EESTI TEADUSTE AKADEEMIA KÜBERTURVALISUSE KOMISJON

Küberturvalisuse komisjoni protokoll nr 4

Tartus 19. detsembril 2023

Koosolek kestab kl 10.30–13.00

Osalevad: komisjoni esimees akadeemik Dan Bogdanov, Alo Einla, Jan Willemson, Kristjan Krips, akadeemik Tarmo Uustalu, Ahto Truu, Teet Raidma ja Ivo Kubjas.
Külalisena Indrek Leesi valimiskomisjonist.
Puuduvad Mihkel Solvak, Liisa Past ja Priit Vinkel.

PÄEVAKORD:

1. Arengutest internetivalimiste arenduses (VVK, RIA, RVT, MKM esindajad). Arutame hiljutist uudist, et m-valimised toimuvad kõige varem 2025. aastal (https://www.err.ee/1609193728/mobiiliga-saab-esimest-korda-haaletada-ilmselt-2025-aasta-valimistel).
2. Kuidas mõjutab m-valimiste edasilükkamine TA küberturvalisuse komisjoni tööplaani 2024. aastal? Kas komisjon saab pikendatud ajakava tingimustes rohkemate uuringute toetada? (akad Bogdanov juhib arutelu)
3. RIA koodivaramusse üles seatud hoidla tutvustus (RVT).
4. Koodivaramu algse sisu tutvustus (Kristjan Krips, Cybernetica). Järgneb kodutööde jagamine komisjoni liikmetele.
5. Juhul kui MKM esindajal õnnestub osaleda, siis jätkame arutelu tuleviku protokolliarenduste korralduse üle, mille eelmine kord alustasime.

PROTOKOLL:

1. Arengutest internetivalimiste arenduses.
    a. Akadeemik Dan Bogdanov nendib, et MKM on välja käinud mõtte, et m-hääletamine ei tule 2024. aasta eurovalimistel vaid 2025. aasta KOVide valimistel. On see tõde ja kas selles suunas tuleb liikuda nüüd ajalises tempos?
    b. Arne Koitmäe kinnitab, et see on tõde ja 2024. aastal nutiseadmetega valida ei saa. Ajaliselt ei jõua seda varem käiku anda, hiljaks on jäädud protseduuriga alustamisega, mille viimane aeg oleks olnud 15. novembril, aga seaduslik pool on lahtine. Kõik arendused ei ole veel valmis. Ka suhtlus Apple'iga on pooleli ja tulemusi ei tea. Huvi jätkata on siiski suur. 2025. aasta oktoobrikuus on kohalikud valimised, mis on palju suurema tähelepanu all kui Euroopa Parlamendi valimised. Hetkel on õiguses vaakum ja see ei toeta m-valimisi.
    c. Teet Raidma tõdeb, et valimiskomisjon ootab seadusandlikku alust. Kui seadusandlikku alust ei teki, saame selle mõtte vaid teadmiseks võtta. Tegutsemiseks tuleb enne seadus vastu võtta.
    d. Alo Einla kinnitab, et RIA direktori ja RVT juhi poolt on allkirjastatud ühismemorandum, kus on kirjas, et 2024. aasta valimistel ei ole otstarbekas m-valimist kasutusele võtta, kuna m-hääletamisel ei ole hetkel kehtivat õigusruumi, eelkõige korraldajate jaoks. Riskid, mis on seotud verifitseerimise, võltsimise ja auditeeritavusega ei ole veel lõplikult analüüsitud. Riskid ei ole hästi kahandatud. Sellega kiirustamine võib seada löögi alla e-hääletamise tervikuna. Samuti ei ole RIAle laekunud veel tellimust.
    e. Teet Raidma mure on, et senini ei ole olnud otsuse väljaütlejat, soov on, et see oleks VVK kui valimiste korraldaja. Peale seadusemuudatuse jõustumist esitab RVT RIAle tellimuse, paika panna tuleb rahastus, seaduse rakendamine, sealt edasi tellimuse vormistamine. RVT ja RIA

peavad koos looma kasutajatoe, uued juhendid valijatele, audiitoritele, viima läbi turvatestid. m-hääletamist tuleb auditeerida. RIAlt tuleb tellida jätkuarendused, et tagada ajakohane elektroonilise hääletamise süsteem.

f. Jan Willemson viitab, et ka e-hääletamisel on pidev rahastamine ja jätkuarendused olulised.
g. Akadeemik Bogdanov pakkus ka välja, et kui Android ja iOS rakenduste seire lahendus välja töötatakse, võiks seda testida kõigepealt mõne muu rakenduse peal, kui m-valimiste rakendus. Sobiks näiteks m-riik, aga ka Smart-ID. Alo Einla konsulteerib RIA m-riigi arendusmeeskonnaga, kas see oleks võimalik.
h. Arne Koitmäe mainib, et kui tekivad õiguslikud vaidlused, on seadusandlus väga oluline. Korrektne seadusandlus aitab tagada, et peale valimisi ei oleks probleeme. Ilma seadusandluseta on palju selgusetust, see peab olema väga selge, täpne ja tehnoloogianeutraalne. Võibki juhtuda, et seadusandlus on pidevas ümberkirjutamise staadiumis ja ei too endaga selgust, mis lihtsustaks nt kaebuste lahendamist.

2. Akadeemik Dan Bogdanov leiab, et komisjon õiguslikes küsimustes riiki efektiivselt aidata ei saa. Aga kui m-valimised toimuvad esimest korda 2025. aastal, annab meile lisaaja ja mida saaks komisjon sellega ette võtta.
    a. Alo Einla andis lühiülevaate 2024. aastal m-valimiste arendustegevustest.
    b. Teet Raidma viitab erilisele vajadusele tuua eraldi punktina välja avaliku kommunikatsiooni teemad ja teha seda võimalikult vara.
    c. Akadeemik Dan Bogdanov leiab, et TA küberturvalisuse komisjoni tööplaanis olev avalikustatav riskianalüüs võiks toetada m-valimiste kommunikatsiooni. Kui esimese tööaasta lõpuks (mai 2024) õnnestuks m-valimiste riskianalüüs kokku lepitud metoodikaga valmis teha, siis saaksid pärast EP 2024 valimisi RVT ja RIA selle üle vaadata ning ka sügisel (näiteks septembris 2024) avalikustada. Seejärel saaks tehtud

tööle tagasisidet koguda oktoobris Teaduste Akadeemias toimuval konverentsil.

   d. Komisjoni liikmed kiitsid plaani heaks. Arutleti, kas saaks teha turvaanalüüsi laiemalt kui vaid m-valimiste jaoks. Akadeemik Bogdanov rõhutas, et see sõltub komisjoni liikmete tööviljakusest.

3. Koodivaramule on mitmed komisjoni liikmed juba saanud juurdepääsu.
   a. Arutati koodivaramule juurdepääsu saamise protsessi iseärasusi. Selgus, et ID-kaarti on vaja vaid esmase konto loomise juures.
4. Kristjan Krips tutvustas komisjoni liikmetele riski kirjelduse mustandit.
   a. Järgnes arutelu riskide hindamise metoodika üle. Jõuti järgmistele järeldustele.
      i. Rünnete asemel räägime ohtudest või ohusündmustest, ründaja asemel ohuagendist. Nii on kergem käsitleda ka nt tegematajätmiseid, kus puudub aktiivne ründaja.
      ii. Ohusündmuse sagedust on kergem hinnata kui tõenäosust.
      iii. Riskide klassifitseerimise metoodikas toetume Teet Raidma ja Kristjan Kripsi välja pakutud skaaladele, mida kohendame töö käigus vastavalt eksperthinnangutele. Kui komisjoni eksperthinnangutest jääb vajaka, siis kaasame teisi osapooli.
   b. Kristjan Krips ja Jan Willemson jagavad enne jõulu komisjoni liikmetele järgmise istungi kodutööks kahe riski analüüsid.
5. MKMi esindajal ei õnnestunud koosoleku tööga liituda, seega lükkus selle päevakorrapunkti arutelu tulevikku.

Koosoleku juhataja:	Dan Bogdanov
Protokollija:	Ülle Sirk