eraldiseisva WiFi-võrgu loomist. Nii saab näiteks kodused seadmed, külalised ja nutikodu seadmed paigutada erinevatesse võrkudesse, mis parandab nii turvalisust kui ka võrgu haldamise mugavust," räägib Aljas.

Seega, enne kui ühendad järgmise soodsa nutividina oma koduvõrku, tasub korraks aja maha võtta ja oma ruuteri seadistustele pilk peale visata.

- Lahendused

- Turvalisus
- Võrguseadmed

Pilt

