EESTI TEADUSTE AKADEEMIA
KÜBERTURVALISUSE KOMISJON

Küberturvalisuse komisjoni protokoll nr.3

Tartus 14. novembril 2023

Koosolek kestab kl 10.00-13.00

Osalevad: komisjoni esimees akadeemik Dan Bogdanov, Alo Einla, Jan Willemson, Kristjan Krips, Ahto Truu, Mihkel Solvak, Teet Raidma

Külalistena Indrek Leesi RVTst, Priit Parmakson, Riho Kerge ja Raimo Peterson RIAst

Puuduvad akadeemik Tarmo Uustalu, Liisa Past, Ivo Kubjas ja Priit Vinkel.

PÄEVAKORD:

1) 10:00 Ülevaade valimiste regulatsiooni ja tehnoloogia arengutest viimaste nädalate jooksul (45 minutit)
Komisjoni esimees palus MKM, RIA, RVT ja VVK esindajatel juhtida arutelu selle üle, millised on olnud tähtsamad uudised viimaste nädalate jooksul, mida komisjon peaks teadma.

2) 10:45 Ühtse metoodikaga valimiste turvaanalüüsi järgmised sammud (75 minutit)
Meiega liituvad RIA külalised ning arutame seda, kas RIA saaks ja tahaks majutada võimalikku internetivalimiste turvaanalüüsi arendust.

3) 13:00 Piloot-turvaanalüüsi võtmeteemade valimine
Millistele valimiste moodulitele peaks pilootanalüüsis tähelepanu pöörama?

4) 14:00 Kuidas peaks arutlema valimiste protokolli uuenduste üle?
Komisjoni esimees tõstatab taas ühe varasema arutelupunkti - kuidas saaks tulevikus arutada avatult valimiste protokolliuuendusi?

Enne päevakorra küsimuste juurde asumist teeb komisjoni esimees kokkuvõtte oktoobrikuus Tallinnas akadeemia majas toimunud konverentsi järelkajadest, mis olid enamjaolt positiivsed ja annavad komisjonile jõudu edasi minna teades, et komisjoni töö on vajalik.

PROTOKOLL:

1. Ülevaade valimiste regulatsiooni ja tehnoloogiate arengutest.
    a. Kas kevadised valimised tulevad teistmoodi, millised on arengud? Teet Raidma ja Arne Koitmäe teadmisel läks seaduseelnõu muudetud kujul kinnitamiseks, seda täiendatakse m-valimistega. Tehnilised nõuded valimistele jäävad RVT korraldada. Alo Einla RIAst mainib, et valitsuse liikmetel on ootus, et m-valimistele viitav selgitus saaks sisse seletuskirja, põhiseaduskomisjoni istung on 21.11. Ootus on, et uus seadus jõustuks 1.01.2024. Europarlamendi 2024. aasta ettevalmistusteks on aega jäänud vähe ja tööd on veel palju.
    b. Akadeemik Dan Bogdanov esitab küsimuse, kas on ette näha tehnilisi muudatusi? Arne Koitmäe hinnangul uusi arendusi teha ei jõuaks, Jan Willemson ja Alo Einla mainivad, et on veel lahtisi küsimusi, aga m-hääletust valmistatakse ja arendatakse avatult.
    c. Indrek Leesi toonitab, et kui seadus ka vastu võetakse, siis rakendust alles täiendatakse. On soov teha avalik laialdane demo, aga selle ajakava ei ole hetkel teada. Samuti peab audiitor saama kontrollida Apple'i ja Google'i äppide terviklust. Riigikogule esitati eelnõu ja seletuskiri 13.11.2023.
    d. Mitmed komisjoni liikmed avaldasid muret, et kõige saavutamiseks kevadisteks Euroopa parlamendi valimisteks kipub aega väheks jääma.
2. Akadeemik Dan Bogdanov kinnitab mõtet, et on vajadus turvaanalüüsi hoidla järele, mida majutaks riiklik asutus. Selle aruteluga liituvad külalised RIAst Raimo Peterson ja Riho Kerge. Inspiratsiooniks tõi akadeemik Bogdanov HOIA turvaanalüüsi, mis avaldati Eesti koodivaramus

a. Akadeemik Bogdanov viitas konverentsil enda peetud ettekandele ning selgitas, et lahendamist vajab küsimus, kuidas oleks võimalik luua nn tööhoidla, millele on ligipääs RIA poolt volitatud isikutel ja kus toimuks jooksev töö. Seal saaks teha jooksvat tööd riskianalüüsiga. Saaksime kirja panna ründepinna, ohud koos viidetega ründepinnale ning vastumeetmete kataloogi. Eesmärk oleks ohtudele anda ka skaalade toel võimalikkuse ja tõsiduse hinnangud. Nii saaksime selgelt analüüsida, millised ründed on nii tõsised, et vajaksid uute vastumeetmete teostamist. Bogdanovi sõnul võiks see hoidla asuda RIA juures.
b. Riho Kerge teeb ettepaneku lahendada see küsimus koodivaramu põhjal. Kindlaks tuleb teha, milline on halduskoormus. Nagu soovitud, saaks üks hoidla olla avalik ja teises, mis seda ei ole, toimub ettevalmistav töö.
c. Jan Willemson märgib, et analüüsidest tuleb tuletisi, selle alusel saame midagi genereerida, mida saab pärast kvaliteedikontrolli avaldada.
d. Alo Einla nendib, et vaja on kedagi, kes on selle teenuse omanik, aga kes see võiks olla? Akadeemik Dan Bogdanov toonitab infoarhitektuuri olemasolu vajadust. Kas RIA peaks olema kõigi hoidlate omanik? Tegelikkuses on vajalikud nii vastutav omanik kui ka haldav omanik. Teenuse omanik on Arne Koitmäe sõnul RVT. Komisjon lepib kokku terminis haldav kasutaja ehk haldur.
e. RVT kontrollib juurdepääsu hoidlale ning jagab seda TA küberturvalisuse komisjoni esimehe taotluse alusel komisjoni liikmetele, aga ka teistele turvaanalüüsi teostavatele isikutele. TA komisjoni esimees vastutab selle eest, et teavitada RVT-d juurdepääsu õiguste muutumistest, näiteks komisjoni koosseisu muutumise tagajärjel.

3. Milliste riskide analüüsiga peaks alustama?
    a. Teemaks tulevad ohud enne ja peale valimisi, siin on mõjud erinevad tõdeb Indrek Leesi. Alo Einla soovitab jaotada riskid valimiste üldprintsiipide ja ülejäänud järgi.
    a. Akadeemik Bogdanov tegi ettepaneku, et alustada tuleks m-valimistega seotud riskide analüüsist. Ettepanek leidis ka teiste komisjoni liikmete toetust.
4. Akadeemik Bogdanov tõstatas aruteluküsimuse - kus saab Eestis arutleda e-valimiste protokolli teemadel? Kuidas peaks toimuma protokolli arenduse üle arutelu ja kes selle algatab? Arne Koitmäe tõdeb, et vastavat formaati ei ole olemas, on küll toimunud arutelusid nn seminari vormis, aga selle kohta ametlikku protsessi ei ole.
    a. Ahto Truu toob välja, et ei ole avalikku kanalit, kuhu esitada ettepanekud, sisemine mehhanism on olemas, aga välist liidest avalikkuse jaoks pöördumiseks ei ole.
    b. Ideaalis tuleks luua struktuur ja paika panna formaat, mis võimaldaks konstruktiivset koostööd avalikkusega ning ei koormaks üle niigi väheseid valimiste süsteemi arendajaid.
    c. Alo Einla tõdeb, et kui metoodika on hea ja universaalne, siis saab seda kasutada rohkemaks kui vaid valimiste süsteemi kavandamiseks. Peaks olema formaat, kus saaks diskuteerida, on olemas mitu kogukonda, nii süsteemide arendajad RIAs aga ka avalikkus ja aktivistid.
    d. Konkreetsete soovitusteni komisjon veel ei jõudnud, kuid istung lõppes veendumusega, et selle teema juurde tuleme veel tagasi.

Koosoleku juhataja: Dan Bogdanov

Protokollis: Ülle Sirk