# RIA: Eestis on üle 3000 nakatunud nutiseadme, mida võidakse ära kasutada

6 kuud tagasi - 05.11.2025 Autor: AM

Riigi Infosüsteemi Amet (RIA) hoiatab, et Eestis on tuvastatud üle 3000 nakatunud nutiseadme – robottolmuimejatest ja valvekaameratest kuni külmikute ja teleriteni, mida kurjategijad võivad kasutada küberrünnakute läbiviimiseks. Enamik nakatunud seadmetest on vähetuntud tootjatelt.

RIA analüüsi- ja ennetusosakonna analüütiku Nikolai Kunitsõni sõnul on turul järjest enam niinimetatud *no-name* ehk vähe tuntud või tundmatute tootjate koduseadmeid, mille madal hind tuleb sageli kvaliteedi, turvalisuse ja kasutajatoe arvelt.

## BADBOX on liikvel

„Paljudel sellistel seadmetel puuduvad regulaarsed turvauuendused, mida suuremad ja tuntumad tootjad pakuvad sageli ka aastaid pärast seadme soetamist. Ilma nendeta muutuvad seadmed aja jooksul haavatavaks, sest teadaolevaid turvanõrkusi ei parandata. Samuti puudub tihti usaldusväärne kasutajatugi, mis tähendab, et probleemide korral pole kasutajal kuhugi pöörduda," selgitas Kunitsõn.

Veelgi tõsisem risk peitub seadmetesse paigaldatud tagaustes või pahavaras. „Need riskid pole teoreetilised – näiteks on maailmas levimas robotvõrgustik BADBOX 2.0, mis on Google'i andmetel nakatanud üle 10 miljoni seadme. RIA hinnangul on Eestis tuvastatud pea 3000 nakatanud nutiseadet, peamiselt digiboksi, mis võivad anda küberkurjateijatele ligipääsu seadmetele," märkis RIA analüütik.

Selliseid seadmeid saavad kurjategijad kasutada spämmi levitamiseks, rünnakute korraldamiseks, kasutajate andmete kogumiseks, pahavara jagamiseks ja veel paljuks muuks, milles seadmete omanikud tõenäoliselt luba pole andnud. „Tundmatu päritoluga seadmed võivad näiliselt pakkuda soodsat lahendust, kuid nende kasutamine võib tuua kaasa tõsiseid riske nii kasutaja andmete kui ka kogu võrgu turvalisusele," hoiatas Kunitsõn.

## Iga võrgus olev seade on potentsiaalne uks häkkerile

Ka seadmetootjad rõhutavad, et nutikate koduseadmete puhul peab turvalisus olema sisse ehitatud juba arendusetapis, mitte lisatud hiljem. „Targa kodu võlu seisneb selles, et seadmed kohanevad kasutajaga ja on lihtsad kasutada. Aga kui andmed pole kindlalt kaitstud, ei saa end kodus turvaliselt tunda," lisas Samsungi koolitusjuht Alari Pennar.

Pennari sõnul on uusimad koduseadmed – näiteks robottolmuimejad, mis varem kasutasid kaamerat vaid navigeerimiseks, kuid nüüd pakuvad ka kodu jälgimise funktsiooni – toonud kaasa täiesti uued nõuded andmete kaitsele. „Kui funktsioonid arenevad, kasvab ka andmete hulk ja tundlikkus, mida tuleb kaitsta. Samas peab turvasüsteem arenema samas tempos," märkis ta.

Tänaseks on fookus liikunud üksikute seadmete kaitsmiselt tervikliku süsteemi turvalisusele, kus kõik kodused nutiseadmed jagavad andmeid ja toimivad ühtses, krüpteeritud võrgus.

## Kuidas end kaitsta?

- Eelista tuntud tootjaid, kes pakuvad regulaarseid turvauuendusi ja kasutajatuge.
- Vaheta vaikimisi paroolid kohe pärast seadme kasutuselevõttu.
- Hoia seadme tarkvara ajakohasena – uuendused ei paranda vaid funktsioone, vaid ka turvaprobleeme.
- Kasuta turvalist Wi-Fi võrku ja väldi seadmete ühendamist avalikesse võrkudesse.
- Eemalda või lülita välja seadmed, mida enam ei kasuta.


- Uudised

- Kodumasinad
- Mobiiltelefonid
- Robotid
- Turvalisus


Pilt


14:21