Paavo Pihelgase pöördumine Riigikogu e-valimiste töörühma poole

From: Paavo Pihelgas paavo.pihelgas@gmail.com

Date: 2011/9/23
Subject: E-valimistest
To: jaak.allik@riigikogu.ee, Peeter.Laurson@riigikogu.ee, Valdo.Randpere@riigikogu.ee, Priit.Toobal@riigikogu.ee, heiki.sibul@riigikogu.ee, ylle.madise@vpk.ee, priit.vinkel@riigikogu.ee

Tere,

ma olin väga positiivselt üllatunud, kui lugesin, et e-valimiste edasiarendamiseks moodustati Riigikogus töögrupp.
Jagan mõningaid mõtteid.

I
Eestit tuuakse tihti turvaliste e-valimiste võimalikkuses kahtlejatele eeskujuks kui riiki, kus sellega on justkui hakkama saadud. Seetõttu on mitmed maailmatasemel asjatundjad - näiteks Harri Hursti, Alex Halderman, Rop Gonggrijp ja Ross Anderson - ilmutanud huvi lähemalt uurida tarkvara, millega Eestis valimisi läbi viiakse. Kahjuks ei ole sõltumatu uurimine võimalik, sest Vabariigi Valimiskomisjon nõuab igaühelt, kes tarkvara lähtekoodi soovib uurida, konfidentsiaalsuslepingu sõlmimist. Leppetrahv ulatub 300 000 kroonini ning tingimused keelavad avastatud defektide avaldamise. Praktikas tähendab see, et vea leidmisel on VVKI võimalus teave probleemi kohta summutada ning töö läheb tühja.
Soovin, et konfidentsiaalsusleping kaotataks või loodaks lepingu erivorm, mis lubaks turvaaukude jt defektide uurimist ja tulemuste piiranguteta avaldamist.
Põhjendusena, miks tarkvara lähtekoodi ei peaks saama vabalt uurida, võidakse teile tuua, et see seab ohtu tarkvaras peituvad kaitsemeetmed. See argument ei ole tõsiseltvõetav. Kõik kvaliteetsed turvasüsteemid, näiteks internetipanganduse alustehnoloogiad (HTTPS jt), on täiesti avalikud ning loodud printsiibil, et süsteemi tundmine ei anna eelist eduka rünnaku läbiviimiseks. Ka Norra e-valimiste pilootprojekt, mida hiljutistel valimistel katsetati, lähtub sellest põhimõttest ja on vabalt uuritav - nii dokumentatsiooni kui tarkvara lähtekoodi leiab aadressilt
http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658
Kui sõltumatud eksperdid leiavad turvaauke, siis aitab see kaasa tarkvara paremaks muutmisel. Kui nad midagi ei leia, on see tunnistus e-valimiste turvalisusest. Ma ei näe, et avalikust uurimisest oleks midagi kaotada. Või nagu ütles Barbara Simons: "Kui väidetakse, et süsteem on turvaline, siis ei peaks ju olema probleemi väliseksperte seda uurima lasta. Nad ei peaks olema hirmul. Võib-olla eksperdid ütlevad, et see on OK, võib-olla mitte. Ma soovitan vältida poliitikat ja keskenduda vaid tehnilistele küsimustele. Väliseksperdid pole eestlased ja neil pole mingit huvi, millised valimistulemused Eestis on. Neid huvitavad vaid turvalisusküsimused."
Lisaks väärib rõhutamist läbipaistvus. Nii, nagu kõikidel huvilistel on võimalus vaikimiskohustuseta valimisi jälgida, sealhulgas valimiskaste ja muid vahendeid kontrollida, peab olema võimalus kontrollida tarkvara. Vastasel juhul taandub kõik väikese isikuteringi usaldamisele; hääled läbivad kontrollimatu tarkvara näol "musta kasti"
ning peame usaldama tulemust, kuigi ei näe detailideni, kuidas tulemus saadakse. Ideaalmaastik valimispettusteks.

II

Kohati tundub, et e-valimised on muutunud asjaks iseenesest; kinnisideeks. Üks Riigi Infosüsteemide Ameti töötaja nimetas seda otsesõnu välispublikule suunatud PR-projektiks.
Olen graafikutele kandnud valimisaktiivsuse näitajaid, e-hääletajate demograafilisi ja arvutikasutuse andmeid, kaalunud läbi rahvastikupüramiidiga jms - ning neist andmetest järeldub, et valimisaktiivsus ei tõuse arvestataval määral (ca 80-85% puhul toimub oletatavasti vaid valimisviisi vahetamine; RK 2011 oli rekordmadal jaoskonnas hääletajate osakaal hääleõiguslikest valijatest, alla viiekümne protsendi) ning e-valijate vanuseline koosseis jaguneb üllatavalt lähedaselt rahvastiku koosseisuga. Teisisõnu - e-hääletavad samad inimesed, kes muidu käiks jaoskonnas; vastu igasuguseid ootusi on näiteks vanusegrupp 18-24 lausa alaesindatud.
Ainsaks argumendiks jääb mugavus; mugavuse nimel - nagu käis läbi Euroopa Nõukogu 2008. aasta aruteludest e-valimiste üle - aheneb nende inimeste ring, kes saavad aru ja suudavad jälgida, kuidas kujuneb valimistulemus; kuidas valitsetakse riiki.
Kust jookseb piir, millest kitsamaks ei tohi ringi enam tõmmata?
Kui OSCE viitab peenetundeliselt, et isegi valimiste korraldamise eest vastutav VVK ei saa ööd ega mütsi aru, mis e-valimistel tehnilisel tasemel toimub, siis kas see piir on ületatud?

III

VVK kõikidesse väidetesse tasub suhtuda skepsisega. OSCE/ODIHR vaatlejate aruanne loetleb 10. leheküljel kolm e-valimiste tarkvara
kontrollimisastet:
1) Tarvi Martensi poolt - tarkvara vastuvõtmisel tootjalt;
2) Küberkaitseliidu õppus;
3) anonüümse programmeerija audit.
Teabenõude korras selgus, et Martensi katsetamistulemustest ei ole kirjalikke jäädvustusi. Küberkaitseliidu õppuse kokkuvõtet ei väljastatud juurdepääsupiirangu tõttu (asutusesiseseks kasutamiseks kuulutatud dokument).
Kõige imekspandavam oli lugu anonüümse programmeerija auditiga, kelle identiteetigi keelduti vaatlejatele avaldamast, auditi aruandest rääkimata. Vaatleja David Bismark kinnitas, et VVK väitis auditi toimumist ja lõpparuande olemasolu. Need väited kajastuvad vaatlejate raporti 10. leheküljel. Kui esitasin teabenõude, selgus, et audit telliti Martin Paljakult, kelle haigestumise tõttu tööd läbi ei viidud ja aruannet ei valminud. Julgen öelda, et VVK lihtlabaselt valetas auditi kohta ja seetõttu paistab OSCE aruandest helgem olukord kui tegelikult valitses.
Kuna Martensi katsetused ega Küberkaitseliidu õppus ei hõlmanud tarkvara lähtekoodi auditeerimist, ilmneb, et tarkvara kasutati valimistel ilma igasuguse tõsise kontrollimiseta, millest oleks jäänud maha adekvaatne jäädvustus (e-valimiste protseduure saatev süstemaatiline dokumendijälje puudumine tekitab juba iseenesest küsimuse, et kas hoolimatus või tehakse teadlikult nii). Isegi veebibrauser või emailirakendus, millega käesolevat kirja loete, on läbinud põhjaliku kvaliteedikontrolli!
Kvaliteedikontrolli puudumisest annab hästi aimu vahejuhtum üksikkandidaatidega, kelle nimi ei olnud teatud (ja võrdlemisi
levinud) arvutisätete juures nähtav. Visuaalselt end reetvad probleemid on alati kõige lihtsamini leitavad, sest need sõna otseses mõttes vaatavad testijatele ekraanilt vastu. Kui nii elementaarseid programmivigu ei suudetud õigeaegselt leida, siis kust tuleb veendumus, et programmis ei ole viga, mis avaldub vaid igal, ütleme, viiekümnendal korral, andes hääle teisele kandidaadile kui ekraanil valitud?
Kommertstasemel loodud tarkvaras on reeglina 1000 lähtekoodi rea kohta 20-30 programmiviga; ma ei tea, kui mahukas on e-valimiste tarkvara, aga kindlasti on jutt kümnetest tuhandetest ridadest. Piisab ainult ühest veast kriitilises kohas, et valimistulemus muutuks. Heal juhul muutub piisavalt ekstreemselt, et viga avastataks. Aga kui muutub ainult natuke?
Programmiviga ei pruugi tahtmatu olla. Insider-rünnakuna on tarkvara arenduses osaleva inimese poolt teadliku defekti sissejätmine küllaltki levinud (klassikaliselt näiteks

palgaarvestuse süsteemis), ja oskuslikult korrektselt toimivaks funktsiooniks maskeeritud defekti otsimine ei ole naljategu.

IV

28-30. septembril toimub Tallinnas tipptasemel e-valimiste teemaline teaduskonverents VoteID 2011, mille tõsiseltvõetavust näitab seegi, et ettekanded avaldab tuntud teaduskirjastus Springer. Mulle anti võimalus tutvuda seal esitletava Sven Heibergi, Peeter Laudi ja Jan Willemsoni ettekandega "On applying i-voting for Estonian Parliamentary elections in 2011". Ettekandes kirjeldatakse juhust, kus elektrooniline sedel oli vigane (viitas mitteeksisteerivale
kandidaadile) ning kuulutati kehtetuks.
Kuidas see juhtus?
Paraku vastust sellele ei ole. Tuuakse kaks kõige tõenäolisemat
hüpoteesi: et keegi tahtlikult rikkus sedeli või riknes sedel tuvastamata programmi- või riistvaraveast.
Milliste meetmetega saab kindlaks teha, kas ja mis ulatuses riknes sedeleid mõne programmivea pärast eksisteeriva kandidaadi kasuks ja jäi seetõttu avastamata? Sellele ei saa vastata, sest kontrollimeetmed puuduvad. Valijal ei ole võimalust teada saada, et ta valik läbis pika ja keeruka elektrooniliste seadmete ahela muutumatuna, ja VVKl ei ole võimalust teada saada, et võeti vastu korrektne hääl. Kui jaoskonnas hääletamisel on VVKl ja valijal otsene kokkupuude (valija viibib VVK kontrollitavas keskkonnas), siis e-valimistel haigutab valija ja VVK vahel tühimik. Mõtteline ala, mida VVK kontrollib (valimiste server), ja mõtteline ala, mida valija kontrollib (tema arvuti), ei puutu kokku.
See on samaväärne, kui saata kodudesse sedelid ja lasta jooksupoistel need uuesti kokku koguda. Kuidas kumbki osapool saab muude sidekanalite teel üle kontrollimata veenduda, et jooksupoiss ei trikita sedeliga?
Norra püüab probleemi lahendada e-valimiste süsteemiga, milles hääletaja kasutab kolme sõltumatul teel talle edastatud infokildu:
posti teel saadetud koode, millega hääletada; Internetiühendusega arvutit, millega sedel edastada; ja mobiiltelefoni, millega vastu võtta kinnituskood sedeli korrektsest kohalejõudmisest.
Piltlikult väljendudes kasutatakse kolme jooksupoissi, kes üksteist ei tunne. Konspiratsiooni korraldamine muutub mitme suurusjärgu võrra keerulisemaks. Ründaja peab korraga hõivama telefonisüsteemi, postiteenistuse ja arvutisüsteemid. Iga takistus kergitab avastamise tõenäosust; postisüsteem seob ründaja füüsiliselt rünnatava riigi territooriumile ja jurisdiktsioonile.
Väärib mainimist, et - kui ma ettekannet õigesti mõistan - 1. aprillil tegi VVK otsuse avada defektne elektrooniline sedel moel, mis lubanuks kokku viia sedeli ja valija identiteedi. Nädal hiljem, enne hääle avamist, muudeti otsus ümber ja sedel jäeti avamata, "et mitte luua pretsedenti". Eks ta ole. Põhiseaduses on valimiste kohta ju kasutusel mõiste "salajane", mitte "salajane vastavalt vajadusele" või muu leidlik konstruktsioon.

V

Kõige tähtsam - tulevikule mõeldes - , mis te teha saate, on aidata kaasa e-valimiste standardite kehtestamisele. See on ju selge, et Riigikohus ei saa sisuliselt kaebusi arutada, sest selleks puudub igasugune seaduslik alus, mis vastaks e-valimiste olemusele.
E-hääletamine on olemuselt arvutisüsteemile delegeeritud hääletamine, mille võrdsustamist kirja teel hääletamisega pean loogikaveaks, sest elektrooniliste süsteemide massiline ründamine nõuab palju väiksemaid ressursse kui geograafiliselt hajutatud postisüsteemis tuhandete ümbrikute kallal käimine. E-hääletamine on uus hääletamisviis ja vajab omaette standardeid, mis juhinduvad klassikalise hääletamise põhimõtetest, aga arvestavad digitaalsusega seotud nüansse (reaalmaailmas on 10 000 võlts-sedeli täitmine suur vaev, käekirjaekspertide jt poolt tuvastamatuna ehk isegi võimatu; virtuaalmaailmas aga triviaalsus).

Minu teada on ainus rahvusvaheliselt tunnustatud e-valimiste standard Euroopa Nõukogu Ministrite Komitee soovitus Rec(2004)11, saadaval aadressil https://wcd.coe.int/wcd/ViewDoc.jsp?id=778189
Ratta leiutamise asemel oleks mõistlik see Norra eeskujul seada Eesti e-valimiste aluseks. EN soovitus on rahvusvahelise koostöö raames iga kahe aasta tagant uuesti läbiarutatav lühike, selgeid reegleid kehtestav dokument: e-valimiste süsteem peab võimaldama tulemuste õigsuse tõestamist; tarkvara peab läbima sõltumatu sertifitseerimise; igas etapis peab olema tagatud salajasus; jms.
Kui VVK suudab e-valimiste korraldamise kvaliteeti tõsta nendele mõistlikele nõuetele vastavaks, oleme teinud suure sammu edasi. Kui ei suuda, siis ma leian, et me ei kaota e-valimiste kadumisega midagi väärtuslikku.

Kõike head soovides,
PP