



Valimiste tehnoloogia riskianalüüs – mis tehtud, mis teoksil?

Kati Ambo-Vaher

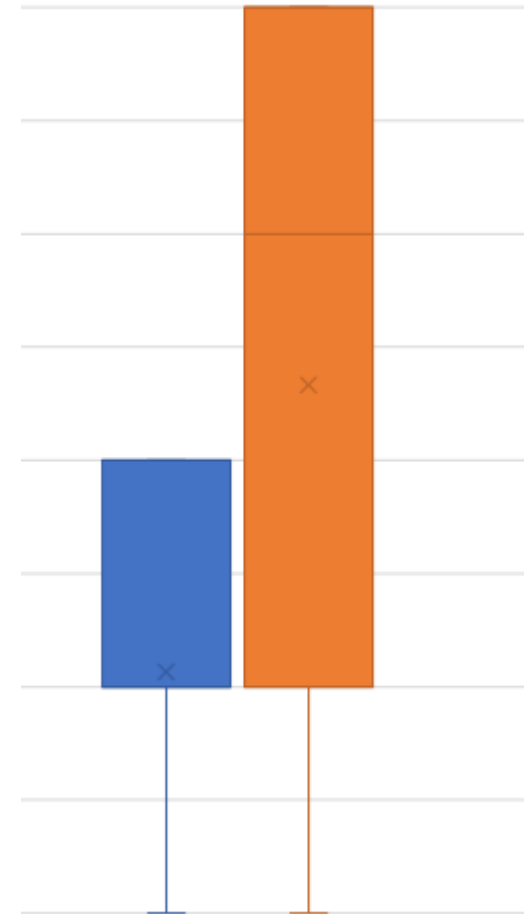
Riigi valimisteenistuse juhtivnõunik

Alo Einla

Riigi Infosüsteemi Ameti valimiste ja eriprojektide osakonna
juhataja



- Kaks aastat, kaks koosseisu, 17 panustajat
- 51 hinnatud ohtu
- 0 väga suurt ja 0 suurt ohtu
- Väärtuslik sisend mitmeks täienduseks





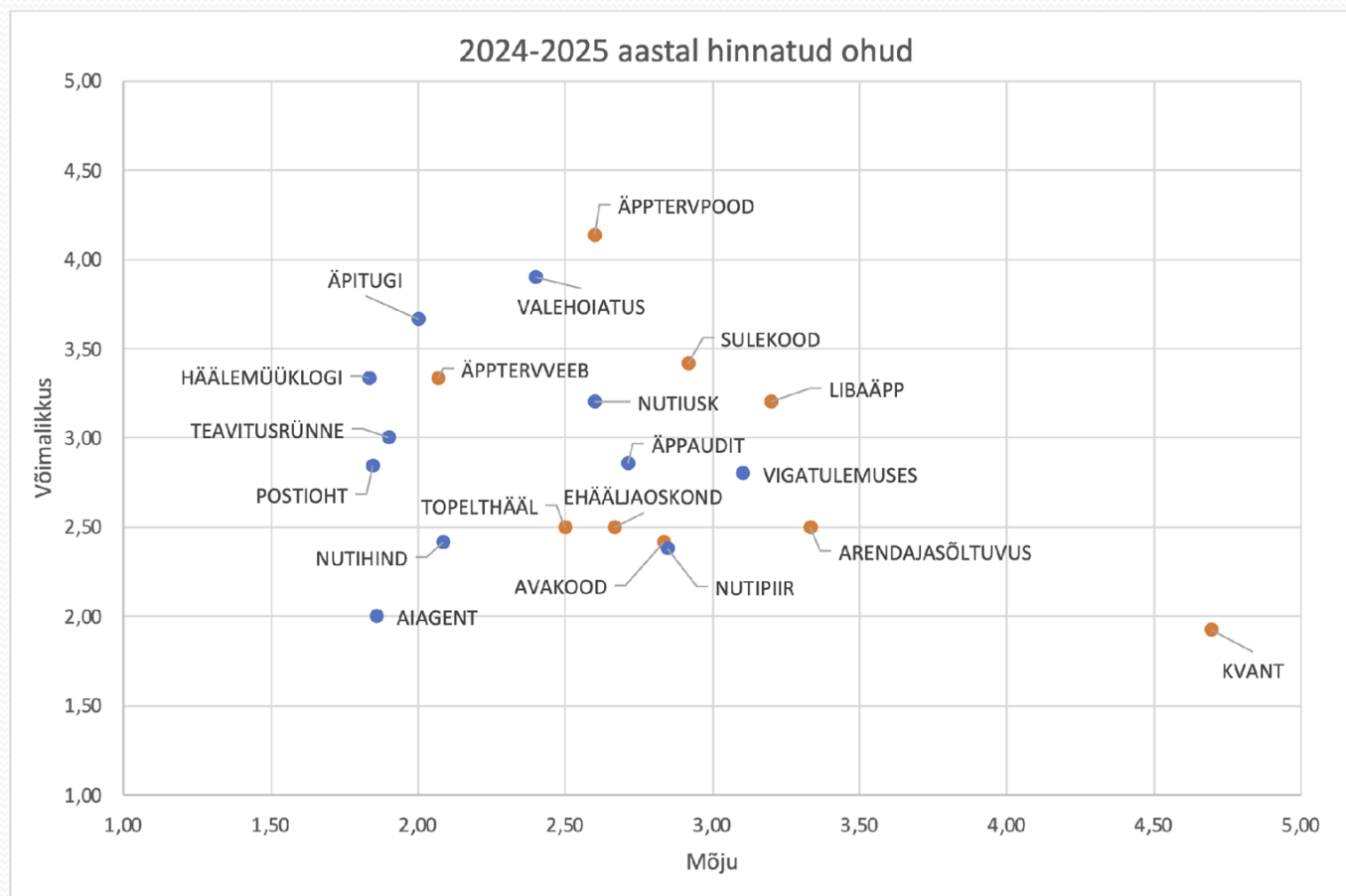
2023-2024 hooaeg

31 hinnatud ohtu

- 25 väikese riskiklassiga ohtu
 - 6 keskmise riskiklassiga ohtu
 - 0 suure riskiklassiga ohtu
 - 0 väga suure riskiklassiga ohtu
- Valeinfokampania kahjustab valimiste usaldusväarsust
 - E-hääletamise kritiseerimine viib hääletusviiside valiku kahanemiseni
 - Nutiseadme valijarakenduse autentsus ja terviklus pole tõendatavalt auditeeritud
 - Mõni e-hääletamise etapp ei võimalda auditeerimist/vaatlemist
 - Mõned valimiste etapid jäetakse auditeerimata/vaatlemata
 - Valimiste infosüsteemide internetiühendused võivad katkeda



2024-2025 hooaeg





Tähelepanuväärseks hinnatud ohud

- Libavalijarakenduste levimine
- Avaliku võtme krüptograafiat ohustav kvantarvuti
- Nutiseadme valijarakenduse autentsus ja terviklus pole tõendatavalt auditeeritud
- Valijarakenduse koodi avalikkus lihtsustab ründeid ja libarakenduste levitamist
- Valijarakenduse koodi suletus raskendab turvanõrkuste leidmist
- Pahatahtlik jaoskonna töötaja sekkub valija hääletusviisi märgetesse
- Sõltuvus arendajast





Riskihinnangust otsusteni

Iga hinnatud risk saab tähelepanu

- Kas vajab maandamist?
- Millised on maandamismeetmed?
- Millised on võimalused meetmete rakendamiseks?





RISK: Osa e-hääletamise etappe võib jääda auditeerimata

- Kaitsemeetmed

Välised teenused sõltumatult auditeeritud tunnustatud standardite ja heade tavade alusel

Infosüsteeme testitakse ja auditeeritakse sobivate standardite alusel, tehakse riskianalüüse

Logide terviklust tagatakse krüptoaheldamisega

- Maandavad tegevused

Auditeerimine täiendavalt automatiseeritud alates 2027

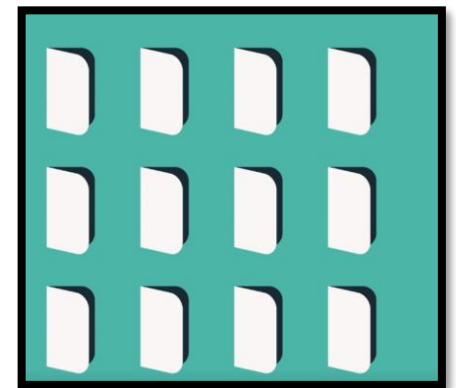
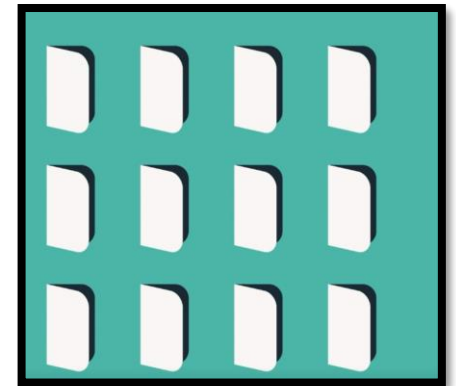
Testandmed koos veaolukordade kirjeldustega

Dokumentatsioon, süsteemi kirjeldus, veateated



RISK: Sõltuvus arendajast

- Kaitsemeetmed:
 - Vähendada sõltuvust ühest arendajast
 - Süsteemiteadmised tellija juures
 - Dokumentatsiooni kvaliteet
 - Pikaajaline rahastus
- Maandavad tegevused
 - Arenduskeskkond RIA taristus
 - Sisemine arendusvõimekus
 - AI võimalused
 - Lähtekoodid avalikud
 - Teadlaste ja ekspertide kaasamine





RISK: Valijarakenduse koodi avalikkus

Avalik kood võib lihtsustada ründeid

Suletud kood võib jätta turvanõrkused leidmata

↳ **Suletud lähtekoodi puhul on ohusündmuse võimalikkus kõrgem**

Kaitsemeetmed

Lähtekoodis ei ole turvanõrkuseid

Maandavad tegevused

- Lisatud täiendav kontroll – nullteadmustõestus
- Turvatestid
- Koodiaudit
- Koodi avalikustamine eeldab seaduse muutmist





RISK: Piisavalt võimas kvantarvuti murrab täna kasutatava avaliku võtme krüptograafia

- Kaitsemeetmed:

Kvantarvutikindel häälte krüpteerimine
Auditeerimise kohandamine

- Maandavad tegevused

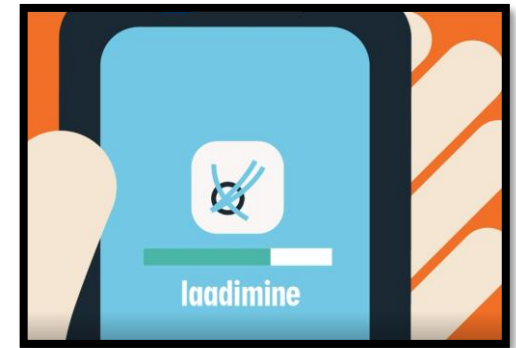
Riiklik tegevuskava tähtajaga 2030
RIA üleminek
Cybernetica AS-i uurimistöö e-hääletamise
kvantkindluse tõstmiseks





Riigikogu valimised 2027

- Täiendav krüptograafiline kontroll e-hääle vastuvõtmisel (ZKP)
- Täiendav isikutuvastuse võimalus jaoskonnas – Eesti äpp
- Lisandub tugi Thales toodetud ID-kaartidele
- Valijarakenduses kasutusel Smart-ID+ lahendus
- Täiendatud auditirakendus – audiitor teeb edaspidi kõik kontrollid ka iseseisvalt läbi
- Valijarakenduse avaldamine nutiseadmete operatsioonisüsteemidele otsustab Vabariigi Valimiskomisjon oktoobris 2026.





Valimistehnoloogiate Nõukoda

- Alaline nõuandev sõltumatu ekspertkogu RVT juures
- Valimistehnoloogiate läbipaistvuse, usaldusväarsuse ja jätkusuutliku arendusvõime toetamiseks
- Hindab valimiste korraldamist mõjutavaid tehnoloogia- ja küberturberiske ning arenguid
- Ei võta üle riigi valimisteenistuse ega teiste valimiste korraldamise eest vastutavate asutuste ülesandeid ega otsustuspädevust



Täname!

Kati Ambo-Vaher, kati.ambo-vaher@valimised.ee

Alo Einla, alo.einla@ria.ee