Riigi valimisteenistusele

Märt Põder
sündinud 11.09.1979
elukohaga Jakobi 13-2, Tartu 51006
kontaktitav gafgaf@infoaed.ee

VALIMISKAEBUS RIIGIKOGU VALIMISTEL 2023

Vaidlustan süsteemi võtmepaari genereerimise usaldusväärsuse valimiste korraldaja poolt 15. veebruaril, kuna vaatlejatele ja audiitoritele ei antud vastavalt e-hääletamise käsiraamatus nõutule võimalust "veenduda, et süsteemis ei sisaldu pahavara, mis häälte avamise võtit salvestab või kasutab" [1].

Minu kui vaatleja palve peale selline võimalus tagada esialgu eirati palvet kommentaarideta 15. veebruaril ja sain alles 16. veebruari vaatlejakoolituse raames nõudmise peale selgituse, mille põhisisuks näis olevat väide, et pahavara puudumise tuvastamiseks piisab kasutatava kõvaketta pitseerimisprotseduuride visuaalsest vaatlusest ja pitseerimise tõttu ei saa andmed kettalt lekkida.

Sellised väited aga on eksitavad, sest esiteks võib olla pahavara kettale jõudnud juba enne pitseerimist ja esimest kasutamist ametlike valimisprotseduuride käigus. Kuna ketta vormindamise ja tarkvara paigaldamise vaatlemist pole ette nähtud, on võimalik pahavara olemasolu või puudumist elementaarsel tasemel tuvastada vaid kõvakettale juba paigaldatud opsüsteemi ja rakendustarkvara analüüsides.

Teiseks aga sisaldub neis väidetes ekslik eeldus, et pahavara eesmärk saab piirduda andmete lekitamisega kettalt – näiteks võib eelnevalt paigaldatud pahavara anda ette genereeritavate võtmete pähe varem ettevalmistatud võtmepaari, mis on n-ö lekkinud juba enne protseduuride algust ning simuleerida kogu protsessi üksnes kasutajaliideses. Lisaks ei ole põhjust piirata pahavara eeldatavat funktsionaalsust lekitamisega, vaid selle eesmärk võib olla manipuleerida võtmepaari genereerimist mõnel muul viisil, nt muutes krüptograafilisi parameetreid selle nõrgestamise eesmärgil.

Lisan kaebusele kuvatõmmised vaatlemiskeskkonnast, millel on näha mu esitatud palved ja ettepanek tagada kõvaketta tõmmisega tutvumisega mulle kui vaatlejale võimalus veenduda, et süsteemis ei sisaldu pahavara.

[1] https://www.valimised.ee/sites/default/files/2023-02/IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat.pdf (versioon 0.7 kuupäevast 13.02.2023, lk 5-6)