Riigikogu Kantselei riigi valimisteenistus

Euroopa parlamendi elektroonilise hääletuse toimingute audit

VAHEARUANNE II

Jaan Oruaas CISA, ISO27001 juhtaudiitor
Hillar Põldmaa, CISA, CISM

juuni 2024

Vastavalt FocusIT OÜ ja Riigikogu Kantselei riigi valimisteenistuse vahel 16. mail 2024 sõlmitud lepingule viis FocusIT OÜ läbi 2024. aasta Euroopa parlamendi valimiste elektroonilise hääletuse e-valimiskasti Riigi valimisteenistusele (RVT) üleandmisprotsessi, häälte avamise võtme kasutamise esmasel ja teisel lugemisel ning krüptograafilise segamise auditi.

Käesolev aruanne on EP e-hääletuse auditi teine vaheaudit.

1 Auditeeritavad toimingud

Juhindudes Riigikogu valimise seadusest ja audit ülesandest jälgisid audiitorid e-valimiste järgmisi tegevusi:
- e-valimiskasti sulgemine;
- e-valimiskasti üleandmine RVT-le;
- häälte avamise võtme kasutamine esmasel häälte lugemisel;
- häälte avamise võtme kasutamine teistkordsel lugemisel,
- häälte anonümiseerimine;
- häälte krüptograafiline segamine;
- häälte lugemine.

E-häälte lugemisel jälgisid audiitorid vastavalt kinnitatud ja avaldatud juhenditele, sealhulgas audiitoritele ja vaatlejatele edastatud juhendile IVXV: E-hääletamise käsiraamat Versioon 0.8[1] ja IVXV kogumisteenuse haldusjuhend[2].

Protsessi käigus kontrolliti:
- kas e-valmiskast suleti ja anti üle vastavalt juhenditele,
- kas töötlusprotsesse tehti juhendites ettenähtud ulatuses võrgust lahti ühendatud arvutites ja mälukettal. Kontrolliti arvuti BIOSi, väliste seadmetega WiFi ja Sinihamba ühenduste puudumist ning vaatlusega võimalike lisaseadmete puudumist;
- kas töötlusprotsessid tehti mälukettal;
- kas sisendite laadimine ja väljundite salvestamine tehti DVD-plaadil;
- kas sisendandmed, konfiguratsioonifailid ja väljundid olid kinnitud allkirjadega;
- kas toimingud logiti vastavalt nõuetele.

Protseduurideks kasutatud võtmeosakud kiipkaartidel ja süsteemiketas kaitsti turvakleebistega.

1.1 Koguja tegevused

Protsessi käigus jälgiti järgmisi tegevusi:
- e-valimiskastile juurdepääsu sulgemine ja teenuste sulgemine;
- valmistulemuste kontrollsumma arvutamine;
- valimistulemuste kopeerimine.

Kasutatud arvuti ja irdkandjad suleti audiitor juuresolekul turvakleebistega turvaümbrikutesse.

Valimistulemused anti RVT-le üle nõuetekohaselt irdkandjatel ja turvaümbrikutes. Andmekandjate transporti turvas politsei.

[1] https://www.valimised.ee/sites/default/files/2024-05/RVT%20Korraldus%20nr%2010%20lisa%20%28IVXV%20e-h%C3%A4%C3%A4letamise%20k%C3%A4siraamat%2008%29-1.pdf
[2] https://www.valimised.ee/sites/default/files/2024-05/RVT%20korraldus%20nr%2012%20lisa%20%28IVXV-kogumisteenuse%20haldusjuhend%29.pdf

1.2 e-valimisskasti vastuvõtmine

e-valimiskasti vastuvõtmisel RVT-s kontrolliti järgmist:

- üle antud e-valimiskasti ja logide sõnumilühendeid, mis olid allkirjastatud RIA esindaja poolt audiitori juuresolekul;
- registreerija poolt kogutud ajatempleid koos allkirjastatud sõnumilühendiga;
- e-valimiskasti ja ajatemplite kontrollsummade allkirjastajate sertifikaatide õigusust;
- üle antud andmete loetavust ja töödeldavust.

1.3 Häälte lugemine

Euroopa parlamendi valimiste elektrooniliste häälte lugemine toimus 9. mail 2024 Riigikogu hoones.

Võtmeosakute loomiseks e-valimiste ettevalmistamisel ja häälte lugemiseks kasutati ainult selleks otstarbeks komplekteeritud arvuteid. Arvutite soetamiseks on RVT-s koostatud juhend „Suure kaitsetarbega arvuti komplekteerimise kord“. Arvutite kasutamise riskid on hinnatud ning sellel alusel komplekteerimise peamisteks põhimõteteks on:
- hankida riistvara, mille juhtmevabade ühenduste loomiseks komponendid puuduvad või need on võimalik eemaldada;
- püsivara (BIOS) kontrollsummade kontroll, uuendamine usaldusväärsest allikast;
- kasutada maandatud metallkorpust signaalide summutamiseks;
- kahtluse korral teostada 3-nda osapoole audit riistvarale;
- tarkvara võtta ainult usaldusväärsest allikast, kontrollida sertifikaadi usaldusväärsust ja kontrollsummasid.

Häälte lugemiseks valmistati ette kontrollitud konfiguratsiooniga arvuti mäluketas.
Audiitorid jälgisid häälte lugemise käiku.
E-valimiskast avati viie privaatvõtme osakuga. Audiitor tuvastas eelnevalt, et kõigi osalenud võtmeosakute kiipkaartide ja süsteemiketta turvakleebised olid terved. Kasutatud võtmeosakute kiipkaardid ja süsteemiketta sulges audiitor uuesti turvakleebistega ning märkis üles turvakleebiste numbrid. Turvakleebiste numbrid on ainult audiitori valduses.

E-valimiskastis avamisel tuvastati selles 153 847 häält, millest korduvate e-häälte andmisega ja paberhäältega ülehääletatud e-häälte tühistamise protseduuridega muutusid kehtetuks 578 häält. Arvesse minevaid hääli oli 153 269.

Korduvate e-häälte tühistamine, anonümiseerimine ja e-häälte krüptograafiline segamine tehti vastavalt juhendile IVXV: E-hääletamise käsiraamat Versioon 0.8.

Häälte krüptogrammide kontrollimise käigus, kasutades avalikku häälte krüpteerimise võtit, tuvastati üks nõuetele mittevastav hääl. Häälte krüptogrammide avamisel tuvastati lisaks üks nõuetele mittevastav hääl. Kumbagi e-valmiskastis olnud nõuetele mittevastavast häälest ei arvestatud.“
Häälte krüptograafilise segamise ja kokkulugemise tõendeid kontrolliti korduslugemise käigus audiitorrakendusega.

Euroopa parlamendi valimiste elektroonilise häälte korduslugemine toimus 10. mail 2024 Riigikogu hoones. Korduslugemise käigus kontrolliti juhuvalimiga, kas jaoskondades hääletanute e-hääled tühistati ja kas kohapeal olnud e-hääletajate isikukoode ei olnud tühistusnimekirjades.

1.4 Häälte lugemise kontroll

Audiitor kontrollis audiitorrakendusega oma loodud mälukettal häälte lugemise korrektsust vastavalt auditeerimise suunistele. Lahknevusi häälte lugemise ja audiitorrakendusega saadud tulemustes ei tuvastatud.

Andmeauditi käigus kontrolliti punktis 1.2 kirjeldatud RVT-s vastuvõetud andmete terviklikkust ja töödeldavust. Kõiki andmeid kasutati andmeauditi sisendina. Audiitorrakendusega kontrolliti e-häälte krüptograailise segamise ja lugemise tõendeid.

2 Tähelepanekud

Töötleja juhendis ei olnud eraldi välja toodus täpseid juhiseid, mis on olemas valimiste korraldamise põhimõtetes, e-häälte nõuetele mittevastavate „sedelite“ tühistamiseks.

Kinnitada pädeva ametniku poolt juhend „Suure kaitsetarbega arvuti komplekteerimise kord“. Dokumendi avalikustamisel kaaluda riskide loetelu mitteavalikustamist.

3 Kokkuvõte

Audiitorid ei tuvastanud e-valimiskasti sulgemisel ega häälte lugemisel puudusi, mis võiksid kuidagigi mõjutada e-hääletamise tulemusi. Häälte lugemisel järgiti toimingutes andmete terviklikkuse ja konfidentsiaalsuse tagamiseks vajalikke turvalisuse nõudeid.

Audiitor
Jaan Oruaas
CISA, ISO27001 juhtaudiitor