Auditointiraportti kunnallisvaalien sähköisen äänestyksen pilotista

Tiivistelmä

Auditoinnin kohteena on syksyn 2008 kunnallisvaaleissa kolmessa kunnassa toteutettava sähköisen äänestyksen kokeilu. Kyse ei ole kotoa tapahtuvasta sähköisestä äänestämisestä, vaan kokeilusta, jossa pitkälti jäljitellään tavanomaisia vaaleja. Jo tällaisessakin tietokoneavusteisessa vaalissa ilmenevät monet sähköiseen äänestämiseen liittyvät turvallisuus- ja luottamusongelmat. Näiden ongelmien analysointi ja arviointi on tämän auditoinnin keskeinen tavoite.

Auditoinnin perusteella suunniteltu kokeilu on vakaalla ja turvallisella pohjalla edellyttäen, että kaikki toimijat noudattavat annettuja pelisääntöjä. Näiltä osin järjestelmä vastaa pitkälti nykykäytäntöä. Sähköisten vaalien yhteydessä keskeiseksi kuitenkin muodostuu kysymys siitä, miten huolehditaan luottamuksen säilymisestä, ts. siitä, että mikään vaalin osapuoli ei pysty huijaamaan muita. Tavanomaisten vaalien yhteydessä kontrolli on varsin hyvin toteutettu. Sähköisissä vaaleissa tämä on olennaisesti vaikeampaa teknisten yksityiskohtien ja järjestelmän avainhenkilöiden toiminnan osalta. Näiltä osin auditoinnin tuloksena esitetäänkin pohdittavaksi joidenkin yksityiskohtien tarkentamista. Erityisesti on syytä kiinnittää huomiota virkailijoiden koulutukseen ja siihen, että kriittisissä kohdissa edellytetään moninkertaista valvontaa.

Kokonaisuutena kuitenkin katsomme, että sähköisen äänestyksen kokeilu on toteutettavissa nyt kaavaillulta pohjalta. Valvonnan toimivuuden varmistaminen on käsityksemme mukaan hankkeen suurin haaste.

1 Johdanto

Tietoverkoissa järjestettävien yleisten vaalien problematiikkaa on tutkittu paljon. Useimmiten tavoitteena on ollut rakentaa sellainen luotettava vaalijärjestelmä, jossa kukin voisi äänestää vaikka kotoaan joko tietokoneella tai kännykällä. Lähtökohtana on tällöin ollut, että järjestelmän tulee toteuttaa ainakin seuraavat vaatimukset:

1. Vain äänestyskelpoiset voivat äänestää, ja hekin vain kerran.

2. Vaalien tulosten tulee olla yleisesti verifioitavissa.

3. Vaalisalaisuuden on säilyttävä.

Vaatimusten toteuttamiseen tarvitaan ”rakennuspalikoina” mm. salattuja ja autentikoituja viestiliikenneyhteyksiä. Lisäksi tarvitaan myös muita monimutkaisia kryptografisia menetelmiä, jotta *vaalisalaisuuden säilyminen ei perustuisi luottamukseen, vaan se seuraisi järjestelmän ominaisuuksista.*

Tässä auditoidussa vaalijärjestelmässä lähtökohta on ollut toinen. Tavoitteena on ollut luoda nykyistä lippuäänestystä jäljittelevä järjestelmä. Erona on se, että nyt äänestyskopissa on tietokone, jolla äänet lähetetään internetin kautta ”sähköiseen uurnaan”. Järjestelmän turvallisuutta on tarkoitus kontrolloida samoin kuin nykysysteemissä: varmistamalla, että sekä äänestyspaikoilla että ääntenlaskupaikalla on läsnä joukko eri tahoja edustavia luotettavia vaalivirkailijoita. Tämän lisäksi pitäisi tietysti varmistaa, että äänestämisessä ja tulostenlaskennassa käytettävät tietokoneohjelmat toimivat tarkoitetulla tavalla.

Minimivaatimuksena vaalijärjestelmälle voidaan pitää edellä mainittujen ehtojen toteutumista edellyttäen, että kaikki vaaleihin osallistuvat virkailijat toimivat rehellisesti. Tämä toteutuu tässä arvioitavassa järjestelmässä. Auditoinnin kannalta on kuitenkin syytä tarkastella järjestelmän luotettavuutta myös tilanteessa, missä joukkoon on eksynyt jokunen vilpillinenkin virkailija. Tällöin valitussa ratkaisussa on myös heikkouksia. Alla luetellaan yleisiä ongelmia ja myöhemmissä luvuissa käsitellään joitakin mahdollisia ongelmatilanteita yksityiskohtaisemmin.

Mainittakoon vielä, että tässä raportissa on tarkoitus lähinnä tuoda ilmi havaittuja potentiaalisia ongelmia. Osa niistä voi tuntua kaukaa haetuilta, mutta on muiden instanssien tehtävä päättää, kuinka relevantteja maalatut uhkakuvat ovat pilotissa.

- On syytä korostaa, että useimmat tässä raportissa mainitut mahdolliset ongelmat voivat toteutua vain, mikäli vaalivirkailija toimii vilpillisesti ja muiden virkailijoiden fyysinen valvonta pettää. Vaikka samat ongelmat voivat toteutua myös nykyisessä lippuäänestyksessä, on sähköisessä äänestyksessä virkailijoiden fyysinen valvonta huomattavasti hankalampaa. Jos kontrolli kaikista varotoimenpiteistä huolimatta pettäisi, voisivat seuraukset olla dramaattisia. Tietokonevaaleissa tulisikin kaikilta vaalivirkailijoilta edellyttää ainakin jonkinlaisia tietoteknisiä taitoja. Erityisen ongelmallinen on tilanne, jossa yksi vaalivirkailija on alan ekspertti ja muut statisteja.

- Vaalijärjestelmä tunnistaa äänestäjät heille generoidun sähköisen äänestyssalasanan avulla. Tämän tunnuksen äänestäjä saa haltuunsa älykortille kirjoitettuna äänestyspaikan vaalivirkailijalta. Kahdelta yhteistyössä toimivalta vilpilliseltä virkailijalta voi siis saada haltuunsa lukuisia äänestystunnuksia ja äänestää niillä mielensä mukaan.

- Auditoitavan järjestelmän äänestystilanne poikkeaa olennaisesti nykysysteemistä. Lippuäänestyksessä äänet pudotetaan vaaliuurnaan julkisesti, jolloin äänestäjä tietää ja vaalivirkailijat voivat todistaa äänen menneen uurnaan. Tarkasteltavassa järjestelmässä äänien siirtymistä sähköiseen uurnaan ei todista kukaan. Järjestelmästä voi vain tarkistaa, milloin uurnaan on talletettu ääni äänestäjän nimissä. Äänestäjän pitää vain luottaa, että virkailijat ja ohjelmistot toimivat oikein ja ääni on juuri se, miksi hän sen tarkoitti.

- Vaalijärjestelmässä käytetään useita tietokoneohjelmia, joista suurin osa on ulkomaiselta järjestelmän suunnitelleelta yhtiöltä ja loput on tehnyt TietoEnator. Välttämätön edellytys systeemin luotettavuudelle on ohjelmistojen toimivuus tarkoitetulla tavalla. Lähdekoodi ei kuitenkaan ole avoin ja vain koodin kriittiset kohdat on tarkastettu. Vaikka koodi olisikin läpikotaisin tarkastettu, pitäisi vielä pystyä varmistumaan, että suoritettava koodi vastaa tarkastettua koodia, ja että suorittavassa tietokoneessa ei pyöri ylimääräisiä ohjelmia. Vastaavat ongelmat esiintyvät varmasti kaikissa tietoverkkoihin suunnitelluissa vaalijärjestelmissä. Siksi olisi toivottavaa, että äänestäjä pystyisi varmistamaan oman äänensä päätyneen uurnaan ja että uurnasta lasketut vaalitulokset voitaisiin yleisesti verifioida oikeiksi.

- Digitaalinen uurna sijaitsee TietoEnatorin tiloissa. Järjestelmää käyttävät sekä sen ovat suunnitelleet ja toteuttaneet TietoEnatorin asiantuntijat Oikeusministeriön valvonnassa. Näin ollen järjestelmän turvallisuus perustuu OM:n kykyyn valvoa jokaista vaihetta. Koska sama organisaatio on vastuussa kaikista vaiheista, sen valvominen on haastava tehtävä.

- Olisi ehkä syytä pohtia, riittääkö se, että järjestelmän suunnittelijat ja "sisäpiiriläiset" pystyvät vakuuttumaan sen turvallisuudesta. Tämä luottamus pitäisi voida siirtää myös äänestäjien keskuuteen.

Seuraavassa listataan yksityiskohtaisemmin huomioita auditoitavasta järjestelmästä. Aluksi on kommentoitu OM:n järjestelmälle asetettamia rajoituksia. Seuraavaan lukuun on kerätty aluksi mainittujen kolmen vaaliprotokollalta vaadittavan ominaisuuden toteutumiseen liittyvät kommentit.

Korostettakoon vielä, että kaikki mainittavat ongelmatilanteet edellyttävät ainakin jonkinasteista valvonnan pettämistä.

2 Asetetut rajoitukset ja niistä aiheutuvat ongelmat

Suomen vaalilakiin perustuen on päätetty, että äänestystapahtumasta ei säilytetä paperitulostetta tai anneta sähköistä kuittia äänestäjälle. Tästä syys-

tä äänestäjä ei voi mitenkään varmistua siitä, menikö hänen antamansa ääni oikein perille. Hänen on vain luotettava siihen, että laitteisto, ohjelmisto ja virkailijat toimivat niin kuin on tarkoitettu. Epäselvässä tilanteessa äänestyspaikan vaalivirkailija voi tosin tarkistaa, että äänestäjän äänioikeus on järjestelmässä merkitty käytetyksi.

Äänestyksessä käytetään normaalia PC-laitteistoa ja CD:ltä ajettavaa käyttöjärjestelmää. PC-laitteiston suojaaminen siten, että siihen ei voi lisätä ylimääräisiä laitteita tai ohjelmia, on haastava tehtävä. CD:n kopiointi on helppo tehdä huomaamattomasti ja levyn haltuun saaminen helpottaa väärinkäytöksiä. Näistä syistä vaalivirkailijoilta tulisi edellyttää tietokonetaitojen hallitsemista.

Käytettävä ohjelmisto on liikesalaisuus, eikä sitä voida julkistaa. Vaikka ei olekaan mitään syytä epäillä ohjelmistoa vialliseksi, ei voida kokonaan sulkea pois sitä mahdollisuutta, että siihen on jäänyt virheitä tai tahallisia heikkouksia. Koko koodin tarkistaminen huolella veisi kuitenkin useita henkilötyövuosia.

Jatkuva yhteys keskuskoneeseen mahdollistaa äänestyskelpoisuuden tarkastamisen reaaliaikaisesti ennakkoäänestyksen aikana, mutta altistaa järjestelmän palvelunestohyökkäyksille. Palvelunestohyökkäyksen vaikutusta voidaan rajoittaa, mutta sellaisen onnistumista ei voida täysin sulkea pois.

3 Äänestysprotokolla

3.1 Äänestysoikeuden valvonta

Äänestäjillä tai kokonaan vaalien ulkopuolisilla tahoilla ei ole käsityksemme mukaan mahdollisuuksia huijata systeemiä; ts. äänestää ylimääräisiä kertoja.

Vilpillinen virkailija voi muiden virkailijoiden fyysisen valvonnan tai huolellisuuden pettäessä äänestää kenen tahansa puolesta. Virkailija voi esimerkiksi antaa äänestämään tulevalle apurilleen useiden henkilöiden äänestystunnukset tai mahdollisesti jopa muuttaa oman tietokoneensa äänestyspäätteeksi. Tämän takia on ehdottoman tärkeää, että virkailijat huolehtivat tarkasti ohjeiden mukaan toistensa valvomisesta sekä hallussaan olevista salasanoista ja muusta materiaalista.

Äänestäjän pääseminen äänestyspaikalla äänestyskoppiin ei takaa sitä, että hän pystyisi siellä äänestämään, sillä vilpillinen virkailija on voinut yllä mainitussa tilanteessa jo aiemmin käyttää hänen äänestysoikeutensa. Äänestäjän voi olla mahdoton saada rehellisiäkään virkailijoita vakuuttuneeksi tästä, sillä he eivät voi tietää, onko äänestäjä mahdollisesti itse käynyt jo aikaisemmin äänestämässä vai onko joku muu äänestänyt hänen sijastaan.

3.1.1 Äänen myymisen estäminen

- Havaintoluokitus: 4

- Korjaava toimenpide: Äänestyskortin PIN-koodi pitää piilottaa paremmin.

Jos äänestäjällä on äänestyskopissa mukanaan kortinlukulaite ja hän tietää kortin PIN-koodin, hän saattaa pystyä tekemään äänestyskortista kopion. Jos henkilö ei itse äänestä, hänellä on 30 minuuttia aikaa myydä äänestykseen oikeuttava kortti jollekin äänestämään tulevalle. PIN-koodi on mahdollista selvittää, jos saa käsiinsä yhden salasanan ja pari tiedostoa tai äänestyspaikan fyysinen valvonta pettää.

Jos hyökkääjä onnistuu kirjoittamaan omia äänestyskortteja, hän saattaa pystyä tekemään myös kortin, jolla voi äänestää toisen vaalipiirin ehdokasta.

3.1.2 Virkailija- ja äänestyspääteyhteyksien valvonta

- Havaintoluokitus: 3
- Korjaava toimenpide: Järjestelmään voitaisiin lisätä automatisoitu seuranta, joka varoittaa, jos järjestelmään ilmaantuu ylimääräisiä virkailija- tai äänestyspäätteitä.

Vilpillinen henkilö, jolla on äänestysoikeutettujen hetuja, jonkin äänestyspaikan virkailijatunnukset, asiakasvarmenteen salasana, muutama tiedosto virkailijapäätteen CD:ltä, kortinlukija sekä älykortteja, voi kirjoittaa äänestykseen oikeuttavia äänestyskortteja. Jos tällä henkilöllä on lisäksi äänestyspäätteen avauskortti ja salasana, hän voi myös äänestää tekemillään äänestyskorteilla. Tällaisen väärinkäytöksen riski korostuu järjestelmän sisäpiiriläisten kohdalla.

Järjestelmää on syytä tarkkailla jatkuvasti myös muiden epäilyttävien tapahtumien varalta. Tällaisia ovat esimerkiksi liian nopeassa tahdissa tapahtuvat äänestykset tai äänestysoikeuskyselyt.

3.2 Vaalituloksen laskenta

- Havaintoluokitus: 2
- Korjaava toimenpide: Sisäinen ohjeistus laskennan aikaisesta toiminnasta. Lisäksi laskentapaikalla tulee olla riittävä määrä eri tahoja edustavia asiantuntijoita, jotka jaetaan kahteen rinnan toimivaan ryhmään. Molemmat ryhmät kääntävät itsenäisesti tarvitsemansa ohjelmat ja laskevat vaalituloksen omilla koneillaan.

Vaalitulokset laskeva ohjelma ei tuota todistusta tulosten oikeellisuudesta. On siis pystyttävä varmistumaan siitä, että tulokset lasketaan oikealla ohjelmalla. Turvallisuutta voidaan parantaa laskemalla tulos kahden eri ryhmän voimin.

Joukko järjestelmän sisäpiiriläisiä pystyy periaatteessa generoimaan kokonaan uuden, aidon näköisen sähköisen vaaliuurnan ja järjestämään siitä laskettavat vaalitulokset haluamikseen. On siis pystyttävä varmistumaan, että tulokset lasketaan oikeasta uurnasta. Hallussamme olevien dokumenttien avulla on vaikea arvioida kuinka suuri vilpillisten henkilöiden joukko tähän tarvittaisiin. Tämän takia on tärkeää, että uurnaa käsiteltäessä on läsnä tarpeeksi asiantuntijoita. (Ongelmalta oltaisiin voitu välttyä myös, jos valeuurnaa ei voitaisi täyttää oikeilta näyttävillä äänillä. Tähän oltaisiin päästy, jos kenelläkään muulla kuin äänestäjällä itsellään ei olisi pääsyä hänen sähköisiin äänestystunnuksiinsa.)

3.3 Vaalisalaisuuden säilyminen

- Havaintoluokitus: 3
- Korjaava toimenpide: Sisäinen ohjeistus sähköisen uurnan ja sen salaisen avaimen generoinnista ja säilytyksestä. Avainta generoitaessa ja sähköistä uurnaa käsiteltäessä paikalla tulee olla riittävä määrä eri tahoja edustavia asiantuntijoita.

Yksittäisen äänestäjän äänen voi selvittää, jos saa haltuunsa kopion sähköisestä vaaliuurnasta ja äänten salauksen purkuun tarvittavan avaimen. Uurnaan pääsevät käsiksi järjestelmää ylläpitävät asiantuntijat. Uurnanavausavain talletetaan sen generoinnin jälkeen kassakaappiin. Avaimen voivat saada haltuunsa henkilöt, joilla on pääsy kyseiseen kassakaappiin ja jotka pystyvät kiertämään sinetöinnit. Samoin tämä onnistuu henkilöltä, joka on onnistunut vaihtamaan avaimen käsittelyyn käytettävää ohjelmakoodia tai pystynyt asentamaan avainta käsittelevään koneeseen omaa koodiaan.

Äänten miksauksen suorittava ohjelma "näkee" minkä äänen äänestäjä antoi. Tässäkin kohdassa pitää siis luottaa siihen, että käytössä on varmasti oikea ohjelmisto.

Lisäksi on muistettava, että äänestäjien äänet ovat selvitettävissä niin kauan, kunnes kaikki kopiot sähköisestä uurnasta tai uurnanavausavaimista on tuhottu. Vaalien elektroniset uurnat ja uurnanavausavaimet on tarkoitus arkistoida useiksi vuosiksi.

3.3.1 Äänten sekoittaminen

- Havaintoluokitus: 4
- Korjaava toimenpide: Mahdollisesti valittava suurempi erä ääniä kerrallaan sekoitettavaksi.

Ennen äänten laskemista ne sekoitetaan tuhannen äänen erissä. Vaalisalaisuus ei välttämättä säily, jos samaan erään sattuu vain vähän samalta äänes-

tyspaikalta annettuja ääniä tai erään sattuu 1 ennakkoääni ja 999 varsinaisena äänestyspäivänä annettua ääntä. Tässä epätodennäköisessä tilanteessakin vaalisalaisuus on turvassa, jos kaikki toimivat annetun ohjeistuksen mukaan.

3.3.2 Uurnan salaisen avaimen säilytys vaalin aikana

- Havaintoluokitus: 5
- Korjaava toimenpide: Toimintojen yksinkertaistaminen.

Auditoitavan systeemin kuvauksessa salainen uurnanavausavain jaetaan osiin ja osat talletetaan älykorteille. Älykortit ja ne avaavat PIN-koodit laitetaan kaikki samaan kassakaappiin säilöön. Avaimen jakamisesta osiin ei ole mitään hyötyä, jos kaikkia osia säilytetään samassa paikassa. Samoin PIN-koodit ovat turhia, jos niitä säilytetään yhdessä korttien kanssa.

3.4 Yhteenveto

Auditoidun systeemin luotettavuus perustuu pitkälti olettamukseen, että vaalivirkailijat pystyvät havaitsemaan kaikki äänestäjien ja muiden virkailijoiden tekemät vilppiyritykset niin äänestyspaikalla kuin ääntenlaskupaikalla. Ei tietenkään ole mitään syytä epäillä, etteikö koko vaaleja järjestävä henkilöstö toimisi asiaan kuuluvalla rehellisyydellä ja tarkkaavaisuudella. Sen sijaan voidaan epäillä, *saadaanko vaalivirkailijoiksi värvättyä riittävästi tietotekniikan perusteet hallitsevaa väkeä,* jotta mahdolliset vilppiyritykset olisi mahdollista havaita.

Yleisesti ottaen voidaan arvioida, että todennäköisyys vilppiyritysten esiintymiselle on Suomessa varsin pieni. Toisaalta onnistuneen vilpin seuraukset olisivat radikaaleja, ainakin jos vilppiyritys tehtäisiin ääntenlaskuvaiheessa. Voidaan myös ajatella, että kyseisen systeemin käyttö joissakin maissa herättäisi vahvan epäilyn tulosten luotettavuudesta. Sijoittamalla vain muutaman ”sopivan” henkilön järjestelmän avainpaikoille pystyisi vaalien tulokset muokkaamaan tarkalleen haluamikseen ja käytännössä ilman kiinnijäämisen riskiä.

Oikeusministeriö lienee oikea taho arvioimaan, onko riskien todennäköisyys riittävän pieni suhteessa riskien mahdollisen toteutumisen aiheuttamiin vahinkoihin.

4 Toteutus

4.1 Huomioita koodista yleisesti

Vaalijärjestelmän pilottiversion auditointiin liittyvä varsinainen koodi jakaantuu pääasiallisesti kahteen suurempaan kokonaisuuteen:

- Itse varsinaisen äänestysjärjestelmän ytimen muodostava koodi, kuten keskitetysti sijoitetun palvelinjärjestelmän äänestystapahtumiin ja sähköiseen uurnaan liittyvä koodi;
- Edellä mainitun ohjelmiston soveltamiseen liittyvä koodi, kuten äänestys- ja virkailijapäätteiden ja näiden palvelinohjelmistoon yhdistämiseen tarvittava koodi.

Koko vaalijärjestelmän kokoonpanoon kuuluu paljon muuta koodia suurimman osan sisältyessä valmisohjelmistoihin, joita ei ole sisällytetty tähän auditointiin koodin osalta. Varsinaisen äänestysjärjestelmän ytimen muodostavaa koodia on tarkasteltu kriittisiksi arvioiduilta osin. Edelleen on tarkastettu äänestysjärjestelmän päätteiden sovellusten sekä palvelintason kriittisten salauskomponenttien lähdekoodi.

Joltain kohdin tarkasteltu lähdekoodi on pirstaleista ja osin puutteellisesti kommentoitua, mikä heikentää luettavuutta etenkin auditointia ajatellen. Koodi itsessään on toimivaa, vaikkakin jotain pientä ohjelmointiteknistä huomautettavaa löytyy.

4.2 Pnyx.core

Varsinaisen äänestysjärjestelmän sähköisen uurnan ja äänestysjärjestelmässä käytettävän keskuspalvelimen koodi sisältää paljon kohtia, joista osa ei ole tämän auditoinnin osalta oleellisia: pilotissa ei tulla käyttämään kaikkia järjestelmän ytimeksi toimitettuun ohjelmistoon implementoituja toimintoja ja ratkaisuja. Yleisesti kokonaisuuksina toimitettuihin ohjelmistoihin liittyy usein käytettävyyteen ja muokattavuuteen liittyviä teknisiä ongelmia. Äänestysjärjestelmän palvelintason ohjelmiston rakenteen ansiosta tämä ei tuota koodin käyttämiseen liittyviä merkittäviä ongelmia. Olisi tietenkin suotavaa, ettei näin kriittiseen käyttöön tarkoitetussa järjestelmässä olisi ylimääräista koodia.

4.3 TietoEnator

Kuten varsinaisen äänestysjärjestelmän kohdalla, myös toimitetussa äänestysjärjestelmän ytimen käyttämiseen liittyvässä koodissa on käyttämätöntä testaukseen liittyvää koodia, jota ei ole tarkoitettu lopulliseen käännösversioon. Äänestys- ja virkailijapäätteiden käyttöjärjestelmän osalta on tarkasteltu käyttöjärjestelmän mahdollistamia väärinkäytön vaihtoehtoja. Käytettyyn Knoppix-käyttöjärjestelmään on tehty muutoksia ja rajoituksia väärinkäytön estämiseksi, mutta lopullisen version puuttuminen on ongelma.

Mainittakoon vielä, että virhetilanteiden käsittelyyn on kiinnitetty melko hyvin huomiota. Osassa virhetilanteita kuitenkin informatiivisempi virhetilanteen käsittely olisi paikallaan, kuten esimerkiksi verkkoliikenteeseen

liittyvissä virheissä, joissa paikallinen atk-tukihenkilö mahdollisesti pystyisi olemaan avuksi.

4.3.1 Ohjelmistoversioiden hallinta

- Havaintoluokitus: 3
- Korjaava toimenpide: Riittävä määrä tarpeeksi asiantuntevia henkilöitä pitää olla paikalla, kun ohjelmistoja asennetaan.

On tärkeää että kaikista ohjelmistoista käytetään juuri oikeaa, tarkastettua versiota. Tähän ei ole juuri muita toteuttamiskelpoisia tapoja kuin ohjelmien kääntäminen tarpeeksi monen henkilön voimin. Myös äänestys- ja virkailijapäätteiden käynnistyslevyjä koottaessa on tärkeää, että levyt sisältävät oikeat versiot oikeista ohjelmista.

4.4 Knoppix-CD

- Havaintoluokitus: 2
- Korjaava toimenpide: Lopullinen versio käyttöjärjestelmälevyistä.

Käyttöjärjestelmälevyjen kehitystyö on vielä kesken. Käyttöjärjestelmällä on olennainen rooli järjestelmän turvallisuudessa.

5 Tietoliikennejärjestelyt

5.1 Äänestyspaikkojen ja toimittajan verkkojen väliset yhteydet

Yhteyksissä äänestyspaikalta toimittajan verkkoon käytetään julkisia verkkoja (äänestyspaikan olemassaolevaa Internet-verkkoyhteyttä), joiden läpi informaatio kuljetetaan pakettimuotoisena IP-protokollaa (IPv4) käyttäen.

5.1.1 Toteutuksen tietoturvan ja toiminnan varmuuden kestävyys

- Havaintoluokitus: 4
- Keskeisin uhka: Palvelukatkos, jonka seurauksena siirrytään käyttämään varajärjestelmää (lippuäänestys).Vaalisalaisuus ei vaarannu katkon seurauksena.
- Korjaava toimenpide: Selvityspyyntö yhteysvälin operaattoreilta, mikäli nähdään tarpeelliseksi.

Verkkoa pitkin kuljetettava informaatio on voimakkaasti salattua sekä sovelluskerroksessa että kuljetuskerroksessa, joten vaalisalaisuuden voidaan katsoa olevan tältä osin varmistetun.

Yhteyksien toimintavarmuuden ja verkkokerroksen tietoturvan osalta (IP-osoitteiden ja TCP-porttien selväkielisyys) keskeisessä asemassa ovat tietoliikenneyhteydet järjestäneet operaattorit. Molemmat osa-alueet riippuvat operaattorista ja operaattorilta hankitusta palvelukokonaisuudesta. Operaattori saattaa esimerkiksi tarjota keskitettyjä tietoturvaratkaisuja, mutta näiden osalta ei voida tehdä olettamuksia.

Yleisesti ottaen Suomessa internet-palveluntarjoajien järjestämät tietoliikenneyhteydet ovat varmatoimisia. Normaalissa toimintatilanteessa lyhyitä satunnaisia katkoksia voi kuitenkin esiintyä. Mahdollisen katkoksen seurauksena joudutaan siirtymään varajärjestelmän käyttöön (lippuäänestys). Mahdollinen käyttökatko tietoliikenneyhteyksissä ei vaaranna vaalisalaisuutta jo annettujen sähköisten äänten osalta.

Tarkasteltaessa kaupallisten yhteyksien toimintavarmuutta viime vuosien aikana voidaan arvioida, että laajamittaisen ja pitkäkestoisen katkoksen todennäköisyys vaalipilotin aikana on hyvin pieni. Jonkin tietyn operaattorin keskeisiin laitteisiin kohdistuva tietoturvahyökkäys, esimerkiksi palvelunestohyökkäys, on kuitenkin aina mahdollinen. Myös esimerkiksi yhteysvälillä toimivan operaattorin ylläpitämiin www-palvelimiin kohdistuva hyökkäys voisi vaikuttaa sähköisessä vaalissa käytettävien tietoliikenneyhteyksien toimintavarmuuteen.

Yhteysvälillä olevilta operaattoreilta voidaan pyytää selvitys yhteysvälin tietoturvajärjestelyjen tasosta ja esim. verkon toiminnan kannalta keskeisten laitteiden fyysisestä suojauksesta.

5.1.2 Järjestelmään tunkeutumisen ja toimintaan puuttumisen estäminen

- Havaintoluokitus: 4
- Keskeisin uhka: Palvelunestohyökkäys, josta seuraa tietoliikennekatkos, jonka seurauksena siirrytään käyttämään varajärjestelmää (lippuäänestys). Vaalisalaisuus ei vaarannu katkon seurauksena.
- Korjaava toimenpide: IPSec-määritelmään perustuva tunneloitu VPN-yhteys äänestyspaikan ja äänestysjärjestelmän välillä, mikäli tämä nähdään tarpeelliseksi.

Kts. Edellinen kohta. Eri palveluntarjoajien aliverkoista koostuvalla yhteysvälillä verkon keskeisiin laitteisiin tunkeutumisen ja niiden toimintaan puuttumisen estäminen on kunkin kyseessä olevan operaattorin vastuulla. Mahdollinen tunkeutuja pyrkisi onnistuessaan todennäköisesti joko estämään liikennettä (siis katkaisemaan tietoliikenneyhteyden äänestyspaikan ja äänes-

tysjärjestelmän välillä), tai salakuuntelemaan liikennettä muokkaamatta sitä. Jälkimmäisessä tapauksessa tunkeutuja voisi enimmillään saada selville kommunikoivien laitteiden IP-osoitteet ja paikallisten sovellusten TCP-portit, sillä kuljetettava informaatio on salattua sekä verkon sovellus- (OSI-kerros 7) että kuljetuskerrosten (OSI-kerros 4) hyötykuorman osalta. IPSec-määritelmään perustuva tunneloitu VPN-yhteys äänestyspaikan ja äänestysjärjestelmän välillä estäisi kommunikoivien laitteiden IP-osoitteiden ja paikallisten TCP-porttien selvittämisen, mikäli tämä nähdään tarpeelliseksi. Tällöin mahdollinen salakuuntelija pystyisi enää selvittämään tunnelin päätepisteiden IP-osoitteet, ei itse kommunikoivien asemien.

5.1.3 Vaaliorganisaation ohjeistus poikkeustilanteiden varalle

- Havaintoluokitus: 5
- Korjaava toimenpide: Ohjeistuksen tarkentaminen tietoliikennehäiriöiden osalta.

Dokumentin *Äänestyspaikan tekninen opas* lopussa olevassa *Ongelmatilanteet*-osiossa ei käsitellä lainkaan tietoliikennevioista johtuvia ongelmia. Ohjeen osassa 3 tosin annetaan ohjeet yhteyksien testaamiselle.

5.2 Toimittajan sisäisen verkon suunitteludokumentit

Tietoliikennejärjestelyjen osalta toimittajan sisäisen verkon tekniikka on kuvattu dokumentissa *Sähköisen äänestyksen tuotantoympäristön kuvaus*. Toimittajan sisäisessä verkossa käytetään yksityisen verkon IP-osoitteita, kaupallisia (sertifioituja) palomuuri- ja IDP-ratkaisuja ja sähköisten äänten siirtämisen osalta salattuja yhteyksiä.

5.2.1 Toteutuksen tietoturvan ja toiminnan varmuuden kestävyys

- Havaintoluokitus: 4
- Keskeisin uhka: Tietoturvaan julkisesta verkosta kohdistuva hyökkäys, josta seuraa tietoliikennekatkos, jonka seurauksena siirrytään käyttämään varajärjestelmää (lippuäänestys). Vaalisalaisuus ei vaarannu katkon seurauksena. Epätodennäköisemmät uhat kohdistuvat lähinnä toimitilojen fyysiseen tietoturvaan.
- Korjaava toimenpide: Järjestelyt ovat riittävät sähköisen vaalin pilottia varten. Mahdollisten tietoturvaan kohdistuvien hyökkäysten näkökulmasta tuotantojärjestelmä on asianmukaisesti suojattu ja se voidaan tarpeen vaatiessa irrottaa julkisesta verkosta ja äänestyspaikoilla voidaan siirtyä käyttämään varajärjestelmää (lippuäänestys). Fyysisen

tietoturvan osalta keskeistä on vaalinaikainen toimitilojen kulunvalvonta sekä konfigurointi- ja laskentalaitteiden laillisen käytön varmistaminen.

Äänestyksen päätyttyä sähköinen uurna siirretään joko siirrettävää sähköistä (USB-muisti tms.) tai siirrettävää optista (CD-ROM, DVD-ROM) mediaa käyttäen tietoverkoista erillään olevaan laitteistoon vaalituloksen purkamista varten. Laitteet, joiden välillä siirto tehdään, sijaitsevat samassa kulunvalvotussa tilassa. Fyysisten tietoturvajärjestelyjen voidaan tältä osin todeta olevan riittävät.

Itse äänestysjärjestelmän sijaintipaikan fyysistä tietoturvaa (kulunvalvonta, vartiointi tms.) ei ole kuvattu kovin tarkasti. Sijaintipaikan vaalinaikainen fyysinen tietoturvallisuus vaatii oman määritelmänsä pilotin onnistumisen varmistamiseksi.

Tuotantoympäristössä on käytössä järjestelmä, jossa on kahdennetut palvelimet (toinen "kylmänä", käyttöönottoajaksi arvioidaan 0,5-2h tilanteen vaatiessa). Käyttöön valittu palomuurijärjestelmä on sertifioitu toimialueen ulkorajakäyttöön. Palomuurijärjestelmään sisältyy IDS-toiminto, mutta vaalien tuotantojärjestelmässä tätä ei käytetä, vaan tilalle on valittu erillinen IDP-järjestelmä. Palomuurisäännöissä määritellään tietyt sallitut IP-osoitealueet äänestyspaikoille, ja IDP-järjestelmä määritetään sallimaan vain tiettyjen sovellusten (äänestyssovellusten) liikenne. Tältä osin järjestelyjen voidaan katsoa olevan riittävät.

Äänestyspalvelimien IP-osoitteita ei julkisteta tietoturvallisuuden lisäämiseksi ja hyökkäysten ehkäisemiseksi. Tämä ratkaisu ei kuitenkaan sulje pois mahdollisuutta selvittää IP-osoitteet liikenneanalyysillä.

5.2.2 Järjestelmään tunkeutumisen ja toimintaan puuttumisen estäminen

Fyysisen tietoturvan, palomuurin ja IDP-järjestelmän osalta kts. edellinen kohta.

Äänestysjärjestelmän ja VAT-järjestelmän välisessä tietoliikentessä osassa yhteysmuodoista käytetään salausta, osassa ei. Tämä liikennöinti tapahtuu kuitenkin toimittajan palomuurin ja IDP-järjestelmän suojaamassa sisäisessä verkossa. Vaikka salaus ei tästä syystä ole välttämätöntä, tulisi sen käyttöönottoa harkita johdonmukaisuuden vuoksi.

5.3 Äänestyspaikan sisäisen verkon ohjeistus ja toteutus

Tältä osin arvio perustuu dokumentteihin *Arkkitehtuuri* ja *Äänestyspaikan tekninen opas*.

5.3.1 Toteutuksen tietoturvan ja toiminnan varmuuden kestävyys

- Havaintoluokitus: 4
- Keskeisin uhka: Tietoliikennekatkos, jonka seurauksena siirrytään käyttämään varajärjestelmää (lippuäänestys). Vaalisalaisuus ei vaarannu katkon seurauksena.
- Korjaava toimenpide: IPSec-määritelmään perustuva tunneloitu VPN-yhteys äänestyspaikan ja äänestysjärjestelmän välillä, mikäli tämä nähdään tarpeelliseksi. Toimenpiteet fyysisen tietoturvan varmistamiseksi.

Äänestyspaikan sisäisten tietoliikennejärjestelyjen toimintavarmuus ja tietoturvallisuus riippuvat hyvin paljon äänestyspaikalle rakennetun tietoverkon infrastruktuurista. Paikalla voi olla kaapeloitu verkko tai langaton verkko, pinta-asennuksena kaapelikouruihin asennetut sähkö- ja tietoverkkojohdot tai keskitetyt johtokuilut ja seinien sisään putkitetut kaapelivedot. Kaapeloitu verkko, jossa johdot kulkevat pinta-asennuksena esim. kaapelikouruissa, ovat altteimmat fyysiselle sabotaasille (esim. johtojen katkaiseminen).

Äänestyspaikan verkkoon pääsyn omaava henkilö voi esimerkiksi pyrkiä ylikuormittamaan verkkoa massiivisella tiedonsiirtovolyymilla tai salakuuntelemaan verkkoliikennettä liikenneanalyysiä varten. Liikenneanalyysillä voitaisiin mahdollisesti selvittää kommunikoivien laitteiden IP-osoitteet ja TCP-portit. Itse kuljetettavaa äänestysdataa ei pystytä kuitenkaan selvittämään käytössä olevien salausjärjestelyjen vuoksi. Liikenneanalyysiä voitaisiin vaikeuttaa käyttämällä VPN-tunnelia äänestyspaikan ja äänestysjärjestelmän välillä.

Yleisesti ottaen sähköisessä äänestyksessä äänestyspaikan järjestelyissä on perinteiseen äänestystapaan verrattuna huomattavasti enemmän tapoja, joilla äänestyksen toimintavarmuutta ja tietoturvallisuutta voidaan pyrkiä heikentämään merkittävää huomiota herättämättä.

5.3.2 Järjestelmään tunkeutumisen ja toimintaan puuttumisen estäminen

- Havaintoluokitus: 4
- Keskeisin uhka: Tietoliikennekatkos, jonka seurauksena siirrytään käyttämään varajärjestelmää (lippuäänestys). Vaalisalaisuus ei vaarannu katkon seurauksena.
- Korjaava toimenpide: Ohjeistus vaalipaikan fyysisten tietoturvajärjestelyjen tarkistamiselle vaalipäivänä ennen päätteiden avaamista ja vaalitapahtuman aikana.

Järjestelmän toimintaan puuttumisen ehkäisemisen kannalta on keskeistä, että vaalipäivänä suoritetaan tietoliikenneyhteyksien fyysisen tietoturvan tarkastus ja muiden ATK-tilojen kuin äänestystilan lukituksen varmistus sekä ennen äänestyspäätteiden avaamista että useita kertoja vaalipäivän aikana. Tällä voidaan varmistaa, että ennen päätteiden avaamista kukaan ei ole päässyt tekemään omia kytkentöjään tai esimerkiksi päässyt johonkin ATK-tilaan sisään häiritäkseen tai salakuunnellakseen tietoliikennettä. Tämä on oleellista pilotin onnistumisen varmistamisen kannalta. Samoin vaalipäivän aikana tulisi useita kertoja varmistaa, että kytkentäkaapit ovat lukittuja, kytkentöihin ei ole tehty muutoksia ja että ATK-tilat ovat tyhjiä ja lukittuja.

6 Virkailijoiden ohjeistus

Äänestystapahtuma kaikkine mahdollisine tarkastuksineen ja virhetilanteineen on erittäin monimutkainen ja vaatii virkailijoilta vähintäinkin kohtuulliset tiedot tietokoneiden käytöstä ja lisäksi perusteellisen opetuksen. Kaikkea tietokoneisiin liittyvää ei saa jättää yhden ATK-tuen harteille. Kaikkia toimintoja pitäisi olla seuraamassa ainakin kaksi virkailijaa, jotka molemmat ymmärtävät, mitä koko ajan tapahtuu. Myös salasanojen ja muun materiaalin huolellista käsittelyä on syytä painottaa.

Kaikenkaikkiaan virkailijoiden ohjeistus oli vielä erittäin keskeneräinen (esim. virkailijapäätteen sulkeminen) ja virkailijoiden koulutuksen sisältö ei ollut auditoijien tiedossa.

Liite A

Protokollan auditoinnissa olivat käytössä seuraavat dokumentit:

- Pnyx.core functional description v.1.7.1b
- Arkkitehtuuri v.1.4H (17.1.2008)
- Auditoijan opas v.0.94K (31.1.2008)
- Tekninen toteutus ja tietoturvaratkaisut v.1.0E (12.6.2007)
- Äänestyspaikan tekninen opas v.1.31E (23.5.2008)
- Vaalien perustaminen, sähköisen uurnan avaus ja tulosten laskenta v.1.0E (7.4.2008)
- Arkistointikäytännöt v.1.1H (17.4.2008)
- Testaussuunnitelma v.2.0H (6.3.2008)

- Sähköisen äänestyksen tuotantoympäristön kuvaus v.1.0E (19.2.2008)
- Sähköinen äänestämisen testaus -kalvosetti (Oikeusministeriö 12.3.-28.3.2008)

Lisäksi joitakin asioita on jouduttu tarkastamaan lähdekoodeista ja ohjelmistoja testaamalla.

Liite B

Asteikko havaintojen kriittisyydelle:

1. Erittäin kriittinen. Kunnallisvaalien pilotointi ei ole mahdollista ilman korjaavia toimenpiteitä. Pilotoinnin suunnitellut tietoturvatoimenpiteet eivät ratkaise havaittua uhkakuvaa.
2. Kriittinen. Kunnallisvaalien pilotointia ei tulisi tehdä ilman korjaavia toimenpiteitä. Pilotoinnin muut suunnitellut tietoturvatoimenpiteet pienentävät kuitenkin merkittävästi uhkakuvan todennäköisyyttä.
3. Tärkeä. Korjaavat toimenpiteet tulisi tehdä ennen vaaleja. Havaittu riski on vähäinen ja/tai muut suunnittellut tietoturvatoimenpiteet käytännössä ehkäisevät uhkakuvan toteutumisen.
4. Rajallinen. Korjaavia toimenpiteitä ei ole tarpeen tehdä kunnallisvaaleihin 2008. Muut tietoturvatoimenpiteet ehkäisevät uhkakuvan toteutumisen, havaitun riskin vaikutus on vähäinen ja/tai uhkakuvan toteutuminen on hyvin epätodennäköinen.
5. Yleinen havainto. Havainnolla ei ole suoraa vaikutusta sähköisen äänestyksen oikeellisuuteen tai tietoturvallisuuteen. Havainto liittyy esimerkiksi tietojärjestelmien tai toimintaohjeiden laatuun, tai tuotteiden sellaisiin ominaisuuksiin, joita ei käytetä pilotoinnissa.

Liite C

Auditointityöryhmä:

- Professori Juhani Karhumäki, vastuullinen johtaja
- FT Tommi Meskanen, koordinointi ja yleistarkastelu sekä kryptografisten protokollien analysointi 2 kk
- TkT Seppo Virtanen, tietoliikennejärjestelyt 0,5 kk
- FT Arto Lepistö, lähdekoodin analysointi ja yleistarkastelu 2 kk
- FL Petri Salmela, Knoppix-käyttöjärjestelmä 1 kk

- FT Ari Renvall, kryptografisten protokollien analysointi 0,5 kk
- FM Sami Mäkelä, lähdekoodin tarkastaminen 2 kk
- fil. yo. Tommi Penttinen, lähdekoodin tarkastaminen, sovellusten ja vaalien aikaisen toiminnan tietoturvan analysointi 2 kk
- Akatemiaprofessori Hannu Nurmi, vaaliasiantuntija

Auditointiryhmä koostuu Turun yliopiston henkilöistä. Ryhmän johtaja Juhani Karhumäki toimii matematiikan laitoksella diskreetin matematiikan professorina. Akatemiaprofessori Hannu Nurmi on maamme johtavia vaaliasiantuntijoita. Kryptografisten protokollien analysoinnista vastanneet FT Ari Renvall ja FT Tommi Meskanen ovat Turussa kryptografiasta väitelleitä tutkijoita. Renvallin väitöskirjan aiheena oli nimenomaan sähköiset vaalit. Tietoliikenneratkaisujen osalta auditoinnin suoritti TkT Seppo Virtanen. Ohjelmakoodin ja käyttöjärjestelmän tarkistustyön päävastuu oli FT Arto Lepistöllä. Hänen apunaan toimivat piakkoin väittelevät Petri Salmela ja Sami Mäkelä sekä maisteriopiskelija Tommi Penttinen.

Liite D

Auditoinnin toteutus:

Auditointityö suoritettiin Turun yliopiston matematiikan laitoksella. Työryhmän kokoonpano ja vastuualueet on kuvattu liitteessä C. Työhön käytettiin yhteensä 10 henkilötyökuukautta. Se toteutettiin tähän tarkoitukseen varatussa huoneessa, jonne oli pääsy ainoastaan auditointiryhmän jäsenillä. Ohjelmakoodia käsiteltiin tätä tarkoitusta varten hankituilla tietokoneilla, jotka eivät olleet kytkettyinä verkkoon.

Seuraavassa on lyhyesti kuvattu auditoinnin keskeiset osa-alueet.

Projektissa tarkastettiin käytetyt kryptografiset protokollat ja niiden soveltuminen sähköiseen äänestykseen. Samalla arvioitiin pilottia suhteessa manuaaliseen äänestykseen sekä muihin sähköisiin äänestysjärjestelmiin.

Tietoliikennejärjestelyjen osalta on auditoitu äänestyspaikkojen ja sähköisen äänestyksen toimittajan verkkojen välisten tietoliikenneyhteyksien suunnitteludokumentit, sähköisen äänestyksen toimittajan sisäisen tietoliikenneverkon suunnitteludokumentit ja äänestyspaikan sisäisen tietoliikenneverkon ohjeistus ja toteutus.

Auditoijille toimitetut vaalien perustamiseen, valvomiseen ja ääntenlaskentaan liittyvät dokumentit on käyty läpi ja niiden ohjeistus on tarkastettu.

TietoEnatorin toimittama sekä Scytlin pnyx.core-tuotteen kriittisten tietoturvakomponenttien lähdekoodi tarkastettiin ja sitä arvioitiin tiedon kapselointia ja eheyttä sekä ohjelmien toiminnan riittävyyttä ja välttämättömyyttä silmällä pitäen. Toisin sanoen, haluttiin selvittää, tekevätkö ohjelmat sen, mitä niiden pitääkin, ja vain sen.

Projektin aikana tarkasteltiin myös virkailija- ja äänestyspäätteiden tietoturvaa selvittämällä muun muassa, mitkä ovat riittävät ja välttämättömät ehdot niiden käyttämiseksi joltain toiselta koneelta. Vastaavasti tarkasteltiin myös informaation, kuten äänestäjätietojen, muokkausmahdollisuuksia protokollan eri vaiheissa.

Vaalien aikaisen toiminnan, kuten virkailijoiden välisen vuorovaikutuksen, säätelyllä on suuri vaikutus äänestysprosessin onnistumiseen. Projektissa tarkasteltiinkin kriittisesti myös vaalien fyysisiä puitteita ja niiden vaikutusta äänestystilanteen tietoturvaan.

Projektin psta
Turussa 13.6.2008

Juhani Karhumäki
Projektin vastuullinen johtaja

Tommi Meskanen
Yliassistentti