Satakunnan ammattikorkeakoulu

Antti Kekki

WWW-POHJAISEN ÄÄNESTYSJÄRJESTELMÄN TIETOTURVAN JA LUOTETTAVUUDEN ARVIOINTI

Tietojenkäsittelyn koulutusohjelma

2007

WWW-POHJAISEN ÄÄNESTYSJÄRJESTELMÄN TIETOTURVAN JA LUOTETTAVUUDEN ARVIOINTI

Kekki, Antti
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Grönholm, Jukka
Huhtikuu 2007
UDK: 004.056, 004.738.52, 342.8
Sivumäärä: 81

Asiasanat: tietojärjestelmät, tietoturva, WWW

Tämän opinnäytetyön aiheena oli tutkia WWW-äänestysjärjestelmän käytön mahdollisuuksia yhdistyksissä, opiskelijakunnissa ja ylioppilaskunnissa. Aihetta lähdettiin tutkimaan näitä yhteisöjä koskevan lainsäädännön sekä vaalien yleisten vaatimusten näkökulmasta. Tavoitteena oli selvittää lainsäädännön asettamat vaatimukset WWW-pohjaiselle äänestämiselle rajatussa toimintaympäristössä, tutkia tietojärjestelmän eri osien tietoturvariskit vaalisalaisuuden säilymisen ja vaalituloksen eheyden näkökulmasta sekä tutkia äänestysjärjestelmän antaman vaalituloksen luotettavuuden varmistamista ohjelmiston laadunvalvonnan keinoin.

Tietojärjestelmän turvallisuutta lähdettiin arvioimaan pilkkomalla WWW-äänestysjärjestelmä osakokonaisuuksiin, joiden tietoturvauhkia tutkittiin nykyisen tietoturvatilanteen kautta. Äänestysjärjestelmäohjelmiston tietoturvaa tutkittiin ohjelmistosuunnittelun ja lähdekoodin yleisimpien tietoturvavirheiden kautta. Ohjelmiston luotettavuuden varmistamista lähdettiin tutkimaan tietojärjestelmäprojektin laadunvarmistusmetodien kautta analysoimalla tietojärjestelmädokumentaation ja testauksen sekä ylläpidon laadun osatekijöitä.

Äänestysjärjestelmän palvelinpään tietoturvan voi pitää hyväksyttävällä tasolla jatkuvan asiantuntevan ylläpidon ja seurannan sekä ohjelmistojen ja laitteiden tietoturvallisen konfiguroinnin avulla. Vaalin järjestäjä ei sen sijaan voi varmistua äänestäjän Internet-päätteen tietoturvasta, joten vaalisalaisuutta ei voi taata WWW-äänestämisessä.

Äänestysjärjestelmän tuloksen oikeellisuuden varmistaminen onnistuu riittävän tehokkaasti kun määrittelydokumentaation vastaa täysin asiakkaan odotuksia ja kaikesta testaustoiminnasta jää täydelliset dokumentaatiot asiakkaan tarkastelua varten. Myös ohjelmiston ylläpito tulee olla suunniteltu.

WWW-äänestysjärjestelmää ei voi suositella käyttöön vaalisalaisuuden vaarantumisen takia. Lisäksi luotettavan äänestysjärjestelmän luominen vaatii kokenutta toimittajaa ja erittäin huolellista määrittely- ja testausprosessia. Tämä nostaisi ohjelmiston kustannukset tarkoitetun käyttäjäryhmän maksukyvyn ulkopuolelle. Kokonaisuutena WWW-äänestysjärjestelmän käytön suurin este on äänestäjän mahdottomuus varmistua järjestelmän toiminnasta. Oman äänen tallentumista ja laskennassa huomioon ottamista ei voi mitenkään todistaa äänestystilanteessa. Tämä tuhoaa vaalin uskottavuuden. Lakiteknisiä esteitä järjestelmän käytölle ei ole.

EVALUATION OF DATA SECURITY AND RELIABILITY OF INTERNET BASED VOTING SYSTEM

Kekki, Antti
Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
Grönholm, Jukka
April 2007
UDK: 004.056, 004.738.52, 342.8
Number of pages: 81

Key words: information systems, data security, WWW

The purpose of this thesis was to explore possibilities of using Internet based voting system in associations and in student unions. Subject was explored from point of view of legislation that controls associations and student unions and from point of view of general requirements of elections. Intention was to clarify the requirements that are set by legislation to Internet based voting in selected user environment, to explore threats posed to secrecy of the vote and to integrity of election returns by data security threats of voting information system and to explore ways to be ensure the reliability of election returns that voting systems produces by means of software quality assurance.

Security voting system was analysed by splitting the Internet based voting system to smaller sub assemblies and by measuring data security threats by examining present security situation of that part. Security was analysed by identifying common security mistakes in system design and in source code. Assuring the software integrity was explored trough software quality assurance methods of information system project by analysing components of quality that form high quality information system documentation, testing and maintenance.

Voting systems server side security can achieve acceptable level with constant and professional maintenance and by configuring hardware and software in secure way. On the contrary, election organiser has no way to assure that client side security is in order and that it does not threat secrecy of the vote.

Required confidence of election returns produced by voting system can be achieved when information system documentation fulfils all users needs and when complete documentation of testing can be accessed.

Usage of Internet based voting can not be recommend because of the security threat it poses to secrecy of the vote. Another problem is that creation of high quality voting system requires experienced software supplier and thorough design and testing process. This can lead to situation where expenses of the voting software becomes too high to target user group. As a whole, biggest problem in Internet based voting system is that voter is unable to verify how voting system functions. There is no way to prove that voters vote is registered and that it is really counted. This effectively destroys credibility of the election. There is no obstacles placed by legislation on using Internet based voting system.

SISÄLLYS

1. JOHDANTO....5
2. RAKENNE JA VAATIMUKSET....6
3. KÄYTÖN MAHDOLLISUUDET JA RAJOITUKSET....8
4. TIETOTURVA....12
4.1 Mitä on tietoturva?....12
4.2 Tietomurron riski....14
4.3 Tietoturvaan vaikuttavat asiat....16
4.4 Tietoturvan arviointi....20
4.4.1 Käyttäjän Internet-selain....20
4.4.2 Käyttäjän käyttöjärjestelmä....23
4.4.3 Käyttäjän laitteisto....25
4.4.4 Käyttäjän lähiverkko....25
4.4.5 Internet....26
4.4.6 WWW-palvelimen lähiverkko....27
4.4.7 WWW-palvelimen laitteisto....29
4.4.8 WWW-palvelimen käyttöjärjestelmä....32
4.4.9 WWW-palvelimen WWW-palvelinohjelmisto....35
4.4.10 WWW-palvelinohjelmiston palvelinlaajennus....36
4.4.11 Tietokantapalvelinohjelmisto....38
4.4.12 Äänestysjärjestelmä....40
4.5 Yleiset toimintaympäristöt....51
4.6 Tietoturvalliset toimintatavat ja tietoturvapolitiikat....55
5. TESTAUS JA LAADUNVARMISTUS....59
5.1 Ohjelmiston laatu....59
5.2 Laadunvarmistus....60
5.2.1 Määrittelydokumentaation laadun osatekijät....61
5.3 Laadunvarmistuksen toteuttaminen....64
5.3.1 Projektin hallinnon seuranta....64
5.3.2 Ohjelmiston testaus....65
5.3.3 Ylläpito....70
6. JOHTOPÄÄTÖKSET....72
LÄHTEET....75
LIITELUETTELO....80
KUVIOT....81

1. JOHDANTO

Tämän opinnäytetyön tarkoituksena on tutkia WWW-äänestysjärjestelmän käytön mahdollisuuksia ja rajoituksia opiskelijakunnassa ja yhdistyksessä. Tarve tähän selvitykseen syntyi vuosien 2005 ja 2006 aikana jolloin olin mukana Satakunnan ammattikorkeakoulun opiskelijakunnan (SAMMAKKO) hallituksessa. Varsinkin vuonna 2006 pohdimme paljon WWW-pohjaisen äänestysjärjestelmän käyttöönottoa opiskelijakunnassamme. Keskustelimme asiasta muiden opiskelijakuntien ja Suomen ammattikorkeakouluopiskelijayhdistysten liiton (SAMOK) edustajien kanssa. Todellisen tiedon epävarmuus oli ainoa asia joka näistä keskusteluista selvisi. Kaikkien näkemykset asiasta perustuivat ennemminkin mielipiteisiin kuin kokemuksiin ja tietoon. Tästä syystä päätin tehdä opinnäytetyöni tästä aiheesta näiden epäselvyyksien hälventämiseksi, varsinkin kun vuonna 2009 kaikki ammattikorkeakoulut siirtyvät käyttämään uutta yhteistä ProAMK-tietojärjestelmää, joka sisältää mahdollisuuden järjestää opiskelijakunnan vaaleja. WWW-äänestysjärjestelmät ovat siis tulossa osaksi opiskelijakuntien arkea ja tällöin tietämys Internetin kautta toimivan äänestyksen tuomista haasteista vaalisalaisuuden säilymiseen ja tuloksen luotettavuuden osalta on oltava selkeät kaikille. Tämän opinnäytetyön on tarkoitus luoda konkreettinen tarkastuslista ja pohjamateriaali WWW-äänestysjärjestelmän tietoturvan ja luotettavuuden arviointiin.

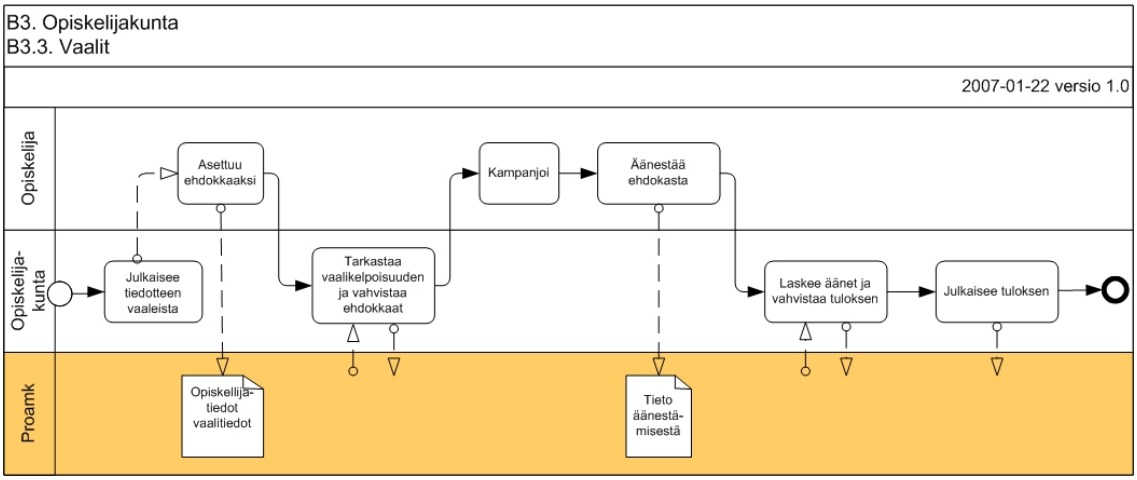
Tutkimuksen näkökulmaan ja rajaukseen vaikuttaa tuloksen suuntaaminen opiskelijakuntien käyttöön. Tuloksen avulla WWW-äänestysjärjestelmän laatua pystytään arvioimaan vaalisalaisuuden säilymisen ja vaalituloksen luotettavuuden näkökohdissa. Tämä työ keskittyykin tuottamaan näkökulman jonka avulla opiskelijakunta pystyy tietoteknisen asiantuntijan kanssa käymään läpi äänestysjärjestelmän ominaisuudet. Tämän työn voi myös antaa äänestysjärjestelmän ohjelmiston toimittajalle ja pyytää heiltä vastaus ja todisteet, että tässä tutkimuksessa esiin tuodut tietoturvan ja laadun vaatimukset toteutuvat heidän tuotteessaan. Tämän takia työn tarkoituksena ei ole tuottaa tietoteknisiin yksityiskohtiin menevää kuvaa tietojärjestelmän tietoturvan näkökohdista, vaan selkeän yleiskuvan perusvaatimuksista. Tietoturvanäkökohtia tutkiessa keskitytään saatavilla

olevien tuotteiden tietoturvatasoon ja äänestysjärjestelmän kohdalla ohjelmiston perustaviin tietoturvavaatimuksiin. Laadunvarmistuksen kohdalla asiaa tutkitaan tietojärjestelmäprojektin tilaajan kannalta. Liitteenä (Liite 1) on Satakunnan ammattikorkeakoulun opiskelijakunnan kanssa yhdessä tehty WWW-äänestysjärjestelmä määrittelydokumentaatio, jota voi käyttää muissa opiskelijakunnissa ja yhdistyksissä pohjana äänestysjärjestelmän määrittelydokumentaatiota tehdessä.

Tutkimuksen tulos on tarkoitettu opiskelijakuntien käyttöön mutta vaaleja koskevan lainsäädännön identtisyyden puolesta se sopii yhtä hyvin kaikkien yhdistyslain piirissä toimivien yhdistysten käyttöön. Tutkimuksessa otetaan huomioon myös ylioppilaskuntia koskeva lainsäädäntö ja täten selvitystä voidaan käyttää myös ylioppilaskunnissa.

2. RAKENNE JA VAATIMUKSET

Äänestysjärjestelmän perusrakenteena käytetään prosessikuvausta ammattikorkeakoulun opiskelijakunnan äänestysjärjestelmän vaatimuksista. Nämä tarpeet on kirjattu ProAMK-tietojärjestelmäprojektin yhteydessä ammattikorkeakoulukentän opiskelijakuntien ja SAMOK ry:n yhteistyönä tammikuussa 2007 (Kuvio 1). Äänestysjärjestelmän on toteutettava ProAMKile kuviossa määrätyt tehtävät.



Kuvio 1. Opiskelijakunnan vaalien prosessikaavio.

Äänestysjärjestelmässä on oltava tiedot vaalista (avautumispäivä, sulkeutumispäivä) sekä ehdokkaista. Äänestämisen mahdollistamiseksi järjestelmässä on oltava myös tiedot äänioikeutetuista. Järjestelmän on myös pystyttävä laskemaan vaalien tulos. Tämän yleiskuvauksen lisäksi on SAMMAKKOn pääsihteeri Juha Lammisen kanssa yhdessä määritelty lista äänestysjärjestelmän tarkemmista vaatimuksista (sähköpostikeskustelu 14.3.2007). Tästä listasta on johdettavissa äänestysjärjestelmän tärkeimmät tietoturvavaatimukset:

1. Vaalit aukeutuvat ja sulkeutuvat haluttuna päivänä. Vain tänä aikana voi äänestää.
2. Äänestäjän on kirjauduttava äänestysjärjestelmään pystyäkseen äänestämään. Äänestäjän käyttäjätunnukset on oltava yksilölliset ja salaiset.
3. Jokainen äänioikeutettu äänestäjä pystyy äänestämään vaalissa vain kerran.
4. Vaalien tulostietoja ei pysty näkemään ennen niiden julkaisua. Julkaisun tekee ylläpitäjä.
5. Äänestysjärjestelmän on pystyttävä laskemaan vaalien tulos ja tuloksen on vastattava annettuja ääniä.
6. Äänioikeutetun äänestäjän äänestyspäätöstä ei saa saada selville järjestelmästä. Tietoa ei saa tallentaa järjestelmään.
7. Annetut äänet on saatava listattua manuaalista tarkastuslaskentaa varten.

8. Vain ylläpitäjällä on oikeus muokata vaalien tietoja, lisätä tai poistaa äänioikeutettuja, lisätä tai poistaa ehdokkaita, julkaista ja piilottaa vaalien tulos, listata annetut äänet ja poistaa annettuja ääniä.

WWW-pohjainen äänestysjärjestelmä, joka täyttää kuvion 1 prosessikaavion vaatimukset sekä SAMMAKKOn pääsihteerin Juha Lammisen määrittelemät tietoturvavaatimukset, on tietojärjestelmän toimintojen puolesta oikeanlainen käytettäväksi opiskelijakunnan vaaleissa. Käyttöä muussa yhdistysympäristössä tai yhteisössä käsitellään tarkemmin osiossa 3. Tarkemmin äänestysjärjestelmän vaatimuksia on käsitelty äänestysjärjestelmän määrittelydokumentaatiossa (Liite 1).

3. KÄYTÖN MAHDOLLISUUDET JA RAJOITUKSET

Äänestysjärjestelmän käytön mahdollisuudet ja rajoitukset määräytyvät opiskelijakunnan ja yhdistyksen toimintaa määrittävien lakien perusteella. Opiskelijakunnan toimintaa määrittää ammattikorkeakoululaki. Ammattikorkeakoululaissa ei määritellä opiskelijakunnan vaalien toimitustapaa sen tarkemmin. Näissä tapauksissa noudetaan lain pykälän 42 momentin 7 asetusta (9.5.2003/351 Ammattikorkeakoululaki):

> Opiskelijakunnan toimintaan sovelletaan, mitä yhdistyslaissa (503/1989) säädetään, jollei tästä laista muuta johdu.

Tämän perusteella opiskelijakunnan vaalikäytännöt määrätään yhdistyslaissa. Yhdistyslaissa määritellään pykälässä 28 vaaleista, että kokouksessa toimitettavassa vaalissa noudetaan enemmistövaalitapaa, ellei yhdistyksen säännöissä ole toisin määrätty.

Erillisissä äänestystilaisuuksissa tai postitse toimitettavassa vaalissa noudatetaan sen sijaan suhteellista vaalitapaa, jollei säännöissä ole toisin määrätty. Lisäksi yhdistyslaki määrittelee että kaikille päätösvallan käyttöön oikeutetuille on turvattava oikeus osallistua ehdokkaiden asettamiseen vaalia varten. Yhdistyslain pykälässä 29 määritellään enemmistövaalitavan ja suhteellisen vaalitavan ääntenlaskun perusteista mutta siinä määritellään myös, että suhteellinen vaali toimitetaan suljetuin lipuin. Vaalien järjestämistä yhdistyslaki ohjeistaa pykälässä 30 (26.5.1989/503 Yhdistyslaki):

> Jos yhdistyksen päätösvaltaa käytetään erillisissä äänestystilaisuuksissa tai postitse, yhdistyksen on hyväksyttävä tätä varten *äänestys- ja vaalijärjestys,* johon on otettava tarvittavat äänestystä ja vaalia koskevat tämän lain säännöksiä ja yhdistyksen sääntöjä täydentävät määräykset.

WWW-äänestämisen säännöistä, vaatimuksista ja käyttömahdollisuuksista on siis määrättävä yhdistyksen hyväksymässä äänestys- ja vaalijärjestyksessä, joka ottaa huomioon yhdistyslain pykälät 28-30 sekä yhdistyksen säännöt. Muuta lainsäädäntöä tai ohjeistuksia ei tarvitse ottaa huomioon.

Satakunnan ammattikorkeakoulun opiskelijakunnan säännöissä pykälässä 5 määritellään että edustajisto hyväksyy ohjesäännöt ja muut tarpeelliseksi katsomansa säännökset, että edustajisto valitaan suoralla vaalitavalla, että äänioikeus on opiskelijakunnan jäsenillä ja jokainen äänioikeutettu on vaalikelpoinen ja että opiskelijakunnan edustajiston vaalien toteutuksesta määritellään erillisessä vaaliohjesäännössä (Satakunnan ammattikorkeakoulun opiskelijakunta – SAMMAKKO 2005). Yhdistyslain vaatimukset on SAMMAKKOn kohdalla täytetty kun vaalien järjestämistavasta on määrätty säännöissä ja jokaiselle jäsenelle on annettu mahdollisuus asettua ehdolle (pykälä 28) ja kun vaalien toteutuksesta määrätään erillisessä edustajiston hyväksymässä vaaliohjesäännössä (pykälä 30). Opiskelijakuntaa tai yhdistystä ohjeistava lainsäädäntö siis ei aseta mitään vaatimuksia tai esteitä WWW-äänestysjärjestelmän käytölle. Mikä tahansa äänestystapa on käyttökelpoinen ja virallinen, kunhan yhdistyksen kokous (opiskelijakunnassa edustajisto) on asian hyväksynyt vaaliohjesäännössä tai vastaavassa dokumentissa.

Ylioppilaskunnilla ei ole mitään vaaleihin liittyvää lainsäädäntöä, sillä ylioppilaskunnan toimintaa määrää vain Yliopistolaki (645/1997) 40.3 § ja Ylioppilaskunta-asetus (116/1998). Näiden pohjalta ylioppilaskunnan edustajistolla on täysi valta määrätä säännöistä ja vaaliohjesäännöistä.

WWW-äänestysjärjestelmien käyttö ylioppilaskunnissa ja opiskelijakunnissa on ollut vähäistä mutta ainakin Helsingin Kauppakorkeakoulun Ylioppilaskunta on käyttänyt sähköistä WWW-äänestysjärjestelmää vuodesta 2005 lähtien edustajistovaaleissa, Teknillisen Korkeakoulun Ylioppilaskunta (TKY) jo vuodesta 2003 lähtien (Teknillisen Korkeakoulun Ylioppilaskunta, Helsingin kauppakorkeakoulun ylioppilaskunta 2005). Keskustelu sähköisen äänestysjärjestelmän käyttöönotosta törmää usein vastaväitteisiin vaalisalaisuuden ja vaalirauhan vaarantumisesta. Vaalisalaisuuden vaarantumisella tarkoitetaan äänestyspäätöksen selville saamista ja vaalirauhan vaarantumisella äänestystilanteen turvallisuutta. WWW-äänestyksen vaalisalaisuuteen vaikuttavia seikkoja käydään tarkemmin läpi osiossa 4, jossa käsitellään WWW-äänestysjärjestelmän tietoturvaa. Vaalirauhan vaarantuminen on sen sijaan periaatteellinen vaaratilanne. Äänestyskopissa ketään ei pysty painostamaan tai vaikuttamaan äänestyspäätökseen, tietokoneen äärellä (missä tietokone sitten ikinä onkaan) tilanne on täysin toinen. Äänestyksen järjestäjä ei myöskään pysty mitenkään varmistamaan äänestystilanteen vaalirauhaa. Tämä ongelma on pysyvä ongelma WWW-äänestyksessä mutta vaalirauhan rikkoutumisen vaaran vakavuus on täysin vaalin järjestäjän arvioitavissa. Yhdistyksen ja opiskelijakunnan kannalta yhdistyslaki mahdollistaa postiäänestyksen käytön (26.5.1989/503 30 §) jossa ongelma on käytännössä sama. Tästä seuraa että yhdistyksen kokous ja opiskelijakunnan edustajisto voi täysin vapaasti arvioida vaalirauhan tärkeyttä WWW-äänestyksen kannalta sillä lainsäädäntö ei luo sääntöjä tässä tapauksessa. Tilanne on vielä vapaampi ylioppilaskunnissa, jossa edes yhdistyslakia ei tarvitse ottaa huomioon.

Rajoituksena WWW-äänestyksen käytössä on yleisesti äänestysjärjestelmän ylläpito. Esimerkiksi Tampereen yliopiston ylioppilaskunnan vuoden 2005 edustajiston vaalien ennakkoäänestys suunniteltiin toteutettavaksi TKY tekemällä äänestysjärjestelmällä

mutta järjestelmää ei saatu toimimaan Tampereen yliopiston tietoteknisessä ympäristössä. TKY:n pääsihteeri Vesa Ruusunen mukaan järjestelmän tekijät ovat vapaaehtoisia eikä heillä ollut aikaa viimeistellä ohjelmaa niin että se toimisi muissakin kuin TKY käyttöympäristössä (Tamminen, T. 2005). Sama kohtalo oli Kuopion yliopiston ylioppilaskunnalla. Suomen ammattikorkeakouluopiskelijayhdistysten liiton järjestösihteeri Antti Hallia sanoi ohjelmiston ylläpidon olevan yleisin ongelma WWW-äänestyksessä opiskelijakuntakentällä. Vaikka äänestysjärjestelmän toimintaperiaate ei ole tietoteknisesti mahdottoman monimutkainen, ohjelmiston käyttö vaatii hyvää dokumentaatiota, jatkokehitystä uusien tarpeiden ilmetessä ja jatkuvaa ylläpitoa käyttöympäristössä että koodin tasolla tietoturvauhkia vastaan. Ilman asiantuntevaa ylläpitoa äänestysjärjestelmä on varmasti tietoturvaton äänestysvaihtoehto eikä sen käyttöä voi tällöin suositella. Järjestelmää käyttävän yhteisön onkin konkreettisesti varattava resursseja äänestysjärjestelmän tekniseen ylläpitoon. Tämä saattaa muodostua esteeksi pienissä yhdistyksissä ja opiskelijakunnissa.

Pelkän WWW-äänestysjärjestelmän käytön hyväksymisen lisäksi vaaliohjeistuksesta yhteisössä päättävän elimen kannattaa myös ehdottomasti laittaa vaatimuksia äänestysjärjestelmän tietoturvalle. On oltava konkreettisia mittareita, joilla äänestysjärjestelmän turvallisuutta voidaan arvioida. Esimerkiksi Teknillisen Korkeakoulun Ylioppilaskunnan vaalijärjestyksessä onkin listattu neljä selkeää kohtaa, jotka pitää toteutua äänestysjärjestelmän käyttämiseksi (Teknillisen Korkeakoulun Ylioppilaskunta 2004):

1. äänestäjän äänestyslaitteen ja keskuskoneen välillä käytetään riittävää tietoturvaa
2. äänestäjän henkilöllisyys varmistetaan ennen äänestämistä
3. äänestäjän henkilöllisyyttä ei pystytä jälkikäteen yhdistämään mihinkään tiettyyn annettuun ääneen
4. äänestäjä ei pysty äänestämään kuin yhden kerran sähköisesti tai uurnavaalilla.

Vaalisalaisuuden kannalta kohta yksi on heti ongelmallinen. Koska TKY:n vaalijärjestyksessä ei ole erikseen määrätty tietoturvan arvioinnin tekijää, termi ”riittävä tietotur-

va” voi tarkoittaa hyvin eri asioita tietotekniikka tuntevan ja sitä tuntemattoman tarkkailijan mielestä. Arvioinnissa pitäisi käyttää vähintäänkin tämän opinnäytetyön osiossa 4 listattuja WWW-järjestelmän tietoturvan näkökohtia. Lisäksi listalta puuttuu ohjelmiston laadunvarmistus. Kenen vastuulla on testata että vaalien tulos vastaa annettuja ääniä? Vaalijärjestys ei kerro tätä. Samat puutteet löytyy esimerkiksi Turun kauppakorkeakoulun ylioppilaskunnan vaalijärjestyksestä. Laadunvarmistukseen löytyy ohjeistusta kappaleesta 5.

WWW-äänestysjärjestelmää on mahdollista käyttää niin yhdistyksissä opiskelijakunnissa kuin ylioppilaskunnissakin. Lainsäädäntö ei Suomessa aseta käytölle mitään esteitä. Ohjelmiston laadusta ja tietoturvasta pitää kuitenkin muistaa varmistua, eikä sähköistä äänestysjärjestelmää pitäisi ottaa käyttöön ilman tietoturvan ja ohjelmiston laadun huolellista analyysiä. Lisäksi on syytä arvioida käytännöllisiä näkökohtia siitä, onko kaikilla äänestäjillä pääsy WWW-päätteelle ja onko järjestelmä tarpeeksi helppokäyttöinen.

4. TIETOTURVA

4.1 Mitä on tietoturva?

Aluksi pitää määritellä mitä termillä tietoturva tarkoitetaan. Peruslähtökohta on, että tietokone on tietoturvallinen jos siihen voi luottaa ja sen ohjelmistot toimivat odotetusti (Garfinkel, Spafford & Schwartz 2003, 5). Ohjelmiston odotettu toiminta on määritelty määrittelydokumentissa ja luottamus järjestelmään syntyy kun se toimii täsmälleen niin kuin määrittelyssä lukee. Miten kuitenkaan voidaan varmistua, että todellinen järjestelmän toiminta vastaa määrittely? Jos esimerkiksi määrittelydokumentaatiossa lukee lause

”Käyttäjän on kirjauduttava annetuilla tunnuksilla järjestelmään pystyäkseen käyttämään sen palveluja”, miten voidaan varmistua että käyttäjä ei todellakaan pääse käsiksi palveluihin ilman kirjautumista? Tai mistä tiedetään että annettuja käyttäjätunnuksia todella käyttää niiden haltia? Näiden tietojärjestelmän kohtien toiminnan luotettavuuden arviointiin ja varmistamiseen täytyy käydä tietojärjestelmän kaikki osat läpi ja tehdä arvio tietoturvasta jokaisen osan kohdalla.

Tietoturva on pohjimmiltaan kokoelma teknisiä ratkaisuja ongelmaan, joka ei ole teknisen (Garfinkel ym. 2003, 32). Tahon, jonka hallussa on tietoa tai resursseja joiden haltuunotto kiinnostaa muita, on puolustettava järjestelmänsä tietoturvaa, jotta tietomurtoa ei tapahtuisi. Kyse on siis ihmisten välisestä voimien mittelystä tietokoneiden ja tietoverkkojen välityksellä. Tämä asetelma tekee puolustajan aseman huomattavasti tiukemmaksi kuin hyökkääjän. Puolustajan on varmistuttava järjestelmän jokaisen osan tietoturvasta mutta hyökkääjä voi etsiä ja hyökätä järjestelmän heikoimpaan kohtaan. Järjestelmän jokaisen osan tietoturvan varmistaminen vaatii valtavasti työtä. Lisäksi puolustaja voi puolustautua vain tiedettyjä uhkia vastaa mutta hyökkääjä voi etsiä tuntemattomia haavoittuvuuksia järjestelmästä. Esimerkiksi tietoturvallisten ohjeiden mukaan konfiguroitu palvelimen käyttöjärjestelmä ei suojaa järjestelmää, jos itse käyttöjärjestelmästä löytyy uusi tietoturva-aukko. Tietoturva-aukkoja on erittäin vaikea löytää itse lähdekoodia lukemalla, eikä se edes ole mahdollista suljetun lähdekoodin ohjelmistoissa. Hyökkääjä voi myös hyökätä juuri haluamallaan ajanhetkellä mutta puolustajan on oltava valmiina jatkuvasti. Järjestelmän tilaa on seurattava jatkuvasti ja kaikkiin epäilyttäviin merkintöihin järjestelmän lokissa on reagoitava. Vaikeimpana erona puolustajan ja hyökkääjän välillä on lainsäädäntö. Puolustajan on järjestelmän tietoturvaa varmistaessa ja valvoessa noudettava lainsäädäntöä ja järjestelmän käyttäjien yksityisyyden suojaamisen sääntöjä. Hyökkääjä sen sijaan voi tehdä mitä haluaa, ilman lainsäädännön tai yhteisön moraalin paineita. Kokonaisuudessaan puolustaminen on vaikeampaa, se vie enemmän aikaa ja hyökkäyksen tapahtuessa puolustaja on aina alakynnessä. Hyökkääjän tietotason vaatimukset tippuvat jatkuvasti, koska hyökkäyksiä voi tehdä valmiilla koodinpätkillä mutta toisaalta hyökkäyksen alla olevien järjestelmien tärkeys on kasvanut vuosi vuodelta. Nykyään ja varmasti myös jatkossa hyökkäykset ovat yhä kehittyneempiä ja hyökkäyksen alla olevissa järjestelmissä säilytetään yhä tärkeämpää dataa

(kuten äänestystuloksia), joten tietoturvaan on panostettava jatkossa yhä enemmän. (Howard, M & LeBlanc, D. 2003, 19-21; Allen, J. 2002, 2)

Ainoa keino saavuttaa edes jonkin tason luottamus järjestelmän tietoturvaan on varautua hyökkäyksiin ennalta. Ilman tehokasta valmistautumista ja järjestelmän jatkuvaa seurantaa on mahdoton varmistua siitä, onko tietomurto tapahtunut vai onko se jopa yhä käynnissä, kuinka paljon vahinkoa tietomurto sai aikaan ja miten murrettu järjestelmä saadaan takaisin luotettavaksi. Ensimmäisenä askeleena on järjestelmän vahvistaminen ja turvaaminen. Tämä tarkoittaa ohjelmistojen tietoturvallista konfiguraatiota, kaikkien tietoturvapäivitysten asentamista ja tehokasta käyttäjäoikeuksien hallintaa sekä lokitoimintojen aktivointia. Toisena askeleena on valmistautuminen. Järjestelmän normaali toiminta on dokumentoitava tarkkaan jotta kaikki epäilyttävä toiminta voidaan havaita erona tähän perusmalliin. Kolmas askel perustuu kahden edellisen perustalle: tietomurron havaitseminen vaatii toimivia lokeja ja kykyä niiden tulkintaan. Pelkkä loki kun ei kerro luotettavasti tietomurrosta mutta se voi antaa vinkkiä ja oikean suunnan tietomurron havaitsemisessa. Havainnon jälkeen tietomurtoon on reagoitava ja tietoturva-aukot on korjattava. Reagointi vaatii toimiakseen selkeää vastuunjakoa ylläpidossa, järjestelmän hyvää dokumentaatiota ja oikein toimivia lokeja. Ilman mahdollisuutta tietää tietomurron tarkkaa laajuutta sitä ei myöskään voida paikata. Viimeisenä askeleena on tietoturvan parantaminen. Tapahtuneesta tietomurrosta kerätyn tiedon perusteella on tehtävä järjestelmän tietoturvaa parantavia päivityksiä ja muita parannuksia, muuten luotto järjestelmän tietoturvaan ei palaudu ja järjestelmä on käyttökelvoton. (Allen 2002, 7-12)

4.2 Tietomurron riski

Yleinen syy tietoturvan laiminlyönnissä on kuvitelma, ettei tietomurtoa voi tapahtua. Äänestysjärjestelmänkin kohdalla voidaan kuvitella, että ketä nyt olisi kiinnostunut yhdistyksen tai opiskelijakunnan vaalien häiritsemisestä siinä määrin että rikkoisi lakia tehdäkseen tietomurron. Mitä ketään sillä saavuttaisi? Jos järjestettävillä vaaleilla on vaikutusta vallan tai rahan käyttöön yhteisössä (kuten esimerkiksi opiskelijakunnan

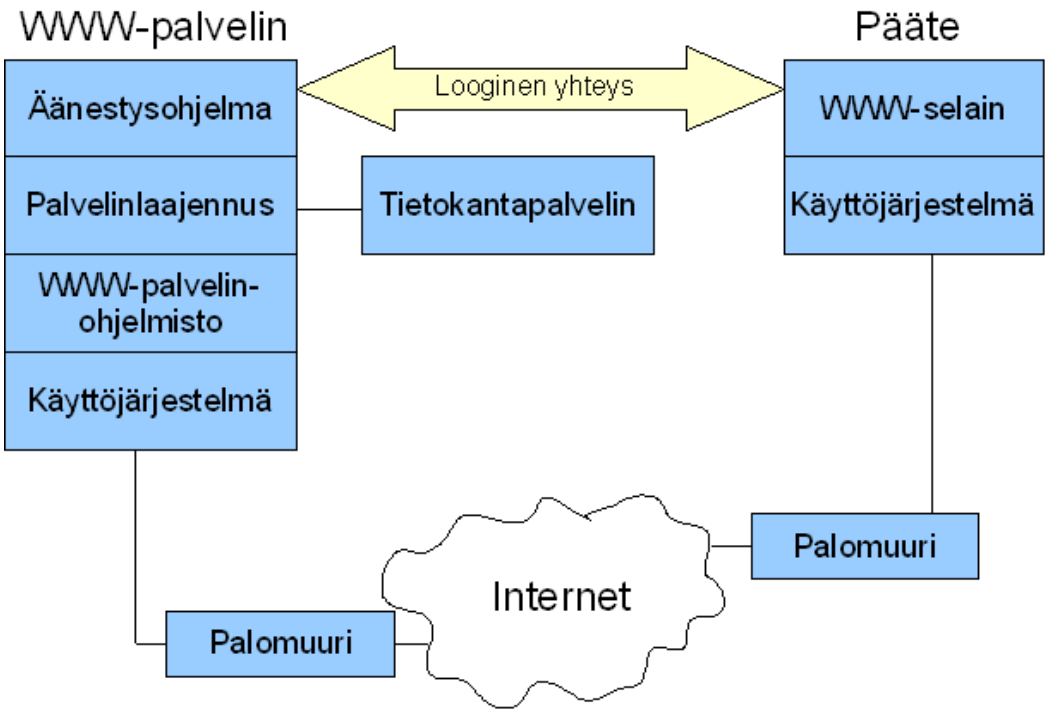
edustajiston vaaleissa), varmasti löytyy taho joka haluaisi kumpaakin lisää jos siihen on helppo mahdollisuus tietomurron kautta. Yhtä todennäköinen syy hyökkäykseen on resurssit. Palvelin ja sen tietoliikenneyhteys ovat resursseja jotka hyökkääjä voi kaapata omaan käyttöönsä. Tällöin ei ole mitään merkitystä palvelimen alkuperäisellä käyttötarkoituksella. Internettiä tietoturva-aukkojen toivossa skannaavat ohjelmistot eivät valitse kohteitaan kielen, alueen tai käyttötarkoituksen perusteella. Äänestysjärjestelmän kaappaaminen ja käyttäminen esimerkiksi palvelunestohyökkäyksen osana tai roskapostipalvelimena eivät siis välttämättä ole suunniteltuja hyökkäyksiä yhteisön demokratiaa vastaan vaan ainoastaan resurssien takia tehty kaappaus. Internetissä oleva palvelu on koko maailman nähtävillä ja sitä vastaan voidaan hyökätä mistä päin maailmaa tahansa. Oman järjestelmän tietojen tärkeyden tai tarkoituksen tyypin arviointi osana tietoturva-analyysiä ei enää näyttele niin tärkeää osaa. Tietoturvaan on panostettava vaikka Internetissä kiinni oleva palvelin ei olisi missään käytössä. Jos resurssi näkyy Internettiin, se on potentiaalinen tietomurron kohde. (Howard & LeBlanc 2003, 723-728)

Internet ei ole muuttumassa yhtään turvallisemmaksi paikaksi vaikka jokaista uutta käyttöjärjestelmän ja ohjelmiston versiota kehutaan aina edellistä tietoturvallisemmaksi. Ajanjaksolla heinäkyy 2006 – joulukuu 2006 tiedon kalastelu (phishing), roskapostit, kaapattujen koneiden verkostot, Troijalaiset ja uusien tietoturva-aukkojen hyödyntäminen ennen sen julkaisua lisääntyivät. Haittaohjelman avulla kaapattuja tietokoneita havaittiin aktiivisena Internetissä keskimäärin yli 63000 kappaletta. Ohjelmistoista raportointiin löydetyn yli 2500 tietoturva-aukkoa, joka on suurin määrä mitä koskaan ennen minkään puolen vuoden tarkastelujakson aikana. Tietoturva-aukoista 66 % koski Internet-selaimen kautta käytettäviä sovelluksia ja palveluita. 79 % aukoista oli helposti hyödynnettäviä. 136 uutta haitallista koodia sisältävää ohjelmaa (virukset, madot, Troijalaiset jne.) havaittiin tällä ajanjaksolla ja vanhoista haittaohjelmista löytyi yli 8000 uutta versiota. Palvelunestohyökkäyksiä tehdään yli 5000 päivässä. Uusia tiedon kalasteluun tarkoitettuja sähköpostiviestejä löytyi yli 166000 kappaletta ja roskapostin osuus kaikesta sähköpostiliikenteestä nousi 59 %. Vastaavia lukuja voisi luetella loputtomiin, eikä kevät 2007 varmastikaan ole tuonut parannusta näihin lukuihin. Tietoturva-aukkoja löytyy lisää jatkuvasti ja niitä hyödynnetään jatkuvasti. Kiistely tietoturvan tarpeellisuudes-

ta voidaan siis lopettaa. Jos haluaa ylläpitää palvelua Internetissä, on myös huolehdittava palvelun tietoturvasta. (Symantec 2007)

4.3 Tietoturvaan vaikuttavat asiat

Koska nyt tarkastelun alla on WWW-pohjainen äänestysjärjestelmä, kuuluu tietojärjestelmään käytännössä kaikki osat käyttäjän selaimesta lähtien aina WWW-palvelimeen asti (Kuvio 2).



Kuvio 2. Äänestysjärjestelmän tietojärjestelmärakenne.

Kuviosta 2 näkyy tietojärjestelmän looginen ja fyysinen toiminta. Loogisella tasolla käyttäjä ottaa omalta koneeltaan yhteyden äänestysohjelmistoon kirjoittamalla sen URL-osoitteen selaimeen. Tietojärjestelmän määrittelydokumentaation mukaan (Liite 1) äänestysjärjestelmän toiminta on seuraava:

1. Käyttäjä avaa sivuston selaimeensa

2. Käyttäjä kirjautuu järjestelmään annetuilla tunnuksilla
3. Käyttäjä äänestää vaalissa

Fyysisellä tasolla vastaava tapahtumasarja on huomattavasti laajempi:

1. Käyttäjä kirjoittaa selaimeen äänestysjärjestelmän URL-osoitteen
2. Selain lähettää pyynnön käyttöjärjestelmälle
3. Käyttöjärjestelmä lähettää sivupyynnön verkkoliitännän kautta
4. Käyttäjän lähiverkon ja Internet-palveluntarjoajan kautta sivupyyntö päätyy lähiverkkoon jossa WWW-palvelin on
5. Palvelimen käyttöjärjestelmä vastaanottaa pyynnön ja lähettää sen WWW-palvelinohjelmistolle
6. WWW-palvelin tunnista että kyseessä on palvelinlaajennusta käyttävä sivu ja lähettää sivupyynnön palvelinlaajennukselle
7. Palvelinlaajennus suorittaa pyydetyn sivun ohjelmakoodin, joka saattaa sisältää tietokantakutsun tietokantapalvelimelle. Jos tietokantapalvelin on eri fyysisellä palvelimella, tapahtuu tiedonhakupyyntö (SQL-komento) WWW-palvelimen käyttöjärjestelmän ja verkkoliitännän kautta
8. Valmis WWW-sivu palautuu palvelinlaajennukselta WWW-palvelinohjelmistolle, joka lähettää sen käyttöjärjestelmälle, joka toimittaa sen verkkoyhteyden kautta käyttäjälle, jonka käyttöjärjestelmä toimittaa sen selaimelle.

Tämä lista vastaa loogisen tason listan kohtaa yksi. Jokaisen sivupyynnön kohdalla sama tapahtumasarja toistuu. Tiedon välitys (käyttäjätunnus, äänestyspäätös) käyttäjältä WWW-palvelimelle tapahtuu sivupyynnön mukana.

Fyysisen tason tapahtumasarjasta voimme poimia kaikki tietojärjestelmän toiminnan osat:

1. Käyttäjän Internet-selain
2. Käyttäjän käyttöjärjestelmä
3. Käyttäjän laitteisto
4. Käyttäjän lähiverkko

5. Internet
6. WWW-palvelimen lähiverkko
7. WWW-palvelimen laitteisto
8. WWW-palvelimen käyttöjärjestelmä
9. WWW-palvelimen WWW-palvelinohjelmisto
10. WWW-palvelinohjelmiston palvelinlaajennus
11. Tietokantapalvelinohjelmisto (jos eri fyysisellä palvelimella, täytyy ottaa huomioon palvelimen verkko ja käyttöjärjestelmä)
12. Äänestysjärjestelmä

Äänestysjärjestelmän toimiminen vaatii että jokainen kahdestatoista tietojärjestelmän osasta toimii moitteetta. Tilanne jossa Internet ei välitä sivupyyntöjä WWW-palvelimelle tai tilanne jossa WWW-palvelimen käyttöjärjestelmä ei välitä sivupyyntöä WWW-palvelinohjelmistolle johtaa varmasti palvelun toimimattomuuteen. Samalla logiikalla pitää arvioida tietojärjestelmän tietoturvaa; yhden osan tietoturvan pettäminen johtaa koko tietojärjestelmän tietoturvan pettämiseen. Tämän takia jokaisen tietojärjestelmän osan tietoturvaa on tarkasteltava erikseen ja huomioon on myös otettava osien erilaisuus koska osat eroavat huomattavasti toisistaan. Esimerkiksi Internetin (fyysinen kokonaisuus, miljoonia käyttäjiä) ja äänestysjärjestelmän (ohjelmisto, rajattu määrä käyttäjiä) toimintamallia kokonaisuuden kannalta on katsottava eri näkökulmista. Lähtökohtana jokaisen kohdan tarkastelussa voidaan kuitenkin käyttää seuraavaa listaa. (Garfinkel ym. 2003, 33-34)

- Luottamuksellisuus. Kenellä on pääsy tämän osion tietoihin ja dataan?
- Tiedon eheys. Pysyykö tieto muuttumattomana ja pääseekö sitä muuttamaan vain ne tahot joille se oikeus on annettu?
- Saatavuus. Onko palvelu käytettävissä?
- Vastaavuus. Toimiiko palvelu odotetusti?
- Hallinta. Kenellä on oikeus muuttaa palvelun asetuksia?
- Valvonta. Miten järjestelmän toimintaa pystyy valvomaan?

Jokaisen tietojärjestelmän osan kohdalla on myös arvioitava lähtökohtia joista tietoturva

syntyy ja miten niitä pystytään soveltamaan tämän osan kohdalla (Garfinkel ym. 2003, 65). Seuraava lista sisältää kohtia joista tietoturva rakentuu.

- Käyttäjien todentaminen. Käyttäjien todentamisella tarkoitetaan esimerkiksi käyttäjätunnusten tai IP-numeron perusteella tapahtuvaa tunnistusta, jonka perusteella voidaan rajata tietojärjestelmän käyttäjät haluttuun ryhmään.
- Käyttäjäryhmä. Käyttäjän todentamisen jälkeen sallitut käyttäjät voidaan jakaa käyttäjäryhmiksi joilla on eri tasoisia oikeuksia palveluun. Ylläpitäjän on päästävä muokkaamaan asetuksia mutta tätä oikeutta ei tarvita jokaiselle käyttäjälle.
- Tiedostojärjestelmän turvallisuus. Kaikkien suoritettavien ohjelmistojen koodi ja tietokantojen data on tallennettu tiedostojärjestelmään. Vaikka ohjelmistojen käynnistämistä kontrolloitaisiin käyttäjäoikeuksilla käyttöjärjestelmän tasolla, on tärkeä varmistua että käynnistettävä ohjelma on odotettu. Samoin tietokannan kohdalla, tietokantapalvelimen käyttäjähallinta ei estä datan ylikirjoittamista tai muuttamista jos tietoa muutetaan suoraan tiedostojärjestelmään kirjoittamalla, eikä siitä jää jälkeä loki-tiedostoihin. (Garfinkel ym. 2003, 613)
- Salakirjoitus. Salakirjoituksella tarkoitetaan matemaattisia tekniikoita joilla tieto voidaan muutta muotoon jossa sitä on mahdotonta ymmärtää ilman oikeaa matemaattista purkuavainta (Garfinkel ym. 2003, 161). Salakirjoituksella voidaan taata että vain halutut tahot pystyvät ymmärtämään viestin sisällön.
- Fyysinen turvallisuus. Fyysisellä turvallisuudella tarkoitetaan fyysisen laitteiston turvallisuutta ja fyysisen tason uhkien vaikutusta ohjelmistojen ja datan turvallisuuteen. Fyysisen ja loogisen tason turvallisuus ovat tiiviissä yhteydessä, sillä jos joku varastaa palvelintietokoneen, hän myös erittäin todennäköisesti saa haltuunsa datan jota palvelimella on säilytetty (Garfinkel ym. 2003, 216). Fyysisen turvallisuuden kohdalla pitää ottaa huomioon myös varmuuskopioiden turvallisuus, sillä jokainen jolla on pääsy järjestelmän varmuuskopioihin, on myös pääsy kaikkeen tallennettuun dataan (Garfinkel ym. 2003, 219). Varmuuskopioiden on myös oltava kirjoitussuojattuja jotta niiltä palautettavaan järjestelmään voidaan luottaa. Suojautuminen fyysisiltä vahingoilta (tulipalo, vesivahinko, maanjäristys jne.) on myös tietoturvallisuutta koska nämä johtavat helposti datan tuhoutumiseen tai korruptoitumiseen.

- Käyttäjien turvallisuusarviointi. On tärkeää muistaa että tietomurrot ovat ihmisten tekemiä. On tärkeää määritellä kenelle annetaan oikeudet käyttää järjestelmää ja millä perusteilla käyttäjän luotettavuus pystytän todentamaan.

Tietojärjestelmän määrittelyssä (Liite 1) on määritelty tärkeiksi tietoturvallisuuden kohdiksi äänestyssalaisuus, eli äänestyspäätöstä ei saa pystyä linkittämään äänestäjään, äänestäjän tunnistaminen, jotta voidaan varmistua että äänen pystyy antamaan vain äänioikeutettu, ja ääntenlaskun luotettavuus, eli tuloksen on vastattava annettuja ääniä.

4.4 Tietoturvan arviointi

Kappaleessa 4.3 määriteltiin lista tietojärjestelmän osista, lista ominaisuuksista jotka vaikuttavat tietoturvaan ja lista tekniikoista joista tietoturva rakentuu. Näiden avulla voidaan luoda yleinen tarkastuslista jokaisen tietojärjestelmän osan kohdalle, joka ottaa huomioon tarkasteltavan osan erityisominaisuudet ja tietoturvauhat äänestysjärjestelmän tietoturvavaatimusten kannalta (Liite 1).

4.4.1 Käyttäjän Internet-selain

Äänestysjärjestelmän käyttäjä syöttää järjestelmään käyttäjätunnuksensa ja äänestyspäätöksensä Internet-selaimen kautta ja näiden tietojen on pysyttävä salassa. Koska äänestykseen käytettäviä koneita käytetään hyvin todennäköisesti myös muuhun Internetin selaamiseen, voi selaimen tietoturvariskit vaikuttaa myös koko käyttäjän tietokoneen käyttöjärjestelmän turvallisuuteen, koska tietoturva-aukkojen kautta koneelle saattaa asentua vakoiluohjelmia (spyware) joka saattaa vakoilla ja lähettää eteenpäin tietoa käyttäjän näppäimistölle syöttämästä tekstistä (käyttäjätunnukset) ja selaimen muistiin tallennetuista salasanoista sekä ottaa säännöllisiä ruutukaappauksia (äänestyssalaisuus

vaarantuu). (Hackworth 2005, 4)

Käyttäjän selain voi myös toimia virheellisesti ja vaarantaa tietoturvan välillisesti jos se esimerkiksi ei salakirjoita tietoa odotetulla tavalla. Koska tietojärjestelmän määrittelyn mukaan (Liite 1) käyttäjän ja äänestysjärjestelmän välinen liikenne salakirjoitetaan, selaimen virheellinen toiminta saattaa johtaa virheelliseen äänestyspäätöksen tulkintaan äänestysjärjestelmässä.

Käyttäjän Internet-selain voi vaarantaa koko tietojärjestelmän luotettavuuden, koska järjestelmän käyttämiseen oikeuttavat käyttäjätunnukset saattavat päätyä tahoille joille niitä ei ole tarkoitettu. Tämä käytännössä vaarantaa koko äänestystuloksen luotettavuuden jos käyttäjätunnusten avulla äänioikeudeton henkilö pääsee käyttämään jonkun muun äänestysoikeutta. Tilanne on vielä huomattavasti vaarallisempi jos äänestysjärjestelmän ylläpitäjän käyttäjätunnukset päätyvät vääriin käsiin. Tällöin tunnusten haltia pystyy lisäämään ja poistamaan äänestäjiä ja saamaan selville heidän käyttäjätunnuksensa. Tämä tietomurto on mahdollinen koska tietojärjestelmän määrittelyn perusteella (Liite 1) äänestysjärjestelmää on pystyttävä hallinnoimaan ylläpitäjän tunnuksilla selaimen välityksellä.

Selaimen turvallisuutta voidaan parantaa huolehtimalla että käytetään selainta joka on lähtökohtaisesti riittävän tietoturvallinen, josta löydetyt ja löydettävät tietoturvauhat paikataan ja selaimeen julkaistaan päivityksiä ja että nämä päivitykset asennetaan käyttäjän koneelle. Selaimen lähtökohtaisesta tietoturvan tasosta tietyllä ajanhetkellä pystyy varmistumaan vain ja ainoastaan lukemalla selaimen lähdekoodin ja näin tarkastamalla ettei siinä ole tietoturvallisuuden kannalta vaarallisia teknisiä ratkaisuja tai ohjelmointivirheitä. Koska lähdekoodin lukeminen onnistuu vain vapaan lähdekoodin selainten kohdalla ja koska tietoturvauhkien havaitseminen lähdekoodista vaatii huomattavaa ohjelmointikokemusta ja koulutusta, on käytännössä luotettava ulkopuolisiin arvioihin selainten turvallisuudesta. Kaikista suosituimmista selainperheistä (Internet Explorer 5 - 7, Mozilla Firefox 1 - 2 ja Apple Safari 1 - 2) on löytynyt aikavälillä marraskuu 2006 – maaliskuu 2007 tietoturva-aukkoja jotka mahdollistavat komentojen suorittamisen

käyttäjän koneella ja vakoiluohjelmiston asentamisen (W3C 2007; US-CERT 2007a; US-CERT 2007b; US-CERT 2006a; US-CERT 2006b). Ei ole olemassa mitään yleistä todistetta että yksikään näistä kolmesta suosituimmasta selaimesta (tai muista selaimista) olisi nyt tietoturvallinen, ei yhdenkään selaimen käyttöä voida suositella jos halutaan varmistua selaimen tietoturvasta. Selainten mainittuihin tietoturva-aukkoihin on julkaistu päivitykset mutta niiden toimivuus pitäisi tarkistaa lukemalla lähdekoodi, sillä päivitykset saattavat tuoda mukanaan uusia tietoturva-aukkoja tai ne epäonnistuvat korjaamaan olemassa olevaa aukkoa. Tästä ei ole tietoa koska yhdenkään selaimen mainitun tietoturvapäivityksen testaustuloksia ei olla julkaistu.

Koska selaimien turvallisuutta ei pysty takaamaan, ainoa mahdollisuus on muistuttaa käyttäjää selaimen aktiivisesta päivittämisestä ja selaimen tietoturvaominaisuuksien opettelemisesta ja oikeiden tietoturva-asetusten säätämisestä (Dormann & Rafail 2007). Yhtäkään selainta ei voi suositella ylitse muiden koska Internet Explorerin versioissa 6 ja 7, Mozilla Firefoxin versiossa 2 ja Apple Safarin versiossa 2 on tällä hetkellä (19.3.2007) paikkaamattomia tieturva-aukkoja (Secunia 2007a; Secunia 2007b; Secunia 2007c; Secunia 2007d).

Toinen vaihtoehto olisi vaatia äänestäjältä, ettei äänestykseen käytettävällä koneella saa avata mitään epäilyttävää Internet-sivua koneen käyttöön ottamisen ja äänestystapahtuman välisenä aikana, jotta mitään vakoiluohjelmistoja ei pääse asentumaan. Koska epäilyttävistä sivuista ei ole luotettavaa listaa, pitäisi käyttäjältä kieltää kaikilla muilla Internet-sivuilla käyminen. Arvioinnin kannalta äänestysjärjestelmä on ainoa luotettava Internet-sivu maailmassa koska tietojärjestelmän määrittelyssä (Liite 1) ei ole määritelty käytettäväksi toimintoja jotka käyttäisivät selaimen tietoturva-aukkoja vakoiluohjelmiston asentamiseen. Tiedossa ei ilman erillistä selvitystä ole yhdenkään muun Internet-sivun koodin turvallisuus. JavaScriptin turvallisuus voidaan arvioida lukemalla lähdekoodi mutta palvelinlaajennuksia (PHP, CGI jne.) käyttävien sivujen lähdekoodi ja niihin mahdollisesti sisällytetty selainkohtainen muunneltavuus ei ole saatavissa suoraan. Internetin käytön rajoittamisen vaatimiseen ei ole lakiteknistä lupaa koska kyseessä on yksityishenkilöt, eikä tällaista käskyä pystyttäisi kuitenkaan valvomaan. Ainoa mahdolli-

suus varmistua käyttäjän selaimen tietoturvasta on siis aiemmin mainittu käyttäjän ohjeistus.

Käyttäjän Internet-selaimen vuotava tietoturva vaarantaa äänestysjärjestelmän luotettavuuden, koska joku on saattanut kaapata käyttäjätunnukset, vaalien vaalisalaisuuden, koska joku saattaa tarkkailla ruutukaappauksilla koneen toimintaa, ja vaalien tulosten luotettavuuden, jos joku on onnistunut kaappaamaan ylläpitäjän tunnukset.

4.4.2 Käyttäjän käyttöjärjestelmä

Käyttäjän käyttöjärjestelmä välittää tietoliikenteen Internet-selaimen ja fyysisen verkon välillä, joten se näkee ja kontrolloi kaikkea äänestämiseen liittyvää tietoliikennettä (käyttäjätunnukset ja äänestyspäätös). Käyttöjärjestelmä myös välittää kaiken käyttäjän syöttämän tekstin ohjelmille (kuten Internet-selain), joten vaikka välitettävä tietoliikenne selaimen ja äänestysjärjestelmän välillä olisi salattua, käyttöjärjestelmä näkee aina salaamattomat käyttäjätunnukset kun ne kirjoitetaan näppäimistölle. Tätä faktaa ei pysty muuttamaan. Vakoiluohjelmat pystyvät siis tallentamaan kaikki näppäinpainallukset. Siksi on elintärkeää pitää vakoiluohjelmat poissa koneelta. (Hackworth 2005, 4)

Toinen vaarallinen ja vaikeasti huomattava tietoturvauhka on käyttöjärjestelmän reititystaulujen (host-tiedosto) muuttaminen. Tämän avulla käyttäjän selaimen sivuhakupyyntö voidaan ohjata äänestysjärjestelmää matkivalle sivustolle, joka kerääkin käyttäjän syöttämät käyttäjätunnukset. Tää kutsutaan phishing-hyökkäykseksi. Käyttäjä ei pysty näkemään eroa aidon ja väärennetyn sivuston välillä.(Milletary 2005)

Käyttöjärjestelmän tietoturvallisuutta pystyy parantamaan kytkemällä koneen palomuuritoimintoihin kykenevän reitittimen taakse. Jos tämä ei ole mahdollista, on syytä käyt-

tää ohjelmistopohjaista palomuuria. Toinen keino parantaa turvallisuutta on asentaa virustorjuntaohjelmisto. Kolmas keino on huolehtia että kaikki verkkoyhteyttä käyttävät ohjelmat mukaan lukien käyttöjärjestelmä, ohjelmistopalomuuri ja virustentorjuntaohjelmisto joko lataavat ja asentavat päivitykset automaattisesti tai vähintään ilmoittavat uusien päivitysten olevan saatavilla. Näillä toimilla järjestelmän saa suhteellisen turvalliseksi (Woody, C & Clinton, L. 2004; US-CERT. 2003)

Kuten selainten kohdalla, myös käyttöjärjestelmän turvallisuuden arvioiminen on vaikeaa. Lopullisen totuuden löytäminen vaatisi taas lähdekoodin lukemista mikä käyttöjärjestelmien kohdalla on vielä mahdottomampi urakka. Internetin selailuun käytettävistä käyttöjärjestelmistä Windows-tuoteperhe, Linux ja Apple Macintosh OS X ovat suosituimmat (W3C 2007). Windows XP, Apple Macintosh OS X ja Ubuntu Linux 6.10 ovat kaikki altistuneet tietoturvahyökkäyksille vuoden 2007 ensimmäisen kolmen kuukauden aikana niistä löydettyjen tietoturva-aukkojen takia (Secunia 2007e; Secunia 2007f; Secunia 2007g). Ainoa asia mistä tunnutaan enää kiistelevän ikuisissa Windows vs. Linux tietoturvataisteluissa on tietoturva-aukkojen määrä. Yksikin on kuitenkin liikaa.

Käyttäjää voi pelkästään ohjeistaa huolehtimaan käyttöjärjestelmän turvallisuudesta ja päivityksistä. Tästä ei voi mitenkään varmistua eikä voi käyttäjältä vaatia mitään toimia koska äänestystapahtuma saattaa tapahtua yleiseltä Internet-koneelta jonka käyttöjärjestelmän turvallisuudesta käyttäjä ei ehkä saa mitään tietoa eikä ainakaan pysty siihen mitenkään vaikuttamaan.

Käyttäjän käyttöjärjestelmän vuotava tietoturva vaarantaa äänestysjärjestelmän luotettavuuden, koska joku on saattanut kaapata käyttäjätunnukset ja vaalien vaalisalaisuuden, koska joku saattaa tarkkailla ruutukaappauksilla koneen toimintaa.

4.4.3 Käyttäjän laitteisto

Käyttäjän laitteiston rikkoutuminen, varastaminen tai varmuuskopioiden varastaminen ei johda tietoturvaongelmiin äänestysjärjestelmän kannalta, ellei käyttäjä ole kytkenyt selaimesta päälle toimintoa joka tallentaa syötetyt salasanat selaimen muistiin. Nämä tiedot voidaan poimia varastetun koneen kovalevyltä tai varmuuskopiosta. Tämä vaarantaa äänestysjärjestelmän luotettavuuden, koska käyttäjätunnusten todellisesta käyttäjästä ei voi mennä varmuuteen, ja tietenkin palvelun saatavuuden jos äänestäjällä ei ole toimivaa konetta jolla äänestää.

4.4.4 Käyttäjän lähiverkko

Kaikki tietoliikenne äänestysjärjestelmän ja käyttäjän koneen välillä kulkee käyttäjän lähiverkon kautta. Tätä liikennettä on helppo vakoilla asiaan soveltuvien ohjelmistojen avulla jos lähiverkkoon on pääsy ulkopuolisilla henkilöillä. Vakoilua vastaan pystytään suojautumaan salakirjoittamalla liikenne äänestysjärjestelmän ja käyttäjän selaimen välillä. Tällöin äänestysjärjestelmän luotettavuutta tai äänestyksen vaalisalaisuutta ei pysty uhkaamaan tietoliikennettä salakuuntelemalla. Salakirjoitus ei kuitenkaan auta jos käyttäjän sivunhakupyynnön DNS-kysely (Domain Name System) kaapataan ja käyttäjä ohjataan phishing-sivustolle, joka on aidon äänestysjärjestelmän kopio. DNS-kyselyn kaappaaminen onnistuu koska kyselyt tehdään yhteydettömällä UDP-protokollalla jonka pakettien alkuperää on täten vaikea tarkistaa. Tämän phishing-sivuston kautta käyttäjä voidaan huijata antamaan käyttäjätunnukset, jolloin äänestysjärjestelmän luotettavuus vaarantuu. DNS-ohjauksen ja salakuuntelun lisäksi samasta lähiverkosta on helpompi tehdä tietomurtoyrityksiä käyttäjän koneelle koska verkon ulkolaidalla (esim. ADSL-modeemissa) oleva palomuuri ei tällöin estä liikennettä. Jos käyttäjän koneessa ei käytetä ohjelmistopalomuuria, on koneen kaikki portit näkyvissä ulospäin. (US-CERT 1997; Milletary 2005; Allen, Julia H 2002, 84)

Sisäverkon liikenteen tietoturvaa voidaan parantaa estämällä vierailta tahoilta pääsy lähiverkkoon. Kaapeloidussa verkossa tämä on itsestäänselvyys mutta WLAN-verkossa ketä tahansa antennin kantomatkan sisällä oleva pystyy seuraamaan lähiverkon liikennettä (ns. ”piggybacking”), ellei WLAN-verkkoa ei ole suojattua oikein. WLAN-verkon tietoturvaa voi parantaa piilottamalla verkon, muuttamalla verkon SSIS-tunnuksen vaikeammin arvattavaksi, salakirjoittamalla liikenteen, vaihtamalla WLAN-reitittimen ylläpitäjän salasanan ja varmistamalla että WLAN-reitittimen ohjelmistosta on käytössä uusin versio. (US-CERT 2006c)

4.4.5 Internet

Internetillä tarkoitetaan tässä tiedonsiirtoa käyttäjän lähiverkon ja äänestysjärjestelmän WWW-palvelimen lähiverkon välillä. Internet alkaa siis käytännössä puhelinpistokkeesta ADSL-yhteyttä käytettäessä. Koska liikenne on Internetin palveluntarjoajien välistä liikennettä, on normaalin käyttäjän mahdotonta yrittää vakoilla liikennettä tai yrittää Man-in-the-middle -tyyppisiä huijausyrityksiä, jossa joku kaappaa palvelimen ja käyttäjän välisen liikenteen. Tietenkin palveluntarjoajalla on mahdollisuus valvoa ja uudelleen ohjata liikennettä mielensä mukaan, tai tehdä sitä toimintamaan turvallisuuspalvelun käskystä. Täytyy vain toivoa että kiinnijäämisen pelko ja sitä seuraava mediakohu on tarpeeksi suuri syy palveluntarjoajan työntekijöille jättää tutkimatta äänestysjärjestelmän URL-osoitteeseen menevää liikennettä (riippuu tietenkin palveluntarjoajan kotimaasta ja maan lainsäädännöstä). Käytännössä ainoa paikka päästä käsiksi liikenteeseen on puhelinpistokkeen ja paikallisen puhelinkeskuksen välinen matka. Tällä välillä tieto kulkee kuparisessa johdossa jota on helppo salakuunnella johtoa katkaisematta (ns. ”wiretapping”), jos vain tietää mitä johtoa kuunnella ja mistä ne löytää. Kerrostalojen pohjakerrosten selkeästi viitoitetut ”Puhelinkeskus”-kyltit ovissa on hyvä paikka aloittaa. Alueellisten puhelinkeskusten jälkeen tieto kulkee operaattorin verkkoon siitä maailmalle useimmiten valokaapelia pitkin jota ei voi salakuunnella katkaisematta kaapelia ja

laittamatta fyysistä lukijaa väliin. Datamäärät ovat myös niin huomattavia että yksittäisen liikenteen poimiminen sen seasta vaatii erittäin kehittynyttä laitteistoa. Liikenteen salakuuntelu Internetin osalta on erittäin epätodennäköistä ja pienin kaikista tietoturvauhista. (Garfinkel & Spafford 2002, 381-284)

Realistinen uhka Internetin kannalta on yhteyden katkeaminen ja sen kautta tapahtuma palvelun saavuttamattomuus. Tämä saattaa tapahtua paikallisesti, esimerkiksi WWW-palvelimen Internet-yhteydestä huolehtivan palveluntarjoajan teknisin ongelmina, tai koko Internetin toimintaa koskevana toimimattomuutena. Esimerkkinä koko Internetin nimipalveluiden toimimattomuuden mahdollisuudesta antoi viimeksi helmikuussa 2007 tapahtunut palvelunestohyökkäys juurinimipalvelimia vastaan (RIPE NCC 2007).

4.4.6 WWW-palvelimen lähiverkko

Lähiverkon tietoturvallisuutta käsiteltiin jo käyttäjän lähiverkon tietoturva-analyysin kohdalla mutta WWW-palvelimen lähiverkon kohdalla on otettava huomioon huomattavasti enemmän tietoturvaan vaikuttavia kohtia. Koska WWW-palvelin on kiinteällä IP-osoitteella toimiva julkinen palvelu, se houkuttelee huomattavasti enemmän huomiota ja täten kohdennettuja murtautumisyrityksiä kuin väliaikaisella IP-osoitteella toimiva geneerinen kotikone. Lisäksi kotikoneen käytössä on usein huomattavasti laajemmat käyttövaatimukset kuin pelkässä WWW-palvelimessa, kuten BitTorrent ja muut P2P-ohjelmat, verkkopelit, sähköpostiohjelmat ja eri mediansiirtoprotokollat. Osa näistä vaatii suoran yhteyden kotikoneelle ulkopuolisesta verkosta. WWW-palvelimen toimimiselle vaatimuksena on vain portin 80 avoimuus ulkomaailmaan, koska sen kautta tulevat kaikki HTTP-protokollan WWW-sivupyynnöt ja sivuvastaukset. Jos palvelimella käytetään SSL-salausta HTTP-protokollan kanssa, on myös portti 443 avattava liikenteelle. Kaikki loput portit voikin sitten sulkea palomuurin avulla. Tämä rajoittaa huomattavasti hyökkääjän mahdollisuuksia etsiä pääsyä palvelimelle, koska kaiken liikenteen WWW-palvelimelta Internettiin ja takaisin on tapahduttava noiden kahden portin kautta. (Gar-

finkel & Spafford 2002, 433)

Verkkoympäristö jossa WWW-palvelimet toimivat ovat yleensä laajempia kokonaisuuksia kuin 1-2 koneen kotiverkot. Yrityksen verkossa saattaa olla monia eri palvelimia ja kymmeniä pöytäkoneita. Jos nämä kaikki ovat samassa lähiverkossa, on koko verkon tietoturva silloin yhtä vahva kuin sen heikoin kohta. Tällöin esimerkiksi pöytäkoneen käyttäjän huolimaton ja tietoturvaton Internet-selailu ja sen myötä koneelle päässyt vakoiluohjelmisto vaarantaa myös kaikkien palvelimien tietoturvan tarjoamalla aukon sisäverkkoon työaseman kautta. Vakoiluohjelma voi mm. tehdä skannauksen ja tietoturvahyökkäyksen WWW-palvelimen portteihin jotka ovat suljettu ulkopuoliselta liikenteeltä palomuurin avulla tai salakuunnella sisäverkon liikennettä. Koska sisäverkon liikenne on yleisesti salaamatonta, saa vakoiluohjelma helposti selville käyttäjätunnuksia, joita käyttäjät ovat käyttäneet. Pahinta tilanteessa on että salakuuntelua voi olla mahdoton havaita, koska ohjelma ainoastaan äänittä mutta ei lähetä liikennettä. Mihinkään lokiin ei siis jää mitään merkintää. Tällöin tilanteeseen ei auta tiukatkaan palomuuriasetukset koska hyökkäys tulee sisältäpäin. Yhtä hyvin WWW-palvelimesta löytyvä uusi tietoturva-aukko ja sen kautta tapahtuva palvelimen luvaton haltuunotto voi vaarantaa kaikkien pöytäkoneiden tietoturvan. Tämän takia WWW-palvelin on eristettävä muusta sisäverkosta omaksi kokonaisuudekseen. Tämä auttaa myös lokien seuraamista, koska WWW-palvelimen liikenne ja mahdolliset murtautumisyritykset saadaan erotettua muun sisäverkon liikenteestä. Lisäksi WWW-palvelimen tai muun sisäverkon käytön tietoliikenneruuhkat eivät häiritse toisiaan. (Allen 2002, 83; Garfinkel ym. 2003, 216)

Erityistä huomiota tietoturvaan on kiinnitettävä WLAN-verkkojen kohdalla jos palvelin on samassa verkossa. Verkon SSIS nimi on muutettava ja siitä on tehtävä piilotettu sekä verkon liikenne on salattava. Näiden lisääntyneiden tietoturvauhkien takia ei ole suositeltavaa pitää WWW-palvelinta samassa lähiverkossa WLAN-tukiaseman kanssa. Turhaan lisätä uhkia jos tietoturvallisempi ratkaisu on saatavilla (eli kaapeleiden vetäminen). (US-CERT 2006c)

Vaikka kaikki toimisi WWW-palvelimella ja palomuurin kohdalla odotetusti ja kaikki asetukset olisivat tietoturvallisesti, saattaa verkon toiminta silti vaarantua palvelunestohyökkäysten takia. Vaikka ennalta olisi laskettu että verkon suorituskyky (niin sisäverkon laitteiden kuten palomuurin ja reitittimen että ostetun Internet-yhteyden tiedonsiirtonopeus) riittää koko äänestäjäkunnan samanaikaiseen äänestystapahtumaan, moninkertainen sivunlatauspyyntöjen määrä palvelunestohyökkäyksen myötä tekee palvelun saavuttamattomaksi. Hyökkäyksen vaikutuksia saa jonkin verran pienennettyä esimerkiksi estämällä palomuuria vastaamasta ping-komentoihin ja ostamalla alun perinkin tarpeeksi tehokkaan reitittimen ja palomuurin sekä tarpeeksi tiedonsiirtokapasiteettia. (US-CERT 2001)

4.4.7 WWW-palvelimen laitteisto

Laitteiston turvallisuuteen liittyy itse palvelinlaitteiston ja sen ympäristön turvallisuus, sekä palvelimen varmuuskopioiden fyysisten tallennusmedioiden turvallisuus. Itse palvelinlaitteiston tietoturvallisuus on fyysistä turvallisuutta, vastaten lähinnä kysymykseen ”onko palvelin toimintakykyinen suorittamaan sille määrättyjä tehtäviä (käyttöjärjestelmän ajaminen jne.)?” Tietenkin ohjelmistopuolen tietoturvallisuus vaikuttaa osittain myös palvelimen fyysiseen tietoturvaan. Suorin esimerkki tästä on 90-luvun lopun CIH/Chernobyl -virus joka ylikirjoitti osan laitteiston BIOS-muistista tehden laitteistosta toimintakyvyttömän ja sen ajamista palveluista saavuttamattomia (US-CERT 1999).

Fyysisistä palvelimen vaaratekijöistä sisäisiä on palvelimen laitteiston rikkoutuminen ja ulkoisia vaaratekijöitä varkaus, sähkökatkot, tulipalo, vesivahinko, sähköpiikit, lämpötila ja jopa maanjäristykset. Jokainen näistä saattaa johtaa palvelun saatavuuden estymisen lisäksi myös datan tuhoutumiseen. Palvelimen laitteisto rikkoutuminen saattaa tapahtua täysin itsellään ilman ulkoista vaikutusta laitteiston valmistusvirheiden tai käyttöiän loppumisen seurauksena. Vaikka tilattuna olisi ”on-site” huolto ja takuu, on palvelu laiterikon tapahtuessa toimintakyvytön joka tapauksessa tunteja. Tämän pystyy estä-

mään laitteiston osien kahdennuksella ja asettamalla ne ”hot plug” tilaan, jolloin korvaavan laiteosan käyttöönotto tapahtuu automaattisesti ja palvelimen palvelujen häiriintymättä. Laiterikkojen ei voi ennustaa niiden satunnaisuuden takia. Esimerkiksi tutkimus kovalevyjen kestävyydestä paljasti ettei laitteen käyttöaste tai toimintalämpötila vaikuta odotetulta määrältä laiterikon todennäköisyyteen ja käyttöikään, sillä uusi, vähällä käytöllä oleva ja oikeassa lämpötilassa toimiva kovalevy saattaa hajota nopeammin kuin raskaassa käytössä oleva vanha kovalevy, jonka käyttöympäristön lämpötila on korkea (Pinheiro, E, Weber, W & Barroso, L. 2007).

Ulkoisista vaaroista ”normaalein” on varmasti sähkökatko. Pahimmassa tapauksessa palvelimen hallitsematon sammuminen saattaa johtaa datan korruptoitumiseen jos virta katkeaa kesken levyllä kirjoittamisen. Tilanteeseen voidaan varautua UPS-laitteiden (Uninterruptible Power Supply) avulla joiden akkujen varassa palvelu selviää lyhyiden sähkökatkosten yli ja akkujen loppuessa sammuttaa palvelimen normaaliin tapaan. Vaikka UPS ei takaa palveluiden saatavuutta pitkissä virtakatkoissa, se estää datan korruptoitumisen sekä suojaa järjestelmää sähköpiikeiltä. (Ogletree, Terry 2001, 583)

Palvelinta uhkaavat fyysiset ympäristövaarat (mm. tulipalo, vesivahinko, lämpötila ja maanjäristykset) ovat suurilta osin kontrolloitavissa oikeanlaisella palvelinhuoneella, jossa on palovaroitin sekä tehokas ja tasainen ilmastointi. Klassinen tapa sijoittaa palvelimet ensimmäiseen vapaaseen vaatekomeroon lattialle ilman palovaroittimia ja kunnon ilmastointia on äärimmäisen vaarallista, koska vaikka vakuutus korvaisi laitteiston tuhoutumisen ja data löytyisi varmuuskopioilta, vie järjestelmän uudelleen pystyttäminen ja konfiguroiminen paljon aikaa. Aikaa jonka kuluessa palvelu ei ole käytettävissä. Lisäksi pölyn kerääntyminen ja lämpötilan nouseminen saattavat pahimmassa tapauksessa johtaa tulipalon syttymiseen ja huomattaviin aineellisiin vahinkoihin. (Garfinkel & Spafford 2002, 367-375)

Varkauksien ja sabotaasin vaikutukset laitteistolle ovat hyvin samantapaisia kuin ympäristön aiheuttamissa vahingoissa. Palanut palvelinlaitteisto tai koko palvelinlaitteiston puuttuminen töihin tullessa aiheuttaa joka tapauksessa suurta tuhoa. Varkauksien koh-

dalla suurena lisäongelmana on myös datan joutuminen vääriin käsiin, sillä vaikka laitteisto olisi varastettu myyntitarkoituksessa, tietokannassa olevat liikesalaisuudet tai henkilötiedot herättävät varmasti kiinnostuksen. Tällöin palvelun toimimattomuuden lisäksi vaakalaudalla saattaa olla koko organisaation luotettavuus ja maine, ehkä jopa tulevaisuus. Yksinkertaisin ja helpoin tapa estää varkaudet on hankkia ikkunaton palvelinhuone jonka oven saa lukittua. Tämä yksinkertainen tapa estää kaikki ”vahingossa” tapahtuneet palvelinhuoneeseen eksymiset. Lisää turvallisuutta saa koko rakennuksen kulunvalvonnalla, valvontakameroilla ja hälytysjärjestelmillä. Fakta kuitenkin on että jos joku todella haluaa ryöstää palvelimen, kaikki fyysiset turvatoimet ovat vain hidaste, eivät este. Tällöin pitää varmistaa että data on salakirjoitettu tehokkaasti ja näin täysin hyödytöntä varastajalle. (Ogletree, Terry 2001, 583; Garfinkel ym. 2003, 216; Garfinkel & Spafford 2002, 380-381)

Tässä luvussa mainittujen skenaarioiden pohjalta on itsestään selvää vaatia että tietojärjestelmästä otetaan varmuuskopioita säännöllisesti, eikä mukaan ole edes vielä laskettu ohjelmallisten virheiden aiheuttamaa uhkaa. Laitteiston rikkoutuminen tai palvelinhuonetta uhkaavat ympäristötekijät ovat aina vaarana, vaikka uhkiin olisi varauduttukin. Laiterikot eivät tapahdu aina samalla aikavälillä eikä tulipalon vaaraa koko rakennuskompleksissa voi arvioida reaaliaikaisesti. Vaikka varkauksien voisi luulla tapahtuvan enemmänkin tunnetuille palveluille ja arvokkaalle laitteistolle, tarttuu nurkassa lojuva ”hylätty” palvelin helposti ohikulkijan matkaan. Nämä seikat tarkoittavat, että joka aamu on oltava varautunut tilanteeseen että laitteisto on tuhoutunut tai varastettu ja kaikki data sen mukana. Varmuuskopioita pitää siis ottaa päivittäin. Erittäin tärkeää on myös huolehtia varmuuskopioiden turvallisuudesta. Monimutkaisen tietojärjestelmään murtautumisen sijaan on huomattavasti helpompaa varastaa kaikki data järjestelmästä varastamalla palvelinhuoneessa lojuvat, suojauskirjoittamattomat varmuuskopioit. Ympäristötekijät aiheuttavat myös uhan varmuuskopiolle, sillä esimerkiksi magneettiset nauhat ovat yhtä herkkiä tulelle ja vedelle kuin itse laitteisto. Varmuuskopioita pitää siis säilyttää lukkojen takana ja paikassa, joka ei ole palvelinhuone eikä edes sama rakennus. Lukkojen lisäksi varmuuskopioiden tietoturvallisuutta voi kasvattaa salakirjoittamalla niille kirjoitettu data. Varmuuskopioit pitää myös olla kirjoitussuojattuja. Se on ainoa keino varmistua että palautettava data on oikeasti sama kuin sinne kirjoitettu. Varmuus-

kopioita muokkaamalla on helppoa aiheuttaa tietojärjestelmälle jatkuva tietoturvauhka, koska murtautumisen jälkeen tapahtuva järjestelmän palautus varmuuskopioilta sisältää valmiiksi asennetut tietoturvauhat. Viimeinen tarkastettava asia varmuuskopioiden kohdalla on varmuuskopioiden toimivuus. Tallentuuko tieto varmasti varmuuskopioille ja onko se palautettavissa? Koska varmuuskopiointi on käytännössä pakko automatisoida säännöllisyyden takaamiseksi, on järjestelmän palautusta harjoiteltava jotta voidaan varmistua palautuksen onnistumisesta ja esimerkiksi siitä että palautettava datan olevan uusinta saatavilla olevaa. (Garfinkel ym. 2003, 219; Garfinkel & Spafford 2002, 284-297)

Usein unohtuva asia fyysisessä tietoturvallisuudessa on datan oikeaoppinen hävittäminen. Tähän ei ehkä osata asennoitua oikein koska niin paljon työtä ja vaivaa nähdään datan säilyttämisen eteen. Pöytäkoneiden kiintolevyille, cd-rom -levyille, muistitikuille, varmuuskopioille, paperitulosteille ja verkkotulostinten muistipuskureihin jää kaikkiin talteen dataa johon on rajoitettu käyttöoikeus. Laitteita hävitettäessä on varmistuttava että tiedot tuhotaan ja ettei niitä pystytä palauttamaan. Tämän varmistamiseen pitää hankkia asiaan soveltuvia ohjelmistoja ja jopa fyysisiä työkaluja, sillä esimerkiksi kovalevyiltä pystyy palauttamaan tietoa vaikka se olisi poistettu tai jopa ylikirjoitettu. Varmin tapa varmistaa datan tuhoutuminen on tuhota muistimediat fyysisesti. (Ogletree, Terry 2001, 584)

4.4.8 WWW-palvelimen käyttöjärjestelmä

WWW-palvelimen käyttöjärjestelmä on se pohja jolle koko palvelimen ohjelmistollinen tietoturva perustuu. Turvallinen ja oikein konfiguroitu WWW-palvelin ohjelmisto ei ole turvallinen jos käyttöjärjestelmä jolla sitä ajetaan sisältää tietoturva-aukkoja. Kriittisen tietoturva-aukon kautta on mahdollista ajaa haluamiaan komentoja käyttöjärjestelmässä, kuten asentaa vakoiluohjelmia, lisätä ja poista käyttäjiä, tuhota ja muokata dataa sekä muuttaa ohjelmien asetuksia. On siis elintärkeää ettei WWW-palvelimen käyttöjärjestelmässä ole kriittisiä tietoturva-aukkoja.

WWW-palvelimilla käytettäviä käyttöjärjestelmiä on valtava määrä, suurin osa erilaisia Linux-jakeluita ja Windows-tuoteperheen palvelinversioita. Yksikään käyttöjärjestelmä ei edes yritä uskotella olevansa ilman tietoturva-aukkoja, nyt kiistelyn alla on enää kriittisten tietoturva-aukkojen määrä ja korjauspäivitysten julkaisunopeus. Pelkästään joulukuussa 2006 sekä Windows Server 2003 että Red hat Enterprise Linux versioista 3 ja 4 löytyi kriittisiä tietoturva-aukkoja ja kaikilla järjestelmillä nämä aukot olivat paikkaamatta yli viikon (Microsoft 2007). Tämän viikon aikana ainoa mahdollisuus varmistua käyttöjärjestelmän turvallisuudessa on sammuttaa palvelin. Koska täysin turvallista käyttöjärjestelmää ei löydy, ainoaksi mahdollisuudeksi jää yrittää minimoida tietoturvariskit.

Käyttöjärjestelmän tietoturvaa voi parantaa poistamalla palvelimelta palvelut joita ei käytetä. Jos esimerkiksi tietojärjestelmässä käytetään laitteistopohjaista palomuuria, ei WWW-palvelimella kannata pitää päällä ohjelmallista palomuuria, jos sitä ei ole konfiguroitu käyttöön. Jos palvelu on poissa päältä ja siitä löytyy tietoturva-aukko, ei käyttöjärjestelmän tietoturva vaarannu koska hyökkäystä ei voi tehdä. Lista tarjottavista ja oletuksena asennettavista palveluista on käyttöjärjestelmäkohtainen mutta yleisesti kannattaa tarkistaa ettei asennettuna ole tarpeettomia protokollia, sähköpostipalveluita, FTP-palvelua tai telnet-sovellusta. On tärkeää tietää mitä palveluita palvelimella ajetaan ja seurata jokaisen palvelun toimintaa, lokeja ja mahdollisesti niistä löytyvien tietoturva-aukkojen korjausten ilmestymistä sekä asentaa päivitykset välittömästi. Yleisenä ohjeena on asentaa käyttöjärjestelmä minimikokoonpanolla joka vain täyttää palvelutarpeet. (Allen 2002, 89-91; Garfinkel & Spafford 2002, 410-413)

Kun itse käyttöjärjestelmän tietoturva on saatettu tarpeeksi luotettavalle tasolle, on mahdollista määritellä säännöt palveluiden ajamiselle palvelimella. Tärkein asia on turvata, ettei käyttöjärjestelmää pääse käyttämään kuin halutut henkilöt ja halutuilla oikeuksilla. Pääkäyttäjän tunnuksilla (”root” Linuxissa ja”administrator” Windowsissa) on mahdollista muokata kaikkia käyttöjärjestelmän ja sen palveluiden asetuksia sekä kaikkia tiedostojärjestelmän tiedostoja. Yhdellekään palvelulle tai käyttäjälle (muulle kuin ylläpitäjälle) ei saa antaa vastaavia oikeuksia. Esimerkiksi WWW-palvelinohjelmisto ei tar-

vitse ylläpitäjän oikeuksia käyttöjärjestelmään, koska sen ei tarvitse päästä kuin sen toiminnalle tärkeisiin tiedostoihin käsiksi (esimerkiksi hakemisto, jossa html-tiedostot ovat). Tällöin käyttöjärjestelmän tietoturva on taattu vaikka WWW-palvelinohjelmistosta löytyisi tietoturva-aukko. Käyttöjärjestelmän tietoturvan kannalta on tärkeää määritellä ja antaa jokaiselle ajettavalle palvelulle vain minimimäärä oikeuksia tiedostojärjestelmään ja muihin laitteistoresursseihin. Tällöin voidaan varmistua että palvelun dataan pääsee käsiksi vain tämän palvelun kautta (tai ylläpitäjän tunnuksilla). (Allen 2002, 556-559 ja 89-91; Garfinkel & Spafford 2002, 410-413)

Toinen tärkeä osa käyttöjärjestelmän tietoturvaa on lokit. Lokit ovat raportteja joihin automaattisesti (jos näin on asetettu tapahtuvan) kertyy haluttua tietoa käyttöjärjestelmän ja sen palveluiden toiminnasta. Joillakin palveluilla voi olla oma lokijärjestelmä (esimerkiksi WWW-palvelinohjelmisto), osa käyttää käyttöjärjestelmän lokipalveluita. Lokeja voidaan käyttää monen eri parametrin valvontaan järjestelmässä. Esimerkiksi prosessorikuormaa, muistinkäyttöä ja verkkoliikenteen käyttötilastoja seuraamalla saadaan tietoa laitteistoresurssien riittävyydestä palvelun saatavuuden turvaamiseksi. Valvomalla sisäänkirjautumisyrityksiä, palveluiden käynnistämistä, käyttöoikeuksien muuttamisia ja tiedostojärjestelmän kirjoitusyrityksiä voidaan havaita murtautumisyrityksiä tai todentaa tapahtunut murtautuminen ja sen kulku. Jos murtautuja ei halua herättää huomiota, lokit ovat ainoa tapa havaita tietomurron tapahtuminen. (Garfinkel ym. 2003, 679; Garfinkel & Spafford 2002, 414-418, Allen 2002, 197-209)

Pelkästään lokeja seuraamalla ei valitettavasti voi varmistua käyttöjärjestelmän turvallisuudesta. Jos murtautuja on saanut käyttöönsä ylläpitäjän tunnukset, hän voi poistaa lokimerkintöjä tai kokonaan estää uusien lokimerkintöjen syntymisen. Tällöin pelkkiä lokimerkintöjä seuraamalla ei voi varmistua tietoturvan tasosta. Tietoturvan varmistaminen vaatii koko järjestelmän toiminnan tarkkailua ja ylläpitäjän omien toimintatapojen arviointia. Toimiiko järjestelmä samanlailla kuin ennen? Olenko varmasti ainoa jolla on ylläpitäjän oikeudet järjestelmään? Milloin viimeksi vaihdoin ylläpitäjän salasanan? Onko kaikki tietoturvapäivitykset asennettu kaikkiin ajettaviin palveluihin ja itse käyttöjärjestelmään? Tärkein esitettävä kysymys käyttöjärjestelmän tietoturvallisuuden kohdalla

on, että jos järjestelmä raportoi ettei tietomurtoa ole tapahtunut, voiko tähän tietoon luottaa. Varmuuskopiot ovat siis taas elintärkeitä. (Garfinkel ym. 2003, 811)

4.4.9 WWW-palvelimen WWW-palvelinohjelmisto

WWW-palvelinohjelmisto on WWW-palvelimen käyttöjärjestelmässä ajettava palvelu, joka vastaanottaa käyttäjältä tulevan sivupyynnön jonka palvelimen käyttöjärjestelmä on sille välittänyt, muodostaa sivupyynnön määrittämän HTML-sivun ja lähettää sen takaisin käyttäjälle palvelimen käyttöjärjestelmän kautta. Kaksi suosituinta palvelinohjelmistoa ovat Apache (v. 1.3.x – 2.2.x) ja Microsoftin Internet Information Services (IIS, versiot 4-6). Kummastakin tuoteperheestä on löytynyt tietoturva-aukkoja vuoden 2006 aikana. Tietoturva-aukkoja on vähemmän kuin käyttöjärjestelmissä mutta niitä silti löytyy. Tietoturvatilanteen seuraaminen päivitysten asentaminen on siis elintärkeää. (Netcraft 2007; Secunia 2006a; Secunia 2006b)

Tietoturvan kannalta palvelinohjelmisto on monimutkainen kokonaisuus. Vaikka palvelimen käyttöjärjestelmään olisi pääsy vain rajatulla määrällä henkilöitä, WWW-palvelinohjelmiston kautta osaan palvelimen resursseista on käytännössä rajaton pääsy kaikkialta maailmasta. Useissa palveluissa (kuten äänestysjärjestelmässä) on julkisia ja kirjautumisen vaativia alueita. Näiden alueiden datan saatavuudella on oltava selkeät rajat ja niiden on pidettävä. Käyttöjärjestelmän tulee ajaa palvelinohjelmistoa rajatuilla oikeuksilla, jotta palvelinohjelmistolla ei ole pääsyä muuhun kuin sille tarkoitettuun dataan palvelimella ja vain halutuin oikeuksin sekä jotta palvelinohjelmisto ei voi poista lokimerkintöjä käyttöjärjestelmän lokijärjestelmästä. Myös palvelun käyttäjien on oltava näkymättömiä toisilleen vaikka he asioivat samassa palvelussa ja tarkkailisivat samaa dataa. Käyttäjän palvelukäskyt ajetaan yleensä omassa palveluprosessissa, joka on WWW-palvelinohjelmistoprosessin aliprosessi. Tälle aliprosessille myönnetään yleensä vielä vähemmän oikeuksia dataan. Esimerkiksi staattisessa HTML-sivustossa kaikki data on vain tiedostoja tietyssä hakemistopolussa. Palveluprosessilla ei ole tällöin muita

oikeuksia kuin lukea tiedostoja kansioista jotka eivät ole salasanan takana ja jotka ovat palvelinohjelmistolle sallitussa alihakemistossa. Kirjoitus, muokkaus ja poisto ovat kaikki kiellettyjä. Palveluprosessit eivät myöskään näe toisiaan, eikä yhden käyttäjän kirjautuminen sivustolle anna oikeuksia salattuun sisältöön muille käyttäjille, vaikka kaikki käyttävät samaa palvelua. (Allen 2002, 89-91)

WWW-palvelinohjelmisto tietoturvan varmistaminen vaatii, että myös käyttöjärjestelmä on tietoturvallisesti konfiguroitu. Palvelinohjelmiston tietoturvallisen konfiguroinnin ja tietoturvapäivitysten asentamisen lisäksi on tärkeää aktivoida palvelinohjelmiston oma lokijärjestelmä. Koska WWW-palvelinohjelmisto on helpoin tapa päästä palvelimelle asti, tietoturvahyökkäykset ja tunkeutumiset alkavat helposti palvelinohjelmiston skannauksella. Lokiin saattaa ilmestyä merkintöjä joissa kokeillaan laajaa määrä URL-sivuja jolloin etsitään mahdollista tietoturva-aukkoa salasanan vaativaan sisältöön, virheitä palvelinohjelmiston oikeuksista käyttöjärjestelmän muihin resursseihin ja tiedostojärjestelmän dataan tai tehdään ehkä jopa palvelunestohyökkäystä. WWW-palvelinohjelmiston loki onkin tärkeä apuväline tunkeutumisyritysten havainnoinnissa. (Allen 2002, 94-97)

4.4.10 WWW-palvelinohjelmiston palvelinlaajennus

Palvelinlaajennusten (”plug-in”) avulla voidaan luoda palveluun dynaamista sisältöä. WWW-palvelinohjelmisto pystyy ilman laajennuksia toimittamaan käyttäjälle vain staattisia tiedostoja. Palvelinlaajennuksen avulla tiedostot voidaan luoda reaaliaikaisesti, ottaen huomioon käyttäjän syötteet ja hakea dataa tietokannoista. Palvelinlaajennukset mahdollistavat siis täysimittaisten sovellusten rakentamisen. Suosittuja palvelinlaajennuksia ovat PHP, ASP, ASP.NET ja Java/JSP. Näistä selvästi suosituin on PHP, josta on löytynyt monta tietoturva-aukkoa vuoden 2007 kolmen ensimmäisen kuukauden aikana. (Sitepoint 2006; Secunia 2007h)

Palvelinlaajennukset ajetaan WWW-palvelinohjelmien aliprosesseina, joten itse palvelinohjelmiston tietoturva-asetuksilla on suuri vaikutus palvelinlaajennusten tietoturvaan. Tietoturva-asetukset ovat oltava kunnossa koska palvelinlaajennuksen suoritettaman koodin avulla voidaan luoda, muuttaa ja poistaa tiedostoja tiedostojärjestelmästä. Käyttäjän sivukutsun aliprosessilla ei siis missään nimessä saa olla oikeuksia muualle kuin WWW-palvelinohjelmiston käyttöön määriteltyihin tiedostoihin ja kansioihin. Palvelinlaajennuksen suorittaman koodin avulla pystyy myös muuttamaan kansioiden ja tiedostojen CHMOD-attribuutteja eli käyttöoikeusasetuksia. Tämän takia aliprosessilla täytyy olla hyvin tarkasti rajatut käyttöoikeudet tiedostojärjestelmään. Palvelinlaajennuksen mukana tulee usein paljon laajennuskirjastoja ja lisätoiminnallisuuksia. Näissä pitää noudattaa samaa minimikokoonpanon periaatetta kuin käyttöjärjestelmässä, jossa vain toiminnan kannalta välttämättömän toiminnot jätetään käytettäväksi. Yksi palvelinlaajennuksen lisätoiminnoista saattaa olla yhteysmahdollisuus tietokantaserveriin. Tämän toiminnon vaaroista kerrotaan kappaleessa 4.4.11, jossa käsitellään tietokantapalvelimen turvallisuutta. Erittäin tärkeää on myös estää lähdekoodimuotoisten tiedostojen luku ulkopuolisilta tahoilta. Tiedoston URL-osoitteen kirjoittamalla koodi suoritetaan mutta ainakin PHP-ohjelmistossa on mahdollisuus käyttää ”allow_url_fopen” -asetusta, joka mahdollistaa lähdekooditiedostojen hakemisen muilta servereiltä koodia suorittamatta ”include”-komennolla. Tällainen mahdollisuus pitää ehdottomasti ottaa pois käytöstä. (Allen 2002, 97-105)

Palvelinlaajennuksen tietoturvauhat ovat laajempi kokonaisuus kuin pelkkä palvelinlaajennuksen oma koodi, koska palvelinlaajennuksen suorittaman vahingollinen koodi on yhtä tuhoisaa järjestelmälle kuin itse palvelinlaajennuksesta löytyvä tietoturva-aukko. Paras tapa parantaa tietoturvaa palvelinlaajennuksen kohdalla on konfiguroida palvelinlaajennus ajettavaksi minimioikeuksin ja minimiominaisuuksilla, että palvelinlaajennuksesta on käytössä uusin versio ja että suoritettava koodi on turvallista. Suoritettavan koodin turvallisuuden varmistamisesta kerrotaan kappaleessa 4.4.12, joka käsittelee koodin tietoturvaominaisuuksia. Tärkeää on myös että palvelinlaajennus kirjaa WWW-palvelinohjelmiston lokiin tapahtumatietoja. Vahingollinen koodi saattaa yrittää muokata tiedostoja joihin ei ole oikeuksia tai suorittaa koodia joka jää ikuisesti pyörimään ja

näin vahingoittaa koko palvelimen suorituskykyä. Näistä pääsee selvyyteen vain lukemalla lokia. (Allen 2002, 97-105)

4.4.11 Tietokantapalvelinohjelmisto

Kaikki laajaa datamäärää käsittelevät ohjelmistot (mukaan lukien WWW-palvelimen palvelinlaajennusten koodit) käyttävät tiedon tallentamiseen ja hakemiseen tietokantapalvelinohjelmistoa. Suosittuja tietokantaohjelmistoja ovat MySQL, Oracle ja Microsoft SQL Server -tuoteperheet. Sekä MySQL-, että Oracle-ohjelmistoista löytyi tietoturva-aukkoja vuoden 2006 aikana. MySQL-ohjelmistosta on saatavilla vapaan lähdekoodin ilmainen versio, joka on hyvin suosittu halvoissa webhotelleissa. (MySQL AB 2006; Secunia 2006c; Secunia 2006d)

Tietokantaohjelmisto vartioi pääsyä dataan ja sen eheyttä. Näiden tärkeiden tietoturvaominaisuuksien toteutukseen ja luotettavuuteen vaikuttaa moni asia itse ohjelmistossa, sen konfiguraatiossa että koko palvelimen tietoturvallisuudessa. Ensimmäisenä tarkasteltavana lähtökohtana on datan säilytys. Tietokantaohjelmisto tallentaa sen tiedostoina palvelimen kovalevylle. Tämän takia on äärimmäisen tärkeää että palvelimen käyttöjärjestelmän käyttöoikeudet ja eri käyttäjien oikeudet tiedostojärjestelmän eri osiin ovat konfiguroitu tietoturvallisella tavalla. Millään muulla ohjelmalla ei saa olla oikeutta lukea tai kirjoittaa dataa sisältäviä tiedostoja, vaan kaikki toiminnot on suoritettava tietokantaohjelmiston kautta. Käyttöjärjestelmän ylläpitäjän käyttäjätunnuksilla pääsee tietenkin lukemaan ja muokkaamaan kaikkia tiedostoja, joten jälleen yksi syy lisää varmistaa etteivät ylläpitäjän käyttäjätunnukset pääse ulkopuolisten tietoon. Datan muuttumisen havaitseminen on vaikeaa, koska ylläpitäjällä on pääsy kaikkialle järjestelmästä eikä suoraan tiedostojärjestelmään kirjoitettaessa jää jälkeä tietokantapalvelimen lokeihin, ja vaikka käyttöjärjestelmän lokeihin jälki jäisikin, ylläpitäjällä on pääsy poistamaan lokimerkintöjä. Jos datatiedostot tiedostojärjestelmässä ovat salakirjoitettu, ylläpitäjällä on varmasti pääsy sinne missä purkuavainta säilytetään. Jos datasta ollaan laskettu tarkas-

tussummia, ylläpitäjä voi muuttaa dataa ja laskettaa summat uudelleen. Tämä on taistelu jota ei voi voittaa. Datan poistamista on helpompi havaita, tietenkin olettaen että tarkastaa tietokannan taulut rivi riviltä samalla tietäen kuinka paljon rivejä niissä pitäisi olla. (Garfinkel ym. 2003, 630; Welling, L. & Thomson, L. 2005, 338-343)

Kun on varmistettu että vain tietokantaohjelmiston kautta on pääsy dataan, voidaan suunnitella käyttöoikeusasetukset tietokantapalvelinohjelmiston sisälle. Näiden suunnittelussa tulee noudattaa taas samoja yleisen palvelimen yläpitämisen minimikokoonpanon ja minimioikeuksien periaatteita, eli tarpeettomat tietokantapalvelinlaajennukset pois käytöstä ja palvelun käyttäjille mahdollisimman vähän oikeuksia. Tietokantapalvelimelle on tietenkin luotava yksi ylläpitäjän tunnus, jolla on oikeus lisätä ja poistaa palvelun käyttäjiä, muokata heidän käyttöoikeuksiaan, luoda ja poista tietokantoja sekä luoda, muokata ja poistaa kaikkien tietokantatauluja sekä taulujen rivejä. Näillä ylläpitäjän tunnuksilla saa vahinkoa aikaiseksi yhtä nopeasti kuin itse palvelimen käyttöjärjestelmän ylläpitäjän tunnuksilla, joten tunnusten tietoturvaa on varjeltava samalla varovaisuudella. Tietokannan datan käyttäjille pitää antaa huomattavasti vähemmän oikeuksia kuin ylläpitäjälle. Tietokantojen ja niiden taulujen hallinta on harvoin tarpeellinen toiminto jokaiselle datan käyttäjälle. Näitä datan käyttäjän käyttäjätunnuksia pitää tallentaa niitä käyttäviin ohjelmiin (kuten palvelinlaajennusten koodiin), jotta dataa voidaan noutaa automaattisesti kysymättä WWW-sivun käyttäjältä tunnuksia. Tietokantapalvelimen datan tietoturva on siis hyvin riippuvaista myös dataa käytävien ohjelmien tietoturvasta. (Garfinkel & Spafford 2002, 410-413; Welling & Thomson 2005, 338-343)

Tietokantapalvelinohjelmiston sijaitessa samalla palvelimella WWW-palvelinohjelmiston kanssa siirtyy data kahden samassa käyttöjärjestelmässä ajettavan prosessin välillä käyttöjärjestelmän välittämänä. Tämä tiedonsiirto on tietoturvallista jos itse käyttöjärjestelmän tietoturvaan voidaan luottaa. Tietenkin pitää varmistua käyttöjärjestelmän tasolla että WWW-palvelimen lähiverkon tasolla, ettei Internetistä tai edes lähiverkosta voi tehdä tietokantakyselyjä tietokantaohjelmistolle jos näin ei haluta tapahtuvan. Tämän voidaan varmistaa Internetin kohdalla laitteistopalomuurilla ja sisäverkon kohdalla palvelimen ohjelmistollisella palomuurilla. Jos sen sijaan tietokantapalvelin-

ohjelmisto sijaitsee fyysisesti eri palvelimella, täytyy palvelimen kappaleissa 4.4.6 ja 4.4.8 mainitut tietoturvanäkökohdat palvelimen lähiverkon ja käyttöjärjestelmän turvallisuudesta tietenkin ottaa huomioon. Lisäksi on huomioitava tiedonsiirron turvallisuus palvelimien välillä. Jos tietokantapalvelin on samassa lähiverkossa jonka kautta WWW-palvelimen sivupyynnöt kulkevat, voi tietokantapalvelimelle yrittää murtautua jos lähiverkon laitteistopalomuuri tai reititin päästää liikenteen Internetistä tietokantapalvelimelle. Turvallisempaa on laittaa tietokantapalvelin WWW-palvelimen eri verkkorajapinnan taakse omaan lähiverkkoon, johon ei ole pääsy muilla kuin WWW-palvelimella. Lisäksi tietoliikenne WWW-palvelimen ja tietokantapalvelimen välillä on salakirjoitettava. Tähän voidaan käyttää samaa SSL-salausta kuin käyttäjän selaimen ja WWW-palvelimen välisessä tiedonsiirrossa. (Silberschatz ym. 2003; Allen 2002, 83)

Tietokantapalvelinohjelmiston tietoturvan varmistamisessa pitää ottaa huomioon palvelimen käyttöjärjestelmän turvallisuus, tietokantaohjelmiston asetukset ja käyttäjäoikeudet, tietoliikenteen salakirjoitus sekä itse tietokantaohjelmiston tietoturvapäivitysten asentaminen. Lisäksi on varmistuttava että dataa hakeva ohjelmisto (eli esimerkiksi WWW-palvelinohjelmiston laajennus) käyttää uusinta versiota tietokantaohjelmiston yhteyskomponentista, jotta voidaan varmistua että halutut tietoturvallisuusominaisuudet varmasti toimivat. Myös tietokantaohjelmiston että käyttöjärjestelmän lokeja on tarkkailtava epäilyttävien tietokantahakujen tai yhteysyritysten havaitsemiseksi. (Garfinkel & Spafford 2002, 471)

4.4.12 Äänestysjärjestelmä

Äänestysjärjestelmällä tarkoitetaan tässä WWW-palvelimella toimivaa, WWW-palvelinohjelmiston palvelinlaajennuksia ja tietokantaa hyväkseen käyttävää ohjelmistoa. Tietoturvavaatimuksina äänestysjärjestelmälle kappaleen 2 mukaan on että äänestäjäkunta on rajattu, jokaisella on oikeus äänestää vain kerran, äänestyspäätöstä ei saa pystyä yhdistämään ehdokkaaseen ja vaalien tulos pitää olla luotettava. Tässä kappaleessa tarkastellaan näkökulmia joiden kautta äänestysjärjestelmän tietoturvallisuutta voi ar-

vioida.

Aikaisemmissa kappaleissa ollaan keskitytty käsittelemään käytettävien ohjelmistojen ja laitteistojen oikeita asetuksia tietoturvan turvaamisen välineinä. Tämä on ollut mahdollista koska tarkasteltavana on ollut selkeä joukko ohjelmistoratkaisuja ja laitetoimintoja, joiden turvallisuus on eri toimittajista huolimatta rakentunut samoista osista. Äänestysjärjestelmän tietoturva noudattaa tietenkin yleisiä ohjelmiston tietoturvan takaamisen periaatteita mutta koska äänestysjärjestelmä ei ole ohjelmistoryhmänä yhtä selkeä käsite kuin vaikka WWW-palvelinohjelmisto, täytyy turvallisuusnäkökulmat käydä läpi asetusten sijaan lähdekoodia lukemalla. Tämä johtuu siitä etten ole onnistunut löytämään yhtään yleisesti käytössä olevaa avoimen lähdekoodin äänestysjärjestelmää. Ohjelmiston turvallisuutta ei voi varmistaa muuten kuin lähdekoodi lukemalla jos ohjelmiston tietoturvallisesta toiminnasta ei ole olemassa yhtään esimerkkiä tai käyttökokemusta.

Ensimmäiseksi pitää tietenkin varmistua, että järjestelmän kaikkien muiden osien tietoturva on kunnossa. Laadukas koodi ei auta äänestysjärjestelmän turvallisuudessa jos joku pystyy lataamaan omaa koodia palvelimelle liian avointen käyttöoikeusasetusten takia ja ohittamaan kaikki äänestysjärjestelmän tietoturvamekanismit. Samoin aputoimintojen (kuten tietokantapalvelimen tietokanta-ajuri WWW-palvelimen palvelinlaajennusohjelmistossa ja SSL-salauksen tuki WWW-palvelinohjelmistossa) pitää olla tietoturvallisessa tilassa, eli uusimpia versioita ja oikein asennettu.

Ensimmäinen tärkeä toiminto äänestysjärjestelmän kannalta on kontrolloida sitä, kenellä on pääsy äänestysjärjestelmään. Koska itse WWW-palvelimen tuottaman palvelu on tietenkin julkisen WWW-osoitteen kautta kaikkien nähtävissä, on äänestystapahtuman saatavuutta rajoitettava muilla keinoin kuin itse palvelu piilottamalla. Tietoturvaa ei muutenkaan saa koskaan perustaa pelkälle piilottamiselle ja uskomukselle, ettei mikään vihamielinen taho sitä koskaan löydä. Palvelun sisällä pääsyä äänestämiseen voidaan rajoittaa käyttäjätunnusten avulla. Kirjautumisen jälkeen käyttäjä pääsee sivustolle johon ei muuten ole pääsyä eivätkä muut palvelun samanaikaiset käyttäjät näe käyttäjän tekemisiä. Koska HTTP on yhteydetön protokolla, täytyy kirjautuneen käyttäjän tunnistus

tehdä muuten kuin yhteyden tilaa tarkkailemalla. Tämä tehdään sessioiden ja keksien avulla. Onnistuneen kirjautumisen jälkeen käyttäjälle luodaan sessio joka saa oman tunnuskoodin. Tämän koodin avulla WWW-palvelu tunnistaa käyttäjät samanaikaisten käyttäjien joukosta. Tämä tunnuskoodi tallentuu palvelimen lisäksi käyttäjän tietokoneelle pienenä keksi-tiedostona selaimen tiedostokansioon tai koodia voidaan kuljettaa mukana URL-osoitteessa kaikkien käyttäjälle mahdollisten toimintojen linkeissä (esimerkiksi http://www.aanestys.fi/aanesta.php?id=769859). (Welling & Thomson 2005, 479-494; Garfinkel & Spafford 2002, 451; Howard & LeBlanc 2003, 436-437)

Sessioiden kummatkin käyttötavat (tunnuskoodin kuljettaminen URL-osoitteessa tai keksinä käyttäjän tietokoneella) sisältävät tietoturvauhkia. Jos tunnuskoodi joutuu muiden tietoon, ketä tahansa koodin tietävä voi käyttää samaa sessiota palvelussa kuin itse käyttäjä. URL-osoitteen mukana kuljettaminen tekee tunnuskoodista näkyvän. Se voidaan poimia sivupyynnöstä tai käyttäjän selaimen välimuistista. Keksi lähetetään myös sivupyynnön mukana sekä se on tallennettuna käyttäjän kiintolevylle. Liikenteen SSL-salakirjoitus auttaa tietoliikenteen salaamisessa mutta ei suojaa käyttäjän koneella olevaa tietoa jos koneelle on päässyt asentumaan vakoiluohjelmisto. Selaimen välimuistin tiedostot ja keksit kiintolevyllä ovat selkokielisessä muodossa. Itse turvakoodin salakirjoittaminen ei auta, koska tieto on muuttumatonta eli salakirjoitetulla tunnuksella pystyy kaappaamaan sessioin yhtä helposti, sillä palvelimen purkaessa salauksen turvakoodi osoittautuu oikeaksi. Parempi tapa parantaa session tietoturvaa on käyttää tunnistukseen myös käyttäjän tietokoneen MAC-osoitetta (Media Access Control) lisäämällä se turvakoodin laskukaavaan. Tällöin palvelin voi aina tarkistaa, että session käyttäjä tulee samalta koneelta kuin mille sessio luotiin. MAC-osoitetta ei pysty huijaamaan palvelimelle ja näin turvakoodin vuotamisen jälkeen sitä ei silti pysty käyttämään session kaappaamiseen. On myös huomattava luoda äänestysjärjestelmään uloskirjautumisen mahdollisuus, joka lopettaa session. Muuten selaimen sulkeminenkaan ei tuhoa session keksiä. Tämä luo tietoturvauhan yleisillä Internet-tietokoneilla, jossa seuraava käyttäjä voi kaapata käyttäjän session tutkimalla keksiä tai selaushistorian URL-osoitteita, koska sessio on yhä hengissä palvelimella. MAC-suojaus ei tietenkään auta tähän koska tietokone on sama. (Welling & Thomson 2005, 479-494; Garfinkel & Spafford 2002, 451; Howard &

LeBlanc 2003, 436-437)

Itse kirjautumisen tarvitsemien tietojen tarkistaminen käyttäjärekisteristä kuten muutkin yhteydet järjestelmän tietokantaan tulee hoitaa tietoturvallisesti. Itse tietokantapalvelinohjelmiston turvallisuudesta voi varmistua kappaleen 4.4.11 kohtien perusteella. Tietokannan käytössä pitää ottaa huomioon lisää tietoturvallisuusnäkökohtia. Tiedon yksityisyyden takia pääsyä tietokantaan on syytä rajoittaa tietokantapalvelimen käyttäjätunnusten avulla. Ongelmana kuitenkin on käyttäjätunnusten tallentaminen. Koska niitä tarvitaan koodissa tietokantayhteyden luonnin yhteydessä, tunnukset pitää tallentaa jonnekin tietokannan ulkopuolelle, josta koodi ne automaattisesti voi hakea. Tietokannan käyttäjätunnuksia ei kannata sitoa äänestysjärjestelmän käyttäjätunnuksiin, koska käyttäjällä ei saa edes teoriassa olla pääsyä tarkastelemaan äänestystapahtumia ja käyttäjätunnuksia. Siksi tietokannan tunnuksia ei voi kysyä käyttäjältä. Käyttäjätunnukset pitää olla joko koodin seassa kovakoodattuna tai ne voidaan hakea erillisestä tiedostosta levyjärjestelmästä. Tämä luo tietoturvauhan siinä tapauksessa, jossa jollakin on pääsy palvelimen tiedostojärjestelmään, mahdollisuus ladata omaa koodia palvelimelle joka voi lukea lähdekooditiedoston tai pahimpana vaihtoehtona, jos palvelinlaajennuksen tietoturva-asetukset ovat liian väljät, joku pystyy lukemaan tiedoston lähdekoodimuodossa jos tiedostoon on CHMOD-oikeudet ovat edes lukuoikeuksilla. (Garfinkel & Spafford 2002, 463-464 ja 471)

Äänestyspäätöksen anonymiteetti varmistetaan tietokannan loogisella rakenteella, jossa ei pysty yhdistämään äänestäjää ja äänestyspäätöstä. Ainoa äänestäjästä tallentuva tieto on se, onko äänestäjä äänestänyt. Jos äänestäjiä on yhteensä vain muutama on teoriassa mahdollista tarkkailla ja selvittää äänestyspäätöksiä vertailemalla tietokannan dataa tietyin ajanhetkin. Jos esimerkiksi tiettynä aikavälinä tulee vain yksi ääni, voi äänestäjän selvittää katsomalla tietokantataulusta kenen kohdalla äänestysoikeus on käytetty edelliseen tarkasteluun verrattuna. Tällaisen tutkinnan voi estää varmistumalla tietokantapalvelimen tietoturvasta.

Vaalien tulosten luotettavuutta voidaan tarkastella äänestystapahtuman kulun kautta.

Äänestämishetkellä tieto äänestyspäätöksestä tallentuu tietokantaan mutta mistä voidaan varmistua että ääniä laskiessa tämä tieto on pysynyt muuttumattomana? Ylläpitäjä pystyy väärentämään aikaleimoja, uudelleen laskettamaan hash-tarkastuslukuja ja murtamaan ja uudelleen salakirjoittamaan dataa jos purku ja salausavain on jossain järjestelmässä tallennettuna. Lokeihin ei myöskään voi luottaa koska ylläpitäjällä pääsy muokkaamaan myös niitä. Käyttämällä jotain yksilöllistä tietoa (kuten tarkkaa aikaleimaa) äänestystuloksen kanssa hash-tarkastussumman laskentaan, joka sitten salakirjoitetaan tekniikalla, jonka purkuun vaaditaan eri avain. Tätä purkuavainta ei tallenneta mihinkään järjestelmään vaan se voidaan monessa osassa eri ihmisille säilytykseen. Tällöin äänestytettyjä ääniä ei saa tarkasteltaviksi, ellei purkuavainta yhdistetä. Tämä on kuitenkin laiha lohtu, koska ylläpitäjän tunnuksilla vanhat äänestysmerkinnät on voitu poistaa ja luoda uudet tilalle samalla salakirjoitusavaimella ja väärennetyllä aikaleimalla. Mistään ei voi varmistua että tieto, mitä äänestysjärjestelmä antaa äänestyksen tulokseksi, ei ole muuttunut äänestystilanteen ja ääntenlaskennan välillä. Tietoturvaa voidaan tällä osa-alueella parantaa mutta niin kauan kuin tietokantapalvelimelle ja sen käyttöjärjestelmään on edes olemassa ylläpitäjän salasanat, ei tulokseen voida luottaa täydellisesti.

Vaikka lähdekoodi sisältäisi kaikki tässä osiossa mainitut ominaisuudet ja toimisi tietoturvallisella palvelimella, äänestysjärjestelmä saattaa silti olla helposti murrettavissa ilman ylläpitäjän tunnuksiakin turvattoman koodin logiikan takia. Koska äänestysjärjestelmä on interaktiivinen palvelu, ohjelma vastaanottaa syötteitä käyttäjältä. Kaksi tapaa välittää syötteitä palvelinlaajennukselle on käyttää HTML-lomaketta tai liittää tiedot URL-osoitteeseen session tunnuskoodin tapaan. Tämä liikenne käyttäjän ja palvelimen välillä voidaan salakirjoittaa mutta tämä ei olekaan ongelma. Vaaran aiheuttaa tahallaan epäkelpo syöte, jolla pyritään löytämään mahdollisuuksia suorittaa omia komentoja äänestysjärjestelmässä. Kaksi epäkelpoon syötteeseen perustuvaa yleistä hyökkäysmenetelmää on SQL-injection ja Code-injection. Jos äänestysjärjestelmä tekee SQL-kyselyn suoraan käyttäjän syötteiden perusteella, tiettyjä syötteitä käyttämällä SQL-lauseen hakutulos saadaan muuttumaan erilaiseksi kuin se on tarkoitettu. Esimerkiksi ULR-osoite ”http://www.aanestys.fi/aanesta.php&tunnus=123&ehdokas=5” jää muistiin selaushistoriaan ja kertoo lähes selkokielellä, että äänestäjä tunnuksella 123 äänesti ehdokasta 5. Selaushistorian tyhjennys auttaa äänestystuloksen selville saamiseen mutta ovelampi

käyttäjä varmasti kokeilisi syöttää saman URL-osoitteen selaimeen uudelleen onnistuakseen ehkä äänestämään kahdesti, tai muokkaamaan komentoa haluamakseen. Jos syöte ”tunnus” menee lähdekoodissa tarkastamatta SQL-lauseen WHERE-osaan, voi yksinkertaisesti syöttämällä tunnukseksi osoiteriville ”123 AND 124 AND 125” aiheuttaa kolme eri äänestystapahtumaa (jos 123, 124 ja 125 ovat käyttäjätunnuksia) , jos koodissa ja SQL-lauseen muodostamisessa ei ole osattu ottaa asiaa huomioon. Vaalien tulos ei ole enää luotettava vaikka järjestelmän tietoturvaa ei ole murrettu klassisessa mielessä (kenelläkään ei ole hänelle kuulumattomia käyttäjätunnuksia). Pelkän datan luotettavuuden lisäksi SQL-lauseen kautta voidaan yrittää suorittaa kaikkia tietokantaserverin tukemia toimintoja. Esimerkiksi SQL Server -ohjelmistossa komento ”"exec master..xp_cmdshell 'ping 10.10.1.2"” mahdollistaa ping-komennon suorittamisen, jonka avulla hyökkääjä voi tutkia Internettiin näkymättömän lähiverkon koneiden portteja ja etsiä haavoittuvuuksia. (Howard & LeBlanc 2003, 397-412; SecuriTeam 2002)

SQL-injection hyökkäyksiä voidaan estää käyttämällä valmiiksi tallennettuja SQL-kyselyitä (ei juurikaan mahdollista interaktiivisissa ohjelmissa) tai suodattamalla pois käyttäjän syötteestä kaikki SQL-komennon suorittamisen kulkua muuttavat merkit kuten heittomerkit, kauttaviivat ja takakenot sekä kaksoispisteet ja rivinvaihdot. Tämä ei tietenkään ratkaise SQL-komentoon sopivia parametreja, kuten edellä mainittu ”123 AND 124 AND 125”. Tämän ongelman ainoa paras ratkaisutapa on käyttää SQL-lauseen parametrointia. Tällöin SQL-komentoa ei rakenneta merkkijonoja toisiinsa liittämällä vaan upottamalla parametrin valmiiseen lauseeseen tarkastussääntöjen mukaan. Esimerkiksi jos käyttäjätunnus on numero, parametriksi WHERE-lauseeseen kelpaa vain numero. Tämä voidaan tarkistaa helposti. Tietenkin on mahdollista syöttää vain yksi väärennetty käyttäjätunnus SQL-lauseeseen. Tämä mahdollisuus on tietenkin pitänyt estää jos aiemmin varmentamalla, ettei äänestystapahtuma ole mahdollinen kuin session avulla tunnistetulle käyttäjätunnukselle. Lisäksi pitää poistaa käytöstä SQL-hakujen virheilmoitusten printtaus sillä järjestelmästä tietoturva-aukkoja etsivä murtautuja saa niistä muuten arvokasta tietoa SQL-lauseiden rakenteesta. (Howard & LeBlanc 2003, 401-412)

Code-injection on XSS-menetelmä (cross-site scripting) jossa sivuston sisältöön yritetään vaikuttaa syöttämällä virheellistä dataa yrityksenä huijata käyttäjä väärälle sivustolle esimerkiksi phishing-yritystä varten tai ryöstää keksien tietoa. Esimerkkinä voi toimia sähköposti, jonka huijari on lähettänyt äänestäjille ylläpitäjän nimissä, jossa käsketään kirjautua sisään äänestysjärjestelmään. Linkki voi näyttää aidolta (http://www.aanestys.fi) mutta sähköpostin HTML-koodi voi sisältää ”onmouseover”-tyylisiä JavaScript-komentoja, joilla voidaan suorittaa omaa koodia, esimerkiksi lukea sivuston keksin tiedot ja lähettää ne eteenpäin huijarille. Tällöin Internet-selaimen tietoturva, joka estää sivuston JavaScript-koodia lukemasta muiden sivustojen keksejä, ei toimi. Tätä vastaan voidaan suojautua olemalla tallentamatta kekseihin mitään tietoturvan vaarantavaa tietoa (MAC-osoitteella koodattu session numero ei ole tätä juuri tuon MAC-osoitteen ansiosta) tai ainakin salakirjoittamalla tiedot tehokkaasti. (Howard & LeBlanc 2003, 413-438)

Toinen XSS-menetelmä perustuu dynaamisen sisällön heikkouksiin. Itse rakennetun ”julkaisujärjestelmän” tiedonhakumenetelmä voi olla yksinkertaisuudessaan ”index.php?sivu=yhteystiedot”, jossa parametri on vain tiedostonimi tai kansio. Tällöin saattaa olla mahdollista väärentää sivun linkitysjärjestelmä lataamaan WWW-sivusto muualta, kuten esimerkiksi ”index.php?sivu=http://www.pahasivu.net/istutaSeurantakeksi.html”. Linkki lataa sivuston osaksi vahingollista koodia. Linkkiä jakelemalla foorumeissa ja muualla saa varmasti pahaa aikaiseksi, esimerkiksi tekemällä vastaavan linkin äänestysjärjestelmän uutisosioon. Tällaisen XSS-aukon saa korjattua puhtaasti ohjelmoimalla tarkastuksia koodiin URL-osoitteiden varalta, sekä käyttämällä muuta resurssien tunnistusmetodia kuin syötteenä saatua nimeä.

Tiedostopolkukomentojen kanonisen esitystavan varmistaminen on yksi tärkeä osa-alue lähdekoodin tietoturvassa. Ongelmana on mahdollinen varsinkin silloin kun resursseja tunnistetaan nimen perusteella, pahimmassa tapauksessa vielä käyttäjän syötteen pohjalta. Ongelma periytyy myös WWW-palvelinohjelmistoon ja palvelimen käyttöjärjestelmään asti. Jos esimerkiksi kansio ”http://www.aanestys.fi/piilo” sisältää tiedostoja joi-

hin kenelläkään ulkopuolisella ei saa olla pääsy (kuten vaikka tiedoston, jossa on tietokannan salasanat), miten järjestelmä tulkitsee kansionimeä ”PIILO” tai ”piiLO”? Apple Mac OS X ensimmäisen versiossa oli tämä ongelma, jos järjestelmän mukana tullut Apache-palvelin oli käytössä. Tämä ongelma on helposti testattavissa mutta tilanne menee vaikeammaksi koska huomioon pitää ottaa myös eri tavat esittää merkkejä. ASCII koodisivut ovat yleisyytensä ansiosta varmasti kaikkien ohjelmistojen hallussa mutta entä heksadesimaalinen esitysasu (esimerkiksi ”%20” on välilyönti), UTF-8 ja UCS-2 merkistö? Lisäksi on otettava huomioon monikirjaimisten merkkien kirjoitusasu. Esimerkiksi takakeno (\) on UTF-8 merkistössä ”&5c” mutta myös nuo kolme kirjaintakin on koodattava. Eli ”%25%35%63%” vastaa samaa merkkiä. On siis oltava erityisen tarkkana kun tulkitaan URL-osoitteen resurssipyyntöä tai käyttäjän syötettä, varsinkin on oltava selvillä käytettävästä merkistöstä ja siitä, tukeeko järjestelmän jokainen osa (käyttöjärjestelmä, WWW-palvelin, palvelinlaajennus ja tietokantaserveri) käytettävää merkistöä ja onko haluttu merkistö käytössä. Resursseja ei pitäisi koskaan tunnistaa syötteenä saadun nimen perusteella, esimerkiksi kansion käyttöoikeudet pitäisi määrittää session avulla tietyille käyttäjille, ei resurssin nimeen perustuvilla kieltolistoilla. (Howard & LeBlanc 2003, 363-396)

Puskurien ylivuodot ja taulukon indeksin ylitykset ovat yhä yleisimpiä tietoturva-aukkojen syitä niin ohjelmistoissa kuin käyttöjärjestelmissäkin, vaikka ongelma ja sen tietoturvauhat on tiedetty jo ainakin 20 vuotta, periaatteessa jo 1960-luvulta lähtien. Vielä vuonna 2002 kuitenkin näihin perustuvia ohjelmointivirheitä ja niiden seurauksena tietoturva-aukkoja löytyi Apache WWW-palvelimesta, SSH Secure Login Serveristä ja monista Microsoftin tuotteista. Nykyisin ongelma on kuitenkin keskittynyt C ja C++ kielellä tehtyyn koodiin, koska nämä ohjelmointikielet ohjelmoijalle enemmän vapauksia. Esimerkiksi muuttujaan pystyy sijoittamaan enemmän dataa kuin sille varattu muistiosoiteavaruus antaa myöten. Tällöin ylimenevä data kirjoitetaan suoraan muistiin muuttujan muistialueen ulkopuolelle. Jos tämä ylimenevä koodi sisältää suoritettavaa koodia, puskurin ylivuodon avulla saattaa pystyä suorittamaan omia komentoja järjestelmässä. Korkeamman tason kielet, kuten Java, Perl ja C#, tarkkailevat taulukoiden kokoa ja muuttujien kokoa paljon tarkemmin, ja estävät vastaavat ylivuodot. Ohjelma vain kaatuu virheeseen mutta muisti ei korruptoidu. Jos äänestysjärjestelmä toteute-

taan jollain suosituimmista kehitysympäristöistä (ASP.NET, PHP tai Java/Jsp) ei vastaavat virheet ole vaarana. (Garfinkel ym. 2003, 23; Howard & LeBlanc 2003, 363-396)

Tietoturvan murtumista estävin ohjelmointitekniikoiden lisäksi tärkeää on myös luoda ohjelmaan tietoturvan tarkkailua ja ylläpitoa tukevia toimintoja, kuten lokit ja ohjelman tiedostojen tarkastus. Murtautumisyrityksiä voi havaita ennalta ainoastaan lokeja seuraamalla, joten on tärkeää että myös itse äänestysjärjestelmän kirjaa lokia joko omaan lokijärjestelmään tai käyttöjärjestelmän yhteiseen lokiin. Yleisesti hyvänä keinona on kirjoittaa lokiin kaikki ohjelman virheet. Jos kirjautuminen epäonnistuu samasta IP-osoitteesta satoja kertoja lyhyestä ajassa tai jos järjestelmä saa URL-osoitteen kautta epäkelpoja syötteitä, on syytä olettaa jonkun yrittävän tunkeutua järjestelmään. Lokien toiminnan kannalta on tietenkin oleellista että ohjelma kirjoittaa lokiin mielekkäitä virheilmoituksia, josta saa selville tarkan suorituspolun, jossa virhe on tapahtunut. (Garfinkel & Spafford 2002, 445)

Palvelunestohyökkäyksen vaaroja on käsitelty jo palvelimen laitteiston sekä WWW-palvelinohjelmiston kohdalla mutta oikeastaan vaaraa pitää analysoida koko palvelimen toiminnan laajuudelta. Yhdenkin palvelun suorittamiseen tarvittavan osan tehoton tai tuhlaileva resurssien käyttö saattaa tehdä palvelusta tukkeutuneen palvelunestohyökkäyksen aikana. Valmiiden ohjelmistojen kohdalla voimme vain toivoa ohjelman koodin olevan tehokkainta mahdollista. Äänestysjärjestelmän kohdalla asiasta pitää olla erityisen tarkka, koska ohjelmiston kohdalla kokemuksia resurssien käytöstä ei vielä ole. Ohjelmiston tehokkuutta palvelunestohyökkäyksen kannalta voi tarkastella kolmella mittarilla: prosessoriajan käyttö, keskusmuistin käyttö sekä tietoliikenneyhteyden kapasiteetin käyttö. (Howard & LeBlanc 2003, 517-533; Garfinkel & Spafford 2002, 446)

Prosessoriajan käyttö riippuu äänestysjärjestelmän kodin tehokkuudesta. Pienillä käyttäjämäärillä tietyn toiminnon tehottomuutta ei välttämättä vielä havaitse mutta palvelunestohyökkäyksen aikana prosessoriajan tuhlaus nousee helposti esiin. Koodin tehokkuutta ei tietenkään saa nostaa tietoturvaominaisuuksien ohi tärkeysjärjestyksessä mutta varsinkin merkkijonojen käsittelyn määrällä on suuri vaikutus koko ohjelman suoritus-

kykyyn. Tällä on merkitystä varsinkin jos hyökkääjä pystyy samalla syöttämään järjestelmää ylimitoitetun määrän dataa sivunhakupyynnössä. Jos esimerkiksi koodi etsii URL:in kautta syötteenä tulleesta datasta hipsuja ja kenoviivoja, tehoton etsimisalgoritmi saattaa hidastaa koko järjestelmää monikertaisesti pelkkää sivulatauksien määrään perustuvaan palvelunestohyökkäykseen verrattuna. (Howard & LeBlanc 2003, 521-529)

Keskusmuistin käyttö on prosessoriajan käytön kanssa vastaava mittari lähdekoodille, jonka heikkoudet saattavat tulla esille muistin kulutuksen osalta vasta palvelunestohyökkäyksen aikana. Ongelma saattaa syntyä jos tarkasti rajattujen SQL-lauseiden sijaan datan lopullinen rajaus tehdään vasta itse koodissa. Tällöin tietokannasta saatetaan hakea suuria määriä tietoa muistiin, joka valtavalla määrällä sivupyyntöjä ja ehkä vielä SQL-injection hyökkäyksellä maustettuna saa tehokkaankin palvelimen muistin täyttymään. Tähän liittyy myös tehokkuus muiden resurssien käytöstä. Esimerkiksi tietokantapalvelimen suorituskykyyn vaikuttaa valtavasti SQL-lauseden tehokkuus. Monilla laajoilla JOIN-käskyillä tietokantapalvelimen saa varmasti polvilleen. Sama sääntö koskee äänestysjärjestelmän käyttämiä muita resursseja kuten esimerkiksi väliaikaistiedostojen määrää levyjärjestelmän nopeuden kannalta. (Howard & LeBlanc 2003, 529-531)

Tietoliikenneyhteyden siirtokapasiteetin kannalta palvelunestohyökkäys voidaan tehdä joko verkkolaitteistoa rasittavalla ping-hyökkäyksellä (käsitelty palvelimen lähiverkon tietoturvan kohdalla) tai sivulatausten määrällä. Nykyajan raskaat, paljon kuvia sisältävät sivut saattavat olla kooltaan jopa megatavun luokkaa, joten vaikkapa kaksisataatuhatta samanaikaista sivupyyntöä saa minkä tahansa tietoliikenneyhteyden polvilleen. Ongelmaa voi helpottaa pakkaamalla sivut ennen palvelimelta lähettämistä GZIP-algoritmilla, jonka selain käyttäjän koneella sitten purkaa. Toinen vaihtoehto, joka pitäisi olla itsestäänselvyys, on WWW-sivun järkevä suunnittelu ja toteutus. Kuvien määrä ja koko tulisi minimoida, koska pelkästään sadan samanaikaisen käyttäjän kohdalla puolen megatavun kokoero sivustossa tekee 50 megatavun tiputuksen tiedonsiirtotarpeeseen sekunnissa. (Howard & LeBlanc 2003, 532-533)

Prosessorin, keskusmuistin, tietokantaserverin ja levyjärjestelmän käyttöastetta äänes-

tysjärjestelmän kannalta voi optimoida ja minimoida huolellisella suunnittelun ja laadukkaan dokumentaation tuomalla ohjelmiston loogisella toteuttamisrakenteella, laadukkailla ohjelmointimetodeilla ja tietenkin testaamalla järjestelmä huolellisesti sekä tietoturvan että suorituskyvyn näkökulmasta. Liitteenä (Liite 1) oleva äänestysjärjestelmän määrittelydokumentaatio antaa ohjenuoran järjestelmän toteuttamiseen ja kappaleessa 5 käydään läpi ohjelmiston testaamisen näkökulmia äänestysjärjestelmän luotettavuuden ja tietoturvan kannalta. Testaaminen on käytännössä ainoa tapa jolla sinänsä määrittelemättömästä konseptista ”laadukkaat ohjelmointimetodit” saadaan jotenkin mitattava. Toteutettavan äänestysjärjestelmän laatua voi tämän osion 4.4.12 tietoturvallisen koodin näkökohtien lisäksi arvioida seuraavan järjestelmän turvallisuutta kuvaavan listan avulla. Sen määrittelivät Jerome Saltzer ja M.D Schroeder vuonna 1975 artikkelissaan ”The Protection of Information in Computer System”. Lista on yhä ajankohtainen.

1. Käyttäjillä ja ohjelmilla pitäisi olla mahdollisimman vähän oikeuksia järjestelmän resursseihin. Oikeuksia saa olla vain juuri sen verran, että tarkoitettu tehtävä voidaan suorittaa. Kaikki sen ylittävät oikeudet tulisi erikseen pyytää, eikä niitä saisi myöntää oletuksena.
2. Ohjelmiston rakenne tulee suunnitella mahdollisimman selkeäksi ja suppeaksi, jotta sen toiminta voidaan lähdekoodia lukemalla tarpeeksi helposti todentaa ja että sen kaikki ominaisuudet voidaan onnistuneesti toteuttaa, testata ja ylläpitää.
3. Jokaisen toiminnon kohdalla käyttäjäoikeudet pitää tarkistaa erikseen. Mitään oletuksia käyttäjän oikeuksista ei saa tehdä.
4. Ohjelmiston rakenteen tulee olla avoimesti todennettavissa. Tietoturva ei saa perustua ominaisuuksien piilottamiseen.
5. Käyttäjän tunnistaminen tulee perustua useampaan kuin yhteen tarkistukseen. Mikä on tarpeellinen määrä todentamaan että käyttäjä todella on käyttäjä?
6. Järjestelmän samanaikaiset käyttäjät tulee olla eristetty toisistaan. Käyttäjien ei tule saada tietää toistensa tekemisistä.
7. Tietoturvaominaisuuksien pitää olla käytettäviä jotta niitä ei haluta ohittaa.

4.5 Yleiset toimintaympäristöt

Äänestysjärjestelmän toimintaympäristö vaikuttaa paljon sen tietoturvan tasoon, joten tässä kappaleessa käydään muutaman todennäköisimmän toimintaympäristön kautta läpi näiden tietoturvanäkökohtia. Toimintaympäristöllä tarkoitetaan tässä äänestysjärjestelmän osien ylläpitomallia ja hallittavuutta. Ylläpitomalli on erittäin tärkeä koska tietoturvan takaaminen vaatii järjestelmän säännöllistä valvontaa, ohjelmistojen päivitystä sekä yleisen tietoturvatilanteen seuraamista pitkällä aikavälillä. Järjestelmän onnistunut asentaminen ei takaa sen tietoturvaa koko käytön ajaksi vaan tietoturvan ylläpito on jatkuva prosessi (Garfinkel ym. 2003, 543). Hallittavuudella tarkoitetaan tässä yhteydessä järjestelmään pääsyn hallintaa. Miten voidaan tarkistaa ja varmistua siitä, kenellä on pääsy järjestelmään ja kenen tiedossa on ylläpitäjän tunnukset?

Fyysisellä tasolla kolme kokonaisuutta ovat käyttäjän tietokone, Internet ja palvelin. Eri käyttöympäristöissä näiden kolmen komponentin hallittavuudessa ja tietoturvan tarkistamisessa on suuria eroja. Ensiksi pitää tietenkin todeta, ettei äänestysjärjestelmää käyttävällä taholla ole hallintamahdollisuuksia tai edes minkäänlaisia tarkastusmahdollisuuksia Internetin tietoturvaan. Internet on kooltaan niin valtava ja jatkuvasti muuttuva, ettei tietoliikenteen tarkkaa reittiä voi edes mitenkään tarkasti määrittää. Lisäksi Internet-yhteyden palveluntarjoajan järjestelmien tietoturvaa ei varmasti pääse ketä tahansa tarkastamaan omakätisesti. Palveluntarjoajan vastatessa kyselyyn että ”turvallista on”, vastaukseen on vain luotettava. Asialle ei voi tehdä sen enempää.

Käyttäjän eli äänestäjän tietokoneen hallinta riippuu, missä äänestys tehdään. Jos lähtökohtana on, että WWW-äänestys tapahtuu ennalta mainitussa äänestyspaikassa tarkoitukseen varatulla tietokoneella, äänestyksen järjestäjällä on mahdollisuus tarkistaa ja vaikuttaa tietokoneen tietoturvaan, jolla äänestys tapahtuu. Jos sen sijaan äänestää voi miltä tahansa Internet-yhteyden omaavalta tietokoneelta, äänestyksen järjestäjällä ei ole mitään mahdollisuuksia vaikuttaa tietokoneiden tietoturvaan. Tällöin käyttäjää voidaan

vain neuvoa, ohjeistaa ja ehkä korkeintaan kehottaa huolehtimaan äänestämiseen käytettävän tietokoneen tietoturvasta. On kuitenkin otettava huomioon ettei käyttäjällä ole välttämättä tietotaitoa esimerkiksi päivittää Internet-selainta, käyttöjärjestelmää tai muitakaan koneen ohjelmia, saati taitoa tarkistaa koneen lähiverkon turvallisuutta. Äänestys saatetaan tehdä myös tietokoneella johon käyttäjällä ei ole ylläpitäjän oikeuksia, kuten Internet-kahvilassa. Tällöin käyttäjä ei pysty päivittämään Internet-selainta tai käyttöjärjestelmää, eikä välttämättä mitenkään varmistumaan lähiverkon turvallisuudesta. Ei ole olemassa mitään toimintamallia tai tekniikkaa, jolla äänestyksen järjestäjä voisi varmistaa äänestäjän koneen tietoturvallisuuden, jos äänestys voi tapahtua miltä tahansa tietokoneelta. Mikään JavaScript- tai Java Applet -ohjelma ei pysty tarkastamaan sekä tietokoneen ohjelmiston sekä sen lähiverkon turvallisuutta.

Palvelimen näkökulmasta on kolme toimintaympäristövaihtoehtoa. Palvelinta voidaan pitää täysin omassa kontrollissa, jolloin se käytännössä sijaitsee jossain äänestäjän järjestäjän tiloissa. Tällöin palvelimen lähiverkon, laitteiston ja ohjelmiston turvallisuus on äänestyksen järjestäjän vastuulla. Toisessa vaihtoehdossa itse fyysinen laite on esimerkiksi palveluntarjoajan konesalissa mutta järjestäjä hallinnoi sen ohjelmistoja käyttöjärjestelmästä lähtien. Kolmannessa vaihtoehdossa sekä palvelimen laitteisto että ohjelmisto on palveluntarjoajan hallussa. Näihin kaikkiin sisältyy hyviä ja huonoja puolia, kun otetaan huomioon tietoturva sekä yleiset toimintamahdollisuudet äänestysjärjestelmän tarkoitetussa käyttäjäryhmässä.

Palvelimen pitäminen täysin omassa hallinnassa takaa tietenkin parhaan hallittavuuden. Tämä vaihtoehto on ainoa tapa varmistua palvelimen lähiverkon tietoturvasta ja sekä siitä, kenellä on ylläpitäjän käyttäjätunnukset palvelimen eri ohjelmistoihin, käyttöjärjestelmään että lähiverkon muihin laitteisiin. Tietoturvan ja palvelun saatavuuden kannalta on kuitenkin myös oleellista, että kaikki palvelimen asetukset on oikein konfiguroitu ja että palvelimen Internet-liittymän tiedonsiirtonopeus on riittävä äänestäjämäärään nähden. Palvelimen ja sen lähiverkon konfigurointi vaatii asiantuntemusta ja kokemusta eikä äänestysjärjestelmää käyttävistä yhdistyksistä tai opiskelijakunnista välttämättä löydy itseltään asiantuntevaa henkilöstöä tähän. Tällöin asiantuntemus pitää ostaa

ulkopuolelta. Hintataso tällaisille konsultointipalveluille saattaa olla erittäin korkea tilaajan maksukykyyn nähden. Tämä malli ei myöskään tue järjestelmän jatkuvan ylläpidon tarvetta. Koska tietoturvaa pitää jatkuvasti valvoa ja ohjelmistoja päivittää, tarvitsisi konsulttipalveluja ostaa säännöllisesti ja tiheään.

Ohjelmistojen ylläpidon lisäksi on huolehdittava myös laitteiston tietoturvasta ja varmuuskopioista. Toimiston nurkka on äärettömän vaarallinen paikka palvelimelle ympäristöstä aiheutuvien uhkien että varkauksien kohdalla. Opiskelijakunnat toimivat usein koulun tiloissa. Tällöin ei ole tarkkaa tietoa, kenellä kaikilla on pääsy tähän tilaan. Lisäksi varmuuskopioiden ottaminen ja niiden turvallinen säilytys vaativat osaamista ja säännöllisyyttä. Kaiken tämän lisäksi itse palvelinlaitteiston tulee olla tarpeeksi tehokasta ja vikasietoista. Mikään vanha pöytäkone ei kelpaa WWW-palvelimeksi.

Tietoliikenneyhteydet ovat myös oltava tarpeeksi nopeat äänestysruuhkia sekä palvelunestohyökkäyksiä ajatellen. Jos sivuston koko on 100 kilotavua, ei normaalin ADSL-yhteyden 1 megabitin paluukaista riitä kuin kahden samanaikaisen käyttäjän palveluun. Internet-yhteys on siis oltava huomattavasti nopeampi mikä tietenkin tarkoittaa että se on myös huomattavasti normaalia ADSL-liittymää kalliimpi.

Toinen vaihtoehto on vuokrata palvelin ja Internet-yhteys joltain palveluntarjoajalta, jolloin itse laite on palveluntarjoajan konesalissa. Vuokrata voi koko palvelinlaitteiston tai virtuaalipalvelimen. Tässä vaihtoehdossa laitteiston ylläpito ja lähiverkon ylläpito sekä Internet-yhteys ovat palveluntarjoajan ylläpitämiä mutta myös täysin heidän hallinnassaan. Lisäksi käyttöjärjestelmän ja ohjelmistojen konfigurointi sekä tietoturvan seuraaminen vaatii yhä ulkopuolisen konsultoinnin hankkimista. Lisäksi varmuuskopioinnista pitää yleisesti maksaa erikseen.

Tietoturvan kannalta tämä vaihtoehto ratkaisee osan tietoturvaongelmista mutta tuo uusia tilalle. Lähiverkon ja palvelinhuoneen turvallisuutta toivottavasti valvotaan, joten omaa palvelinhuonetta ei enää tarvitse rakentaa. Lisäksi Internet-yhteydet ovat huomat-

tavasti nopeampia, usein jopa 100 megabittiä sekunnissa tai yli. Tietenkään ei pidä olettaa, että lähiverkko on turvallinen tai että palvelinlaitteisto on vikasietoinen. Tästä pitää tietenkin varmistua. Varmuuskopiopalvelun kohdalla pitää ottaa huomioon varmuuskopioiden yleiset turvallisuusnäkökulmat, eli turvallinen säilytys sekä varmuuskopioinnin tiheys. Kenellä tahansa palveluntarjoajan työntekijällä on luultavasti pääsy varmuuskopioihin sekä palvelimen verkkoliikenteen tarkkailuun. Tämä pitää tiedostaa palveluntarjoajaa valitessa.

Kolmannessa vaihtoehdossa koko palvelimen ylläpito on palveluntarjoajan hoidossa, jolloin äänestysjärjestelmän käyttäjälle jää vain itse äänestysjärjestelmän asennus. Palvelinlaajennusten avulla toteutetuissa ratkaisuissa asentamiseksi riittää usein FTP:n kautta tehty tiedostojen siirto. Ohjelma on mahdollista ohjeistaa itse luomaan tarvittavat tietokannat ja muuttamaan kansioiden oikeuksia. Tällainen asennus on mahdollista tehdä hyvällä dokumentaatiolla ilman asiantuntija apuakin. Asennuksen jälkeen tietoturvan taso on kuitenkin tarkistettava, sillä palvelimen konfigurointien erojen takia ajoympäristön asetuksilla saattaa olla suuria vaikutuksia äänestysjärjestelmän toimivuuteen sekä tietoturvaan.

Helppokäyttöisyydessä saavutettu etu kalpenee tietoturvassa menetetyn hallinnallisuuden rinnalla, sillä nyt jollain muulla taholla on ylläpitäjän oikeudet palvelimen käyttöjärjestelmään sekä tietokantapalvelimeen. Palveluntarjoaja voi tehdä haluamiaan muutoksia tietokannan dataan eikä äänestysjärjestelmän käyttäjä voi mitenkään havaita tai estää tätä. Varmuuskopioinnissa on lisäksi samat tietoturvauhat kuin palvelimen vuokraamisen kohdalla. Lisäksi ei myöskään voida varmistua, että palveluntarjoaja seuraa yleistä tietoturvatilannetta ja ohjelmapäivityksiä, saati asentaa päivityksiä. Väärin konfiguroituna palvelu on lisäksi erittäin vaarallinen, jos esimerkiksi saman palvelimen eri käyttäjät pääsevät näkemään toisensa resursseja.

4.6 Tietoturvalliset toimintatavat ja tietoturvapolitiikat

Edellisissä osiossa on käsitelty äänestysjärjestelmän ohjelmisto- ja laitetason turvallisuusnäkökohtia kerros kerrokselta. Tärkeää on kuitenkin olla unohtamatta käyttäjien osuutta järjestelmän tietoturvaan kaikilla tasoilla. On tärkeää muistaa, että kaikkien tietomurtojen takana ihminen, joten on äärettömän tärkeää luoda säännöt sille, kehen luotetaan (Garfinkel ym. 2003, 823). Tämän lisäksi on varmistettava, että kaikkea tietoturvallista tietoa käsitellään tarpeellisella huolellisuudella ja että järjestelmään pääsyn omaavat henkilöt tietävät vastuunsa. Tämä on ongelma yhdistyksissä ja opiskelijakunnissa, joilla harvoin on varaa palkata ihmistä huolehtimaan järjestelmien turvallisuudesta, tai edes rahaa hankkia konsultointiapua näihin kysymyksiin. Tietoturvallisten toimintatapojen taso saattaakin riippua täysin sen hetkisten toimijoiden tietotaidosta ja toimijoiden vaihtuessa käytännöt saattavat muuttua tai kadota täysin. Jos WWW-äänestysjärjestelmä tuodaan tähän käyttöympäristöön, ei teknisen tason tietoturvasta ole apua jos kaikki muut käytännöt eivät ole kunnossa.

Jokaisella äänestysjärjestelmää käyttävällä taholla pitää olla selkeä tietoturvapolitiikka. Tällä tarkoitetaan kaikkien toimintaympäristössä työskentelevien tiedossa olevaa ohjeistuksia ja sääntöjä, joilla yhteisön tietoturvalliset toimintatavat rakentuvat. Politiikan määrittelyssä pitää olla mukana tietoturvanäkökohdista hyvin perillä olevia henkilöitä sekä yhteisön johto/esimiehet. Tällä kokoonpanolla määritellään yhteisön toimintamallin asettamat tietoturvavaatimukset ja tietoturvalliset toimintatavat, joilla toimintamallin tietoturvavaatimukset täytetään. Yhteisöjen toimintamallit vaihtelevat tietenkin rajusti mutta äänestysjärjestelmän kannalta tietoturvavaatimukset on määritelty tietojärjestelmän määrittelydokumentaatiossa (Liite 1).

Tietoturvapolitiikassa lähdetään liikkeelle toiminnan perusasioista. Näitä voidaan listata tietoturvan perusteosten avulla, kuten esimerkiksi Mika Boströmin teoksen Kotimikron tietoturva pohjalta.

- Kenellä on ylläpitäjän oikeudet äänestysjärjestelmään tai sitä ylläpitäviin järjes-

telmiin ja tietääkö tämä henkilö vastuunsa ja velvollisuutensa tietoturvan kannalta?

- Onko käyttäjätunnukset kirjoitettu muistiin jonnekin? Jos on, niin mihin ja kenellä on pääsy tähän tietoon?
- Onko työpaikan tietokoneiden tietoturva kunnossa, niin ohjelmalliselta kuin fyysiseltä osalta? Miten tästä voi varmistua?
- Kenellä on pääsy työskentelytilaan jossa tietokoneet ovat?
- Kenellä on oikeus jakaa oikeuksia järjestelmään ja miten oikeuksien siirto tapahtuu?
- Tietävätkö yhteisön työntekijät salasanojen keksimisen ja uusimisen tietoturvalliset periaatteet?
- Kenellä on vastuu tietokoneiden tietoturvan ylläpidosta?
- Jääkö tietokoneet päälle yöksi toimistoon?
- Muistavatko kaikki käyttäjät varmasti kirjautua ulos?
- Miten toimitaan tietomurron sattuessa?

Kysymykset ovat osa yhteisön tietoturvan perusasioita. Jos yhdelläkin yhteisön tiloja tai tietokoneita käyttävälle henkilöllä on epäselvyyksiä yllä mainittujen peruskysymysten kanssa, on henkilöstö aluksi koulutettava tietokoneen käytön tietoturvan peruskysymyksissä ennen kuin äänestysjärjestelmää voidaan ottaa käyttöön. (Allen 2002, 397-399)

Kun perustietoturvaosaaminen yhteisössä on kunnossa, voidaan siirtyä äänestysjärjestelmän tietoturvan vaatimiin näkökohtiin. Kappaleessa 4.5 Yleiset toimintaympäristöt käsiteltyjen äänestysjärjestelmän teknisen toimintaympäristön erojen lisäksi on otettava huomioon äänestysjärjestelmän vaativan datan syöttämisen ja säilyttämisen tietoturva sekä ennen että jälkeen vaalien. Datan tietoturvaa pitää tarkastella aikajanan avulla.

- Mistä tieto äänestäjistä tulee? Jos se tulee jäsenrekisteristä, voidaanko sen antamiin listauksiin luottaa? Onko tiedot ajan tasalla ja onko jäsenrekisterin tietoturva kunnossa?

- Miten äänestäjän käyttäjätunnukset lähetetään hänelle? Jos äänestäjä soittaa ja kysyy tunnuksia, miten varmistutaan soittajan henkilöllisyydestä? Tietävätkö kaikki äänestysjärjestelmän ylläpitäjät tiedon kalastelun vaaroja?
- Miten vaalitulosta säilytetään ja missä formaatissa? Miten varmistetaan että mahdollisen äänien tarkistuslaskennan käytössä on sama data kuin ensimmäisellä laskukerralla?

Äänestysjärjestelmän datan syötön, luovutuksen ja säilytyksen käytännöt pitää olla selviä kaikille sen käyttäjille. Tähän käyttäjäkuntaan kuuluu mukaan myös itse äänestäjät. Onko äänestäjälle selvää ettei omia äänestystunnuksia saa luovuttaa eteenpäin? Jos joku kysyy tunnuksia äänestäjältä yhteisön nimissä, onko äänestäjää informoitu tunnistamaan tällainen tietoturvaa uhkaavaksi tiedon kalasteluksi? Kaikkiin näihin kysymyksiin on määriteltävä tietoturvan varmistamisen kannalta oikeat vastaukset ja jokaisen käyttäjäkunnasta tulee tietää nämä säännöt sekä toimia niiden mukaan.

Äänestysjärjestelmän käyttöönottoa edeltävä tietoturva-analyysin ja koulutuksen lisäksi on varmistettava, että järjestelmän tietoturvaa seurataan jatkuvasti lokien ja ohjelmistoista löytyvien tietoturva-aukkojen kannalta säännöllisesti, ja että tämän seurannan vastuuhenkilö on nimitetty ja tiedostaa vastuunsa. Käytössä oleva tekninen toimintaympäristö vaikuttaa tietenkin turvallisuustilanteen seurannan mahdollisuuksiin. Jos palvelimen käyttöjärjestelmä tai tietokantapalvelin ei ole omassa hallinnassa, sen tietoturvaa on käytännössä mahdoton itse seurata. On siis varmistuttava myös ulkoistetun järjestelmän ylläpitäjän tietoturvapolitiikasta. Lisäksi käytössä olevan tietoturvapolitiikan noudattamista pitää jatkuvasti valvoa ja politiikkaa pitää tarvittaessa päivittää uusien tietoturvauhkien löytymisen myötä. Yleisesti ottaen kaikissa äänestysjärjestelmän tietoturvaan liittyvissä osa-alueissa pitää olla nimetty vastuuhenkilö ja ylläpitäjä, on kyseessä sitten laitteisto, ohjelmisto, tietoturvapolitiikat tai käyttäjien koulutus. Ilman selkeää vastuunjakoa tietoturva ei voi toteutua. (Allen 2002, 231-264)

Ylläpitorakenne pitää huomioida myös itse äänestysjärjestelmän ohjelmiston kohdalla. Sen käytön ylläpitäjän lisäksi on oltava selkeä rooli myös itse ohjelmiston koodin ylläpidosta. Ohjelmistosta löytyvien tietoturva-aukkojen korjaamisen vastuu ja kustannusra-

kenne pitää olla selkeä. On huomioitava, ettei vapaan lähdekoodin vapaasti jaettavat ohjelmat ratkaise tätä ongelmaa. Vapaa lähdekoodi ei takaa koodin laatua. Lisäksi siitä löytyvän tietoturva-aukon korjaaminen vaatii asiantuntemusta, työtunteja ja huolellista testaamista. Jos ohjelmiston valmistaja kieltää käyttöehdoissa vastuunsa mihinkään ohjelmiston virheestä johtuvaan ongelmaan ja näin ilmaisee julkisesti ettei luota omaan ohjelmistoonsa, miten ohjelmiston käyttäjän pitäisi pystyä luottamaan siihen (Garfinkel ym. 2003, 818)?

Vaikka äänestysjärjestelmän jokaisen osan tietoturvan valvonnan vastuukenttä on selvillä ja kaikki käyttäjät tietävät vastuunsa järjestelmän tietoturvasta, pitää silti määritellä toimintatavat tietomurron varalle. Kaikilla äänestysjärjestelmän ylläpitäjillä pitää olla selkeä käsitys toimintamalleista tietomurron eri vaiheissa. (Allen 2002, 269-298)

- Miten tieto tietomurrosta kulkee yhteisön sisällä ja miten voidaan varmistua että se tavoittaa kaikki asianomaiset?
- Miten järjestelmä ajetaan hallitusti alas jotta tietomurto ei jatku?
- Miten tiedotetaan käyttäjille ja miten käy käynnissä olevien vaalien? Uusitaanko vaalit vai tuleeko äänestämiseen vain tauko?
- Miten tietomurron kulku voidaan selvittää ja mahdolliset aukot tietoturvassa paikata? Miten järjestelmän turvallisuudesta voidaan varmistua?
- Kenellä on tietotaito ja vastuu asentaa, konfiguroida ja ottaa järjestelmä uudelleen käyttöön?
- Miten vastaavat tietomurrot voidaan vastaisuudessa estää?

5. TESTAUS JA LAADUNVARMISTUS

WWW-äänestysjärjestelmän tietojärjestelmän osien toimivuudesta ja turvallisuudesta voidaan varmistua itse äänestysjärjestelmän ohjelmiston laatua lukuun ottamatta ottamalla huomioon osion 4 tietoturvanäkökohdat ja teettämällä järjestelmän konfigurointi ja ylläpito asiantuntijalla. Tämä on mahdollista koska muissa tietojärjestelmän osiossa käytetään valmiita, yleisesti käytettyjä ohjelmistoja (tai ainakin tulisi käyttää). Äänestysjärjestelmän ohjelmiston kohdalla tilanne on erilainen. Koska valmiita laajasti käytössä olevia ohjelmistoja ei ole, äänestysjärjestelmän tietoturvan ja toimivuuden varmistaminen pitää tehdä erityisen huolellisesti.

Tietoturvanäkökohtia äänestysjärjestelmän ohjelmiston tarkastamiseen toi kappale 4.4.12. Näiden tietoturvanäkökohtien tarkastaminen ohjelmistosta vaatii erilaisia lähestymistapoja kuin pelkkä asetusten ohjelmiston tarkastaminen. Se vaatii yleistä laadunvarmistusta.

5.1 Ohjelmiston laatu

Ohjelmisto laatu tarkoittaa että se vastaa täysin määrittelydokumentaation ja asiakkaan odotuksia. Tämä varmistaa että ohjelmisto toimii juuri niin kuin on tarkoitettu ja että se täyttää sen palvelutarpeen johon asiakas on ohjelmiston hankkinut. Ohjelmistolla tarkoitetaan myös ohjelmiston dokumentaatiota ja muita käyttöoppaita, joten myös niiden on oltava asiakkaan tarpeet täyttäviä. Äänestysjärjestelmän kohdalla ohjelmiston laadusta voidaan varmistua kun se täyttää määrittelydokumentaatiossa (Liite 1) määritellyt tarpeet. Määrittelydokumentaatio on tehty yhteistyössä ohjelmiston käyttäjien kanssa, joten siinä ilmenevät vaatimukset vastaavat asiakkaan ohjelmistolta odottamia vaatimuk-

sia. (Galin, D 2004, 24-25)

Ohjelmiston laatua vaarantaa virheet ohjelmistokoodissa. Tämä johtaa virheeseen ohjelmiston toiminnassa. Kun tämä virheellinen toiminto suoritetaan, syntyy virhe ohjelmiston suorituksessa eikä ohjelmisto enää täytä sille odotettuja toimintavaatimuksia. Virheet ohjelmakoodissa voivat johtua monesta eri syystä. Ohjelmiston määrittelydokumentaatio saattaa sisältää virheitä. Se ei välttämättä ota huomioon kaikkia eri käyttötarkoituksia, jolloin dokumentaation pohjalta tehty ohjelmakoodi on tietenkin myös virheellistä. Ohjelmoija saattaa myös ymmärtää väärin asiakkaan kuvailemat tarpeet. Ohjelmoija saattaa myös tahallisesti jättää osan toiminnallisuusvaatimuksista huomioimatta jos hänellä ei riitä taito niiden ohjelmoimiseen, tai jos ohjelmoimisen aikataulu on liian tiukka. Ohjelmoija voi myös tahtomattaan yksinkertaisesti ohjelmoida väärin, tehdä kirjoitusvirheitä, tai ohjelmoida vasten vaadittua ohjelmointityyliä, jolloin muiden on vaikea ylläpitää hänen kirjoittamaansa koodia. Ohjelmiston riittämätön testaaminen ennen käyttöä saattaa jättää ohjelmistoon virheitä ja huolimattomasti tehty testaus jättää myös virheet havaitsematta vaikka testausta olisikin tehty runsaasti. Ohjelmiston tekniseen dokumentaatioon tai käyttäjäoppaisiin jääneet virheet aiheuttavat virheitä ohjelmiston käyttöönotossa sekä käytössä. Nämä mainitut ongelmat luovat suuren uhan ohjelmiston laadulle. On siis käytettävä keinoja joilla voidaan varmistua ettei mainittuja virheitä tapahdu. Tällä tarkoitetaan laadunvarmistusta. (Galin 2004, 16-24)

5.2 Laadunvarmistus

Laadunvarmistuksella tarkoitetaan keinoja, joilla voidaan antaa tarpeellinen näyttö siitä, että koko tietojärjestelmän kehitys- ja ylläpitoprosessi tuottaa määrittelydokumentaatiossa määritellyt ominaisuudet ohjelmistoon. Myös itse projektin pysyminen aikataulussa ja budjetissa varmistaa projektin olevan kykenevä tuottamaan määrittelydokumentaatiossa vaaditun tuotteen. Näiden näkökohtien tarkoituksena on tuottaa tarpeeksi korkea luottamus siihen, että ohjelmisto vastaa odotuksia, että sen ylläpito onnistuu ja että

projekti pysyy aikataulussa ja budjetissa. (Galin 2004, 26-27)

Tärkein ohjelmiston laatuun vaikuttava tekijä on määrittelydokumentaatio, koska se määrittelee täysin ohjelmiston toiminnot. Vain määrittelydokumentaatiota vastaan pystytään arvioimaan ohjelmiston oikeellista toimivuutta ja koko tietojärjestelmäprojektin onnistumista. Jos määrittelydokumentaatio ei ole riittävän laaja tai siinä on virheitä, ohjelmisto sisältää automaattisesti virheitä asiakkaan näkökulmasta. Tärkeintä ohjelmiston laadunvarmistuksessa onkin määrittelydokumentaation laatu, joka rakentuu riittävästä laajuudesta ja virheettömyydestä. Tarkemmin näitä näkökohtia määrittää määrittelydokumentaation laadun osatekijät. (Galin 2004, 36-37)

5.2.1 Määrittelydokumentaation laadun osatekijät

Asiakkaan kannalta ohjelmistoon laatuun eniten vaikuttavia määrittelydokumentaation laadun osatekijöitä ovat oikeellisuus, luotettavuus, tehokkuus, eheys, käytettävyys, ylläpidettävyys, joustavuus, todistettavuus ja selviytyvyys. Näiden osa-alueiden vaatimukset on kirjattava määrittelydokumentaatioon, koska niiden kuitenkin oletetaan kuuluvan ohjelmiston ominaisuuksiin. Myöskään pelkät termit ”toimii ja on nopea” eivät riitä. Vaatimukset on oltava selkeitä ja mitattavia. (Galin 2004, 36-51)

Oikeellisuudella tarkoitetaan ohjelmiston esittämän tiedon oikeellisuutta, virhemarginaalia, reagointia tiedon puuttumiseen, tiedon ajankohtaisuutta ja saatavuutta. Äänestysjärjestelmän kohdalla tämä tarkoittaa esimerkiksi vaalin tulosten näyttämisen kannalta että ohjelmisto näyttää pyydetyt tiedot vaalin tuloksesta, tulosten virhemarginaali on nolla, ohjelma ilmoittaa jos ääniä on enemmän tai vähemmän kuin äänestäneitä äänioikeutettuja, näytetty tieto perustuu viimeisimpään äänestystulosdataan ja että tiedot on saatavilla alle kolmessa sekunnissa. Nämä ovat käytännössä itsestään selviä perusvaatimuksia mutta on tärkeää kirjata ne ylös dokumentaatioon. (Galin 2004, 38-39)

Luotettavuudella ja selviytyvyydellä tarkoitetaan toimimattomuuden suhdetta toiminta-aikaan, sitä kuinka kauan ohjelma saa olla toimimatta ja kuinka usein, ja sitä kuinka nopeasti ohjelma saadaan takaisin toimintaan. Tämä vaikuttaa suuresti ohjelman ylläpitokustannuksiin. Palvelinten ylläpidolle, päivityksille ja palvelinhuoneen varajärjestelmille on laitettava erityisiä prioriteetteja jos palvelun ei sallita olla missään tapauksessa saavuttamattomissa. Esimerkiksi palvelimen ohjelmistopäivitykset vaativat palvelun hetkittäisen alasajon. Äänestysjärjestelmän on oltava vaalien ajan toiminnassa mutta toisaalta viiden minuutin toimimattomuus ei välttämättä tuhoa vaaleja. (Galin 2004, 39-40)

Tehokkuudella tarkoitetaan järjestelmän resurssien käyttösuhdetta, sitä kuinka paljon ohjelma käyttää prosessoriaikaa ja muistia. Tällä on valtavasti merkitystä silloin kun palvelu joutuu palvelemaan suurta käyttäjämäärä. Tällöin pienetkin resurssien tuhlaukset nousevat eksponentiaalisiin mittakaavoihin. Äänestysjärjestelmän kohdalla tämä tarkoittaa palvelun saatavuutta. Vaikka vaaleja olisi testattu sadan henkilön testiryhmällä ja tällöin todettu kahden sekunnin vasteaika hyväksyttäväksi, tuhannen samanaikaisen äänestäjän suma voi muuttaa palvelun saatavuuden vasteajan kahteenkymmeneen sekuntiin. (Galin 2004, 40-41)

Eheydellä tarkoitetaan tiedon eheyttä, sitä että vain halutuilla tahoilla on pääsy muokkaamaan ohjelmiston dataa. Tietoturvaa ollaan käsitelty laajasti osiossa 4 mutta tärkeimpänä ominaisuutena voi tässä mainita, että jos äänestysjärjestelmän datan eheyteen ei voi luottaa, vaalien tulos menettää merkityksensä. (Galin 2004, 41)

Käytettävyydellä tarkoitetaan aikaa joka menee ohjelman käytön opetteluun. Äänestysjärjestelmän kohdalla voidaan esimerkiksi määritellä, että Internettiä vähän käyttäneeltä äänestäjältä ei saa mennä kauempaa kuin 5 minuuttia äänestyksen suorittamiseen ensimmäisellä järjestelmän käyttökerralla. Kaikki tämän ylimenevä aika tarkoittaa että järjestelmää on vaikea käyttää ja että äänestäjä luultavasti turhautuu koska ei ymmärrä miten äänestys suoritetaan. Myös ylläpitäjän kannalta ohjelman käytettävyyttä voidaan sel-

keästi arvioida. Vaalin luominen ja äänestäjien sekä ehdokkaiden syöttäminen ohjelmaan voi pahimmassa tapauksessa viedä viikkoja, parhaassa tapauksessa ehkä vain viisitoista minuuttia. Myös ohjelmiston käytön opetteluun menevä aika on tärkeä käytettävyysmittari myös ylläpitäjän toiminnoissa. (Galin 2004, 41)

Ylläpidettävyydellä tarkoitetaan työmäärä joka menee ohjelman virhetilanteessa virheen löytämiseen, sen korjaamiseen ja korjauksen varmistamiseen. Tähän vaikuttaa voimakkaasti ohjelmiston sisäinen rakenne, virheilmoitusten laatu ja dokumentaation laajuus. Hallitsematon koodisekamelska, joka tuottaa kryptisiä virheilmoituksia ja josta ei ole olemassa kunnon dokumentaatiota saattaa vaatia viikkoja pienenkin virheen löytämiseen, korjaamiseen ja testaamiseen. Modulaarinen ohjelmistorakenne yhdistettynä informatiivisiin virheilmoituksiin ja lokeihin auttaa virheiden löytämisessä ja korjaamisessa, eikä modulaarisuuden takia koko ohjelmistoa tarvitse testata uudelleen. (Galin 2004, 41-42)

Joustavuudella tarkoitetaan työmäärää joka menee uusien ominaisuuksien lisäämiseksi ohjelmistoon. Toimiva ja tehokaskin ohjelma saattaa olla vaikeasti laajennettavissa jos ohjelman sisäinen rakenne ei ole modulaarinen. Vaikka määrittelydokumentaatio olisi tehty kuinka huolella, on varmaa että laajennus- ja muutostarpeita ilmenee ohjelman käyttöiän aikana. Esimerkiksi toimintaympäristö tai lainsäädäntö saattaa muuttua yllättäen. Lisäksi laajennuksen saattaa hyvinkin tehdä eri taho kuin alkuperäisen ohjelman, jolloin ohjelmiston rakenteen selkeys ja luettavuus on elintärkeää. (Galin 2004, 42-43)

Todistettavuudella tarkoitetaan ohjelmistoon lähdekoodin ja dokumentaation selkeyttä ja rakennetta joka auttaa ohjelmiston laadun varmistamisessa. Modulaarinen ja selkeästi kirjoitettu lähdekoodi auttaa huomattavasti sen tarkistuksessa ja ylläpidossa, samoin dokumentaation rakenne ja ohjelman toiminnallisten vaatimusten selkeä ilmaisu. Ohjelmiston testaaminen ei voi onnistua täydellä teholla jos ohjelmiston koodi on sekavaa ja dokumentaatio kuin eri ohjelmistosta. (Galin 2004, 45)

5.3 Laadunvarmistuksen toteuttaminen

Kappaleessa 5.2 on määritelty tärkeimmiksi ohjelmistoon laatuun vaikuttaviksi tekijöiksi muun muassa ohjelmiston määrittelydokumentaation vastaavuus, laajuus ja oikeellisuus, projektin pysyminen aikataulussa ja budjetissa sekä ylläpidon suunnitelmallisuus. Ohjelmiston laadusta ei kuitenkaan voida varmistua vaikka kaikki vaaditut näkökohdat olisi otettu huomioon dokumentaatioissa ja projektisuunnitelmissa koska mikään ei kerro suoraan niitä noudatettu. Laadun varmistamiseksi onkin tehtävä konkreettisia tarkastustoimenpiteitä, jossa varmistetaan kohta kohdalta vaaditun laadun toteutuminen. Konkreettisina toimina voi olla määrittelydokumentaation ja lähdekoodin läpikäynnit, ohjelmiston testaus ja projektin etenemisen jakaminen virstanpylväisiin. (Galin 2004, 49)

5.3.1 Projektin hallinnon seuranta

Projektin hallinnon seurannalla tarkoitetaan laajaa kokonaisuutta projektin eri vaiheissa olevia mittareita. Tämä lähtee jo ennen projektin aloitusta tapahtuvasta suunnittelusta. Onko ohjelman toimittajan lupaama aikataulu ja budjetti realistinen suhteessa työmäärään ja käytettävään työvoimaan? Onko toimittajalla kokemusta projektien läpiviennistä? Onko toimittajan henkilöstö osaavaa ja toimiiko ryhmähenki? Onko toimittajan ja asiakkaan näkemys määrittelydokumentaation sisällöstä varmasti yhteneväinen? Nämä kaikki vaikuttavat voimakkaasti lopullisen ohjelman virheettömyyteen. Projektin aikana laatuun vaikuttaa voimakkaasti muun muassa toimittajan kehitystiimin sisäinen tiedonkulku, henkilökunnan koulutus, esimiestaidot, dokumentaatiokäytännöt, riskienhallinta, henkilöiden tuottavuuserojen huomiointi ja vastoinkäymisistä oppiminen. Nämä ovat voimakkaasti toimittajan sisäinen toiminnan mittareita mutta näistä voidaan varmistua

erilaisten laatustandardien avulla. (Galin 2004, 67-73)

Äänestysjärjestelmän käyttäjäryhmän kohdalla on huomattava että opiskelijakunnat tai yhdistykset pystyvät harvoin tilaamaan kokonaista ohjelmistoa joltain toimittajalta korkean hinnan takia. Ohjelmiston toimittaminen äänestysjärjestelmän vaatimilla laatukriteereillä tekee projektista erittäin kalliin. Erittäin todennäköistä on että äänestysjärjestelmä ostetaan valmiina ohjelmistona. Tällöin ohjelmiston rakentamisen aikaisista projektin laatunäkökohtia ei voi tietenkään enää valvoa. Tarvittavat tiedot projektin etenemisestä eivät välttämättä ole edes käytettävissä sillä toimittaja tuskin luovuttaa projektihallinollista historiatietoa toimittajan sisäisistä toiminnoista noin vain ulkopuoliselle. Tällöin laadunvarmistus pitää tehdä puhtaasti ohjelmistoa tutkimalla.

5.3.2 Ohjelmiston testaus

Yleisin laadunvarmistuksen muoto tietojärjestelmäprojekteissa on testaus. Testaus muodostuu dokumentaation ja lähdekoodin läpikäynneistä sekä ohjelmistotestauksesta. Läpikäynneissä määrittelydokumentaatiota ja lähdekoodia käydään ryhmässä läpi virheitä etsien. Näitä kutsutaan staattisiksi metodeiksi. Ohjelmistotestauksessa toimivalla ohjelmistolla ajatetaan testejä ja ohjelman antaman tuloksen oikeellisuutta arvioidaan. Näitä kutsutaan dynaamisiksi metodeiksi. Eri testausmetodeista tulisi tehdä dokumentaatiot, joista selviää testitapaukset ja testien tulokset. Vaikka ohjelmiston käyttäjä ei itse teekään testausta, hän voi dokumenttien avulla varmistua ohjelmiston laadusta. (Sommerville, I. 2004, 517)

Läpikäyntien kaksi metodia ovat tarkastukset ja vertaisläpikäynnit. Tarkastuksissa ohjelmiston määrittelydokumentaatiota käydään läpi vasten projektin etenemistä ja suhteessa toimittajan sisäiseen dokumentaatioon projektin etenemisestä. Tarkastukset tehdään esimiesvoimin ja ulkoisten konsulttien avustamana. Tarkastuksissa päätetään onko

projektin tietty osio valmis jotta voidaan siirtyä seuraavaan. Eri vaiheiden määrä vaihtelee tietenkin projektista toiseen, eli mitään tarkkaa kaavaa tarkastusten määrästä ei voi antaa. Tarkastustilanteessa päätetään joko pysyä nykyisessä vaiheessa tai siityä eteenpäin. Tarkastuksilla on valtava vaikutus ohjelmiston kokonaislaatuun, koska aikataulupaineiden alla jokin ohjelman osa saatetaan hyväksyä valmiiksi liian aikaisin. Tämä kostautuu pidentyneenä testausaikatauluna tai ohjelmistoon jäävinä virheinä. Tarkastuksesta tulee tehdä raportti, josta käy selville ilmenneet puutteet ohjelmistossa tai sen dokumentaatiossa sekä päätökset projektin eteenpäin viemisestä. Näiden raporttien avulla ohjelmiston tilaaja voi seurata ohjelmiston laatua ja toimittajan laatukriteereitä. Jos raporteissa ei näy raportoituja virheitä tai myöhästymisiä, voidaan toimittajan työtapojen todeta olevan laadukkaita ja laatuun pyrkiviä. Jos taas raportissa on merkintöjä virheistä mutta silti päätös jatkaa projektin seuraavaan vaiheeseen, voidaan koko projektin johdon laatupyrkimykset kyseenalaistaa. Tarkastusraporttien kokonainen puuttuminen kertoo tietenkin omaa synkkää kieltään toimittajan laadunvarmistuksesta. (Galin 2004, 150-157)

Vertaisläpikäynneissä ohjelmoijat käyvät dokumentaatio ja lähdekoodia läpi rivi riviltä ja etsivät virheitä. Hyväksi havaittu metodi on laittaa kaksi ohjelmoijaa tarkistamaan toistensa kirjoittamaa koodia samaan tilaan, jolloin keskustelua toiminnoista ja vaihtoehtoisista toimintatavoista voidaan käydä välittömästi. Läpikäyntejä voidaan tehdä myös ulkoisen asiantuntijan johdolla ja ottamalla mukaan loppukäyttäjä tilaavalta taholta. Myös näistä läpikäynneistä tulisi tehdä dokumentaatiot. Raportit läpikäynneistä tulisi olla huomattavasti tarkempia ja yksityiskohtaisempia kuin tarkastuksissa. Virheet tulisi kuvata tarkasti ja niille esittää ratkaisuvaihtoehtoja. Nämä raportit toimivat samanalaisena ikkunana toimittajan työskentelytapojen laatuun kuin tarkastustenkin raportit. Näistä voi myös seurata tietoturvallisuuden painoarvoa kehityksen aikana. Jos ohjelmasta ei ennen lopputestausta ole löydetty yhtään tietoturva-aukkoa, tarkoittaa se ettei niitä ole edes etsitty. Staattisen testauksen laatu riippuu myös hyvin paljon testaajien ammattitaidosta. Tietämätön ei tiedä mitä etsiä lähdekoodista. (Galin 2004, 158-170, Sommerville 2004, 538, Howard & LeBlanc 2003, 568)

Dynaamisessa testauksessa tutkitaan ohjelman toimintaa ja sen antamia tuloksia odotettuihin tuloksiin, jotka on johdettu määrittelydokumentaatiosta. Pääasiallisena tarkoituksen on löytää virheitä ohjelmasta. Tämä erottaa dynaamisen testauksen staattisesta. Staattisissa läpikäynneissä virheiden löytymättömyys voidaan tulkita laaduksi mutta dynaamisissa metodeissa se tarkoittaa testauksen epäonnistumista. Dynaaminen testaus pitää tehdä ohjelmointitiimin ulkopuolisen tahon tekemänä ja suunnitelmallisesti. Ohjelmoijien suorittaman satunnainen testaaminen ei ole dynaamista testaamista, koska testauksessa pitää ottaa huomioon testitapausten kattavuus. Lisäksi kenenkään ei pitäisi testata tekemäänsä koodia, sillä siitä ei varmasti halua löytää virheitä. Suunnitelmallisuudella tarkoitetaan lisäksi testi suorittamisen tapoja. Ohjelmisto pitää testata moduuli kerrallaan, ei koko ohjelmaa yhtenä kokonaisuutena, koska tällöin virheiden paikallistaminen on vaikeaa. Dynaamisessa testauksessa kaksi eri näkökantaa ohjelmiston testaukseen. Toiminnallisessa testauksessa tutkitaan pelkästään syötteiden ja tulosten suhdetta. Rakenteellisessa testauksessa yritetään saavuttaa mahdollisimman laaja lähdekoodin testausprosentti. (Galin 2004, 178-189, Sommerville 2004, 538)

Rakenteellisessa testauksessa (niin sanottu White Box Testing) yritetään saavuttaa mahdollisimman laaja lause- ja polkukattavuus. Tällöin jokainen ohjelman suoritusta muuttava ehtolause luetaan polun haarakohdaksi. Tällä metodilla syntyy sarja polkuja jotka kaikki on testattava läpi ehtokattavuuden toteutumiseksi. Lausekattavuudella yritetään varmistaa että jokaisen ohjelmiston koodilause tulee suoritettua. Rakenteellisen testauksen testitapaukset muodostetaan lähdekoodia lukemalla. Rakenteellisen testauksen pääasiallisena etuna on lausekattavuuden tuoma varmuus lähdekoodin virheettömyydestä. Ongelmana tässä lähestymistavassa on testitapausten valtava määrä. Esimerkiksi kymmenen peräkkäistä ehtolausetta, joista ohjelman suoritus voi jatkua kahta eri reittiä, luo jo 1024 kappaletta erilaisia suorituspolkuja. Laajassa ohjelmistossa saattaa olla satoja peräkkäisiä ehtolauseita, jolloin rakenteellinen testaus käy työmäärältään mahdottomaksi. (Galin 2004, 189-197, Sommerville 2004, 559-561)

Toiminnallisessa testauksessa (niin sanottu Black Box Testing) yritetään saavuttaa varmuus ohjelmiston tuottamasta tuloksesta suhteessa syötettyyn tietoon. Toiminnallisessa

testauksessa testitapaukset luodaan määrittelydokumentaation pohjalta, josta etsitään kaikki mahdolliset ohjelman syötteet ja odotetut tulokset. Testitapausten rajoittamiseksi syötteet jaetaan ekvivalenssiryhmiin, jolloin saman tuloksen tuottamat syötteet laitetaan samaksi testitapaukseksi. Ekvivalenssiryhmiksi on otettava mukaan myös epäkelvot syötteet. Äänestysjärjestelmän ääntenlaskun testauksen ekvivalenssiluokkia voivat olla esimerkiksi seuraavat tapaukset:

1. Ehdokas on saanut nolla ääntä
2. Ehdokas on saanut yhden äänen
3. Ehdokas on saanut kaikki äänet
4. Ehdokas on saanut enemmän ääniä kuin kaikki annetut äänet yhteensä
5. Kaikki ehdokkaat ovat saaneet saman määrän ääniä
6. Kaksi ehdokasta on saanut saman verran ääniä

Toiminnallisen testauksen hyvänä puolena on testitapausten vastaavuus määrittelydokumentaatioon. Testauksella saadaan suoraa todistetta siitä vastaako ohjelmiston toiminta määrittelydokumentaatiota. Huonona puolena on lausekattavuuden puuttuminen. Rakenteellisella testauksella ei voida mitenkään varmistua ohjelman sisäisen rakenteen ja algoritmien toimivuudesta. (Galin 2004, 197-201, Sommerville 2004, 544)

Ohjelmiston oikean toiminnan lisäksi on myös muistettava testata siitä muita laadun kriteereitä, kuten suorituskykyä, helppokäyttöisyyttä, luotettavuutta ja ylläpidettävyyttä. Testitapaukset laajenevat siis laajemmiksi, joissa esimerkiksi testataan ohjelmiston kykyä palvella määrittelydokumentaatiossa määriteltyä käyttäjämäärää samalla kun tarkkaillaan vasteaikaa ja resurssien käyttöä. Helppokäyttöisyyden testaus vaatii loppukäyttäjien käyttämistä testauksessa ja ylläpidettävyys konkreettista testiä reagoinnista virhetilanteisiin ja niistä selviämisestä. Osan dynaamisesta testauksesta pystyy nykyään automatisoimaan apuohjelmistoilla mutta moni muu testitapaus jää silti täysin manuaalisen työn varaan. Esimerkiksi käyttäjädokumentaation oikeellisuuden testaus vaatii ohjelmaa ensikertaa käyttäviä loppukäyttäjiä testihenkilöiksi, koska muuten testi ei voi onnistua. Manuaalinen testaus vaatii runsaasti sekä aikaa että resursseja, usein jopa 30 % projektin ajasta ja budjetista menee testaukseen. (Galin 2004, 179, 201-208)

Tietoturva on Daniel Galinin kirjassa Software Quality Assurance laitettu vain yhdeksi toiminnallisen testauksen osaksi mutta sen on oltava läsnä kaikissa laadunvarmistuksen näkökohdissa ja testaustapauksissa. Tietoturvallisuus pitää ottaa huomioon ohjelmiston modulaarisen rakenteen suunnittelusta lähtien. Tietoturva ei ole mikään ohjelmistoon jälkeenpäin liimattava omaisuus vaan tärkeä suunnittelunäkökohta. Käyttäjien tunnistus, datan eheys ja suojaus, järjestelmän kestävyys palvelunestohyökkäyksiä vastaan ja koko tietojärjestelmän kaikkien ohjelmistokomponenttien tietoturva on oltava ohjelmistoprojektin prioriteetteja. Samoin testauksessa tietoturvanäkökulmia pitää tutkia jo läpikäynneissä sekä tarkastuksissa. Tällöin voidaan tehokkaasti huomata tietoturvaa vaarantavia suunnitteluratkaisuja. Dynaamisessa testauksessa lähtökohtana on oltava järjestelmän murtaminen. Jokaista moduulin rajapintaa on yritettävä saada antamaan virheellinen reaktio. Tätä voidaan yrittää esimerkiksi syöttämällä epäkelpoa dataa, kuten NULL-arvoja ja kirjaimia ohjelman odottaessa numeroita. Tietoturvallinen testaus, niin staattinen kuin dynaaminenkin, vaatii testaajilta osaamista tietoturvanäkökohdista ja valitun teknisen käyttöympäristön vaaroista ja vahvuuksista. Tietoturvan huomioonottaminen ja sen testaus on siis oltava mukana kaikissa laadunvarmistuksen näkökohdissa ja sille on asetettava vaatimuksia määrittelydokumentaatiossa. Tärkeää on muistaa ettei tietoturvan testauksellakaan voida varmistua 100 % tietoturvallisuudesta, koska ohjelmiston testaus ei voi saavuttaa 100 % kattavuutta kuin hyvin pienien ohjelmien kohdalla. Testaajien kokemus, oikeat testimetodit ja työkalut sekä erilliset testiryhmät (esimerkiksi yksi jonka tarkoitus on vain murtautua ohjelmistoon ja raportoida siitä) parantavat tietoturvan testauksen laatua mutta eivät tee siitä 100 % varmaa. (Howard & LeBlanc 2003, 567-613, 615-626, Sommerville 2004, 583)

Kaikista staattisen sekä dynaamisen testauksen testitapauksista tulee olla olemassa dokumentaatiot. Ilman testien raportteja ohjelmiston laadusta tai toimivuudesta ei voi mitenkään varmistua. Tämä pitää ottaa avainkysymykseksi äänestysjärjestelmää hankkiessa, koska ohjelmiston käyttöehdoissa kuitenkin lukee ettei toimittaja ota mitään vastuuta tuotteen virheistä. Testiraporteista on käytävä ilmi testatun ohjelman versionumero, testidata, kattavuus ja tulokset. Äänestysjärjestelmän hankkijan ei tietenkään tarvitse itse

osata lukea ja tulkita raportteja vaan tähän kannatta hankkia riippumatonta ulkopuolista asiantuntija-apua. Raportit ovat hyödyttömiä ilman ohjelmiston määrittelydokumentaatiota joten myös siihen on oltava pääsy. Jos toimittaja ei salli pääsyä näihin dokumentteihin, kannattaa kyseinen toimittaja kiertää kaukaa äänestysjärjestelmää hankkiessa. Yhtä synkkää kieltä kertoo dokumentaation puuttuminen. Tällöin testaus pitää suorittaa itse ja palvelu tähän ostaa ulkopuolelta. (Galin 2004, 4, 228-231)

Staattisten ja dynaamisten testausmenetelmien vertailu tehokkuuden ja paremmuuden suhteen ei ole helppoa, sillä ne keskittyvät erilaisiin näkökohtiin testaamisessa. Staattisilla metodeilla voidaan löytää jopa 90 % ohjelmiston dokumentaation ja lähdekoodin virheistä. Ongelmana on ettei staattisilla metodeilla voi varmistua ohjelmiston toiminnasta, sillä vasta ohjelmiston ajaminen antaa varmuuden ohjelmiston toiminnasta. Dynaamisilla metodeilla voidaan varmistua ohjelmiston toiminnasta mutta työmäärä siihen on aivan liian valtava että varmistusta voitaisiin tehdä 100 % varmuudella. Lausekattavuuden hakeminen on laajuudessaan mahdotonta rakenteellisessa testauksessa. Toiminnallisessa testauksessa ei taas voida varmistua ettei ohjelmiston virhe tai virheiden yhdistelmä ole syynä saatuun tulokseen, vaikka se olisikin oikea. Parhaaksi testausmetodiksi onkin osoittautunut sekä staattisten että dynaamisten testaustapojen yhdistelmä. Tällöin voidaan todennäköisyyden periaatteella saada suurin osa ohjelmiston virheistä selville ja näin saada resurssien ja aikataulun rajoissa paras laatu aikaiseksi. Pelkkä testien suorittaminen ei tietenkään riitä sillä myös testauksen laadusta pitää varmistautua. Testaajat pitää olla asiantuntevia ja testaus suunnitelmallista. 100 % virheettömyyteen tuskin koskaan päästään mutta huonon ja hyvä testauksen eroilla on valtava vaikutus ohjelmiston laatuun. (Sommerville 2004, 518, 522)

5.3.3 Ylläpito

Ylläpito on tärkeä osa ohjelmiston käytön onnistumista. Vaikka ohjelmiston määrittelydokumentaatio olisi tarpeeksi laaja ja ohjelmiton toteutus ja asennus olisivat onnistu-

neet, käyttöympäristön muutokset ja uudet tietoturvauhat vaativat selkeän ylläpitosuunnitelman jotta ohjelmiston käyttö voi ylipäätään jatkua. Äänestysjärjestelmältä saatetaan vaatia uusia ääntenlaskutapoja tai teknisestä toteutusympäristöstä saattaa löytyä aiemmin tuntemattomia tietoturva-aukkoja, joka saattaa vaatia lähdekoodin korjaamista. Nämä kummatkin tapaukset vaativat määrittelydokumentaation päivittämistä, koodausta, testausta ja uuden version käyttöönottoa sekä käyttäjien koulutusta. Uusien ominaisuuksien kohdalla kustannusmalli on selkeä mutta tietoturva-aukkojen korjaamisen kustannuksista saattaa tulla erimielisyyksiä, ellei käytäntöjä ole sovittu ennalta. Ohjelmiston rakennusprojektin yhteydessä yleensä sovitaan myös ylläpidosta mutta jos ohjelmisto ostetaan pakettina, ylläpito on varmasti erillinen palvelu. Vapaan lähdekoodin ohjelmatkaan eivät tuo muutosta tähän faktaan. Vaikka koodin korjaamisen pystyisi ostamaan halvemmalla muulta asiantuntijalta kuin alkuperäiseltä toimittajalta, koodaaminen ja testaaminen vaatii silti työtunteja sekä resursseja. Tämä pitää ottaa huomioon äänestysjärjestelmän hankintaa suunniteltaessa, sillä ohjelmistosta tulee kustannuksia varmasti myös alkuperäisen hankinnan jälkeen.

Ylläpidettävyys on yksi ohjelmiston laadun komponentteja ja se rakentuu muustakin kuin pelkästään ylläpitosopimuksesta. Ohjelman rakenne ja suunnitteluratkaisut vaikuttavat ylläpidon onnistumiseen, samoin kuin dokumentaatioiden laatu ja testitapaukset. Modulaarinen rakenne ja selkeä koodi yhdistettynä hyvään dokumentaatioon ja valmiisiin testitapauksiin tekee ylläpidosta huomattavasti helpompaa. Laadukkaaseen ylläpitoon kuuluu myös järjestelmän jatkuva valvonta lokien avulla (käsitelty osiossa 4) ja käyttäjien koulutus. Käyttäjäkunnan vaihtuessa ohjelmiston tietoturvaominaisuuksien lisäksi käyttäjille on muistettava opettaa yleiset tietoturvapolitiikan käytännöt. Kokonaisuutena äänestysjärjestelmän ylläpito vaatii ohjelmiston toiminnan seurantaa, ongelmiin reagointia ohjelmiston koodia korjaamalla, uuden version käyttöönottoa ja käyttäjien koulutusta. (Galin 2004, 255-271)

6. JOHTOPÄÄTÖKSET

WWW-äänestysjärjestelmän käytön mahdollisuuksia yhdistyksissä ja opiskelijakunnissa lähdettiin tutkimaan näitä yhteisöjä koskevan lainsäädännön sekä vaalien yleisten vaatimusten näkökulmasta. Yleiset vaatimukset on listattu osiossa 2 mutta tärkeimpinä ovat vaalisalaisuuden säilyminen läpi vaaliprosessin sekä äänestysjärjestelmän antaman vaalituloksen luotettavuus. Vaalisalaisuuden säilymistä lähdettiin tarkastelemaan äänestysjärjestelmän tietojärjestelmärakenteen eri osien (Kuvio 2) turvallisuusarvioinnin kautta ja äänestysjärjestelmän luotettavuutta laadunvarmistuksen mahdollisuuksien kautta.

Lainsäädännön kannalta esteitä WWW-äänestysjärjestelmän käyttöön yhdistyksissä ja opiskelijakunnissa ei ole. Näissä yhteisöissä vaalien järjestämistä kontrolloin yhdistyslaki, joka antaa yhteisölle täysin vapaat kädet päättää vaalien järjestämistavasta. Myös ylioppilaskunnat saavat vapaasti itse päättää vaalitavastaan.

Osiossa 4 käsiteltyjen äänestysjärjestelmän eri tietojärjestelmärakenteen osien tietoturva-analyysi paljasti että tietomurto on mahdollinen jokaisen tietojärjestelmän osan kautta. Tietomuron kohdistuessa äänestäjän päätteeseen (äänestäjän WWW-selain, äänestäjän käyttöjärjestelmä, äänestäjän tietokone, äänestäjän lähiverkko) on äänestäjän vaalisalaisuus mahdollista murtaa. Tietomurron kohdistuessa äänestysjärjestelmän palvelinrakenteeseen ja sen lähiverkkoon vaarassa on vaalisalaisuuden lisäksi myös vaalin tulokset luotettavuus äänestysjärjestelmän tietokannan tiedon eheyden vaarantumisen kautta.

Palvelinpuolen tietoturvaa parantavat turvallinen palvelinhuone, luotettava Internet-yhteyden tarjoaja, turvallinen lähiverkko, käyttäjien oikeuksien tiukka rajaaminen sekä oikein konfiguroitu ja päivitetty palvelimen käyttöjärjestelmä, palvelinohjelmisto sekä palvelinlaajennukset. Äänestysjärjestelmäohjelmisto pitää olla tietoturvallisesti ohjel-

moitu sekä huolellisesti testattu. Lisäksi pitää huolehtia järjestelmän varmuuskopioista sekä asiantuntevasta yläpidosta, joka vaatii palvelinjärjestelmän kaikkien osien jatkuvaa seurantaa ja ylläpitoa, sekä kaikkien järjestelmän käyttäjien koulutuksessa yhteisön tietoturvapolitiikoihin. Nämä kohdat huomioon ottamalla äänestysjärjestelmän palvelinpuolen tietoturva on tarpeeksi luotettavalla järjestelmän käyttöön tasolla mutta ohjelmistoista löytyvä uusi tietoturva-aukko saattaa vaarantaa tämän turvallisuuden millä hetkellä tahansa. 100 % luotettavuutta äänestysjärjestelmän tietoturvaan on mahdoton saavuttaa suurillakaan rahallisilla investoinneilla tai osaavallakaan asiantuntija-avulla.

Äänestäjän käyttämän päätteen turvallisuudesta on vaalien järjestäjän kannalta mahdoton varmistua. Äänestäjän päätteen tietoturvaa ei pysty valvomaan etäältä, siihen ei voi asettaa teknisiä rajoituksia tai vaatimuksia eikä vaalin järjestäjä pääse selville mahdollisesta tietomurrosta mitenkään. Äänestäjän vaalisalaisuuden säilyminen on siis täysin äänestämiseen käytettävän Internet-päätteen ylläpitäjän tietoturvaosaamiseen käsissä. Tämä tietoturvauhan takia WWW-äänestämistä mistä tahansa Internet-päätteeltä ei voi suositella, koska se vaarantaa äänestäjän vaalisalaisuuden.

Äänestysjärjestelmän antaman tuloksen luotettavuus on kokonaisuudessaan kiinni ohjelmiston yleisestä laadusta, jota käsiteltiin osiossa 5. Äänestystuloksen luotettavuus lähtee ohjelmiston määrittelydokumentaation laadusta, joka koostuu virheettömyydestä ja kattavuudesta. Dokumentaatiossa on oltava listattuna kaikki tarpeet järjestelmän toiminnasta, tietoturvasta, tehokkuudesta ja ylläpidettävyydestä. Ohjelmiston vastaavuutta määrittelydokumentaatioon tutkittava testauksen ja läpikäyntien avulla, joista on oltava saatavilla täydelliset raportit. Laadun varmistumiseksi myös ohjelmiston ylläpito pitää olla suunniteltu, sillä muuten ensimmäinen paikkaamaton tietoturva-aukko tekee koko järjestelmä kelvottomaksi käyttöön. WWW-äänestysjärjestelmää ei tulisi ottaa käyttöön ilman kaikkia vaalien järjestäjän tarpeita täyttävää määrittelydokumentaatiota, varmistusta testausdokumentaation muodossa että ohjelmiston toiminta todella vastaa määrittelydokumentaatiota ja ilman toimintasuunnitelmaa ylläpitomallista. Äänestysjärjestelmän antaman vaalituloksen oikeellisuudesta ei voi varmistua ellei kaikki kolme edellä mainittua laadun taetta toteudu.

Tähän asti äänestysjärjestelmän käyttömahdollisuuksia on tarkasteltu vaalin järjestäjän näkökulmasta. Vaalisalaisuuden ja vaalituloksen luotettavuuden kannalta WWW-äänestysjärjestelmässä on perustavaa laatua olevia ongelmia äänestäjän kannalta, sillä äänestäjä ei voi mitenkään varmistua järjestelmän toiminnasta, vaikka äänestysjärjestelmän ohjelmistoa ja sen tietoturvaa olisi testattu erittäin huolellisesti. Äänestäjän on käytännössä vain toivottava että hänen äänensä tallentuu sellaisena kun hän äänesti ja että se otetaan huomioon ääntenlaskussa. Perinteisessä vaalitavassa ensimmäinen äänestäjä tarkistaa uurnan olevan tyhjä. Tätä ei pysty tekemään äänestäjän kannalta mitenkään luotettavasti sähköisissä äänestysjärjestelmissä. Uurnan turvallisuutta ja äänten laskua on lisäksi perinteisesti valvomassa eri puolueiden edustajia, opiskelijakunnan vaaleissa puolueettomia vaalivirkailijoita. Äänestäjä voi äänestyspaikalla fyysisesti nähdä nämä toimijat ja todeta uurnan olevan lukittu. Sähköisessä järjestelmässä vaalien turvallisuuteen voi pelkästään uskoa, sitä ei voi varmistaa. Kaikki tämä epävarmuus luotettavuudesta ja vaalisalaisuuden säilymisestä vähentää vaalien uskottavuutta äänestäjän silmissä. Tällöin WWW-äänestysjärjestelmän vaalien järjestäjälle tuoma tehokkuushyöty järjestämisessä ja saavutettavuuden tuoma hyöty äänestäjälle nollaantuvat äänestäjän alkaessa epäilemään vaalijärjestelmän toimivuutta. Henkilökohtaisesti äänestäjänä äänestän niin kauan perinteisillä äänestysmenetelmillä kuin se vain on mahdollista. Samoihin johtopäätöksiin sähköisen äänestysjärjestelmän turvallisuusuhista äänestäjän kannalta tuli tekniikan tohtori Antti Honkela Electronic Frontier Finland ry:n lausunnossa uudesta vaalilaista (OM 3/51/2005), joka mahdollistaa sähköisen äänestysjärjestelmän käytön valtiollisissa vaaleissa. Vaikka lausunnossa otetaan kantaa valtiollisiin vaaleihin, en näe syytä miksi yhdistyksissä, opiskelijakunnissa tai ylioppilaskunnissa tulisi ottaa demokratian uskottavuuden näkökohtaa yhtään vähemmän huomioon.

Tämän selvityksen tuomien näkökohtien perusteella en voi suositella WWW-äänestysjärjestelmää ensisijaiseksi äänestystavaksi opiskelijakunta SAMMAKKOn edustajiston vaaleissa, enkä näin ollen myöskään muiden opiskelijakuntien, yhdistysten tai ylioppilaskuntien vaaleissa. WWW-äänestysjärjestelmä voi olla tukemassa vaalien järjestämistä jos jollekin äänestäjäryhmälle on muuten erittäin vaikea järjestää äänestystilaisuutta mutta pääasiallisena äänestyskeinona suosittelen pidettäväksi perinteistä vaali-

tapaa vaaliuurnineen, äänestyslipukkeineen ja äänestyskoppeineen. Vaalien vaalisalaisuuden säilymisen ja vaalien tuloksen luotettavuuden uskottavuus äänestäjän näkökulmasta on niin tärkeä osa mitä tahansa järjestettävää vaalia ettei sitä pitäisi lähteä vaarantamaan vaalien järjestäjän resurssisäästöjen tai järjestämisen mukavuuden perusteella. Tämän selvityksen määrittelemien laatu- ja tietoturvavaatimusten täyttävän äänestysjärjestelmän hankinta ja ylläpito vie varmasti enemmän resursseja ja aikaa kuin perinteinen vaalitapa, kun toimintaympäristönä on opiskelijakunta, yhdistys tai ylioppilaskunta.

LÄHTEET

26.5.1989/503. Yhdistyslaki.

27.6.1997/645 Yliopistolaki

6.2.1998/116 Ylioppilaskunta-asetus

9.5.2003/351. Ammattikorkeakoululaki.

Allen, Julia H. 2002. Verkkotietoturvan hallinta – CERT. Edita Publishing Oy. ISBN: 951-826-588-7

Bostrom, M. 2003. Kotimikron tietoturva. Talentum Media Oy. ISBN: 951-762-813-7

Dormann, W & Rafail, J. 2007. Securing Your Web Browser [viitattu 19.3.2007]. CERT. Saatavissa: http://www.cert.org/archive/html/securing_browser.html

Galin, D. 2004. Software Quality Assurance. Pearon Education Limited. ISBN: 0201-70945-7

Garfinkel, S, Spafford, G & Schwartz, A. 2003. Practical Unix and Internet Security. Third Edition. O'Reilly Media, Inc. ISBN: 0-596-00323-4

Garfinkel, S. & Spafford, G. 2002. Web Security, Privacy, and Commerce. Second Edition. O'Reilly & Associates, Inc. ISBN: 0-596-00045-6

Hackworth, A. 2005. Spyware [viitattu 19.3.2007]. US-CERT. Saatavissa: http://www.us-cert.gov/reading_room/spyware.pdf

Honkela, A. 2006. Ehdotus hallituksen esitykseksi vaalilain muuttamisesta (sähköinen äänestys) 24.10.2005 (OM 3/51/2005). Electronic Frontier Finland ry [viitattu 22.4.2007]. Saatavissa: http://www.effi.org/julkaisut/lausunnot/om-vaalilaki.html

Howard, M & LeBlanc, D. 2003. Writing Secure Code. Second Edition. Microsoft Press. ISBN 0-7356-1722-8

Jerome Saltzer & M.D Schroeder. The Protection of Information in Computer System. Proceedings of the IEEE, syyskuu 1975.

Lamminen, J. SAMMAKKOn www-äänestys vaatimukset. [sähköpostiviesti]. Vastaanottaja: antti.kekki@gmail.com. Lähetetty: 14.03.2007 klo 10.19. [viitattu 17.4.2007]

Microsoft. 2007. Secunia Vulnerability Study [viitattu 25.3.2007]. Saatavissa: http://www.microsoft.com/windowsserver/facts/analyses/secunia.mspx

Milletary, J. 2005. Technical Trends in Phishing Attacks [viitattu 19.3.2007]. US-CERT. Saatavissa: http://www.us-cert.gov/reading_room/phishing_trends0511.pdf

MySQL AB. 2006. Market Share [viitattu 25.3.2007]. Saatavissa:

http://www.mysql.com/why-mysql/marketshare/

Netcraft. 2007. March 2007 Web Server Survey [viitattu 25.3.2007]. Saatavissa: http://news.netcraft.com/archives/2007/02/23/march_2007_web_server_survey.html

Ogletree, Terry. 2001. Inside Verkot. Oy Edita Ab. ISBN: 951-826-186-5

Pinheiro, E, Weber, W & Barroso, L. 2007. Failure Trends in a Large Disk Drive Population [viitattu 25.3.2007]. Saatavissa: http://labs.google.com/papers/disk_failures.pdf

RIPE NCC. 2007. Global Root Server System Stands Firm Against DDoS Attack [viitattu 23.3.2007]. Saatavissa: http://www.ripe.net/news/global-root-server.html

Satakunnan ammattikorkeakoulun opiskelijakunta – SAMMAKKO. 2005. Säännöt [viitattu 17.4.2007]. Saatavissa: http://www.sammakko.net/images/Saannot/opkusaannot.pdf

Secunia. 2007a. Vulnerability Report: Microsoft Internet Explorer 7.x [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/12366/?task=statistics_2007

Secunia. 2007b. Vulnerability Report: Microsoft Internet Explorer 6.x [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/11/?task=statistics_2007

Secunia. 2007c. Vulnerability Report: Mozilla Firefox 2.0.x [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/12434/?task=statistics_2007

Secunia. 2007d. Vulnerability Report: Safari 2.x [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/5289/?task=statistics_2007

Secunia. 2007e. Vulnerability Report: Microsoft Windows XP Home Edition [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/16/?task=statistics_2007

Secunia. 2007f. Vulnerability Report: Apple Macintosh OS X [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/96/?task=statistics_2007

Secunia. 2007g. Vulnerability Report: Ubuntu Linux 6.10 [viitattu 19.3.2007]. Saatavissa: http://secunia.com/product/12470/?task=statistics_2007

Secunia. 2007h. Vulnerability Report: PHP 4.4.x [viitattu 25.3.2007]. Saatavissa: http://secunia.com/product/5768/?task=statistics_2007

Secunia. 2006a. Vulnerability Report: Apache 1.3.x [viitattu 25.3.2007]. Saatavissa: http://secunia.com/product/72/?task=statistics_2006

Secunia. 2006b. Vulnerability Report: Microsoft Internet Information Services (IIS) 6 [viitattu 25.3.2007]. Saatavissa: http://secunia.com/product/1438/?task=statistics_2006

Secunia. 2006c. Vulnerability Report: Oracle Application Server 10g [viitattu 25.3.2007]. Saatavissa: http://secunia.com/product/3190/?task=statistics_2006

Secunia. 2006d. Vulnerability Report: MySQL 4.x [viitattu 25.3.2007]. Saatavissa: http://secunia.com/product/404/?task=statistics_2006

SecuriTeam. 2002. SQL Injection Walkthrough [viitattu 30.3.2007]. Sattavissa: http://www.securiteam.com/securityreviews/5DP0N1P76E.html

Silberschatz, A, Galvin, P & Gagne, G. 2003. Operating System Concepts. Sixth edition, John Wiley & Sons, Inc. ISBN 0-471-25060-0

Sitepoint. 2006. The State of Web Development 2006/2007 [viitattu 25.3.2007]. Saatavissa: http://sitepoint.com/report2006/claim/9c

Sommerville, I. 2004. Software Engineering. Seventh Edition. Pearson Education Limited. ISBN: 0-321-21026-3

Symantec. 2007. Symantec Internet Security Threat Report, Trends for July–December 06 Volume XI [viitattu 3.4.2007]. Saatavissa: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_keyfindings_03_2007.en-us.pdf

Tamminen, T. 2005. Sähköiset vaalit siirtyvät kahden vuoden päähän. Aviisi – Tampereen ylioppilaslehti (12).

Teknillisen Korkeakoulun Ylioppilaskunta. 2004. Vaalijärjestys [viitattu 17.4.2007]. Saatavissa: https://www.tky.fi/java/Index?oid=16489

Teknillisen Korkeakoulun Ylioppilaskunta, Helsingin kauppakorkeakoulun ylioppilaskunta. 2005. Puolet äänistä sähköisesti TKY:n ja KY:n edustajistovaaleissa – avoimena lähdekoodina julkaistava ohjelmisto ylioppilaskuntien yhteiskäytössä [viitattu 17.4.2007]. Saatavissa: https://www.tky.fi/java/Index?oid=152877

US-CERT. 2007a. Cyber Security Alerts [viitattu 19.3.2007]. Saatavissa: http://www.us-cert.gov/cas/alerts/

US-CERT. 2007b. Vulnerability Note VU#753924 [viitattu 19.3.2007]. Saatavissa: http://www.kb.cert.org/vuls/id/753924

US-CERT. 2006a. Vulnerability Note VU#722244 [viitattu 19.3.2007]. Saatavissa: http://www.kb.cert.org/vuls/id/722244

US-CERT. 2006b. Apple Releases Security Update to Address Multiple Vulnerabilities [viitattu 19.3.2007]. Saatavissa: http://www.us-cert.gov/cas/techalerts/TA06-333A.html

US-CERT. 2006c. Using Wireless Technology Securely [viitattu 23.3.2007]. Saatavissa: http://www.us-cert.gov/reading_room/Wireless-Security.pdf

US-CERT. 2003. Before You Connect a New Computer to the Internet [viitattu 19.3.2007]. Saatavissa: http://www.us-cert.gov/reading_room/before_you_plug_in.html

US-CERT. 2001. Denial of Service Attacks [viitattu 23.3.2007]. Saatavissa: http://www.cert.org/tech_tips/denial_of_service.html

US-CERT. 1999. CIH/Chernobyl Virus [viitattu 23.3.2007]. Saatavissa: http://www.cert.org/incident_notes/IN-99-03.html

US-CERT. 1997. Security of the Internet [viitattu 19.3.2007]. Saatavissa: http://www.us-cert.gov/reading_room/tocencyc.html

W3C. 2007. Browser Statistics [viitattu 19.3.2007]. Saatavissa: http://www.w3schools.com/browsers/browsers_stats.asp

Welling, L & Thomson, L. 2005. PHP and MySQL Web Development. Third Edition. SAMS Publishing. ISBN: 0-672-33672-8

Woody, C & Clinton, L. 2004. Common Sense Guide to Cyber Security for Small Businesses [viitattu 19.3.2007]. Internet Security Alliance. Saatavissa: http://www.us-cert.gov/reading_room/CSG-small-business.pdf

LIITELUETTELO

Liite 1 Äänestysjärjestelmän määrittelydokumentaatio

KUVIOT

Kuvio 1 Opiskelijakunnan vaalien prosessikuvaus. Lähde: https://www.proamk.fi/moodle/mod/resource/view.php?id=107

Kuvio 2 Äänestysjärjestelmän tietojärjestelmärakenne

WWW-äänestysjärjestelmän määrittelydokumentaatio

Antti Kekki

21.4.2007

Sisällysluettelo

1. Visio....4
1.1 Tarve....4
1.2 Ongelma....4
1.3 Ratkaisu....4
1.4 Uhat....5
1.5 Yhteensopivuus muihin toimintaympäristöihin....5
1.6 Ohjelmiston yleiskuvaus....5
2. Ohjelmiston toiminnot....6
2.1 Ylläpitäjä....6
2.1.1 Vaalien hallinta....6
2.1.2 Vaalin kysymysten hallinta....6
2.1.3 Äänioikeutettujen hallinta....6
2.1.4 Vaalien tuloksen laskeminen....7
2.1.5 Vaalin tulosten julkistaminen ja hallinta....7
2.2 Äänestäjä....8
2.2.1 Äänestäminen....8
2.2.2 Tuloksen katsominen....8
3. Käyttötapaukset....8
3.1 Vaalin ylläpitäminen....8
3.1.1 Perustoiminta....8
3.1.2 Vaihtoehtoinen toiminta....8
3.2 Vaalin kysymysten ylläpitäminen....9
3.2.1 Perustoiminta....9
3.2.2 Vaihtoehtoinen toiminta....9
3.3 Vaalin kysymysten vastausvaihtoehtojen ylläpitäminen....10
3.3.1 Perustoiminta....10
3.3.2 Vaihtoehtoinen toiminta....10
3.4 Äänioikeutettujen listojen ylläpitäminen....11
3.4.1 Perustoiminta....11
3.4.2 Vaihtoehtoinen toiminta....12
3.5 Äänioikeutettujen käyttäjätunnusten hallitseminen....13
3.5.1 Perustoiminta....13
3.5.2 Vaihtoehtoinen toiminta....13
3.6 Vaalin tuloksen hallinta....13
3.6.1 Perustoiminta....13
3.6.2 Vaihtoehtoinen toiminta....14
3.7 Äänestäminen....14
3.7.1 Perustoiminta....14
3.7.2 Vaihtoehtoinen toiminta....14
3.8 Kirjautuminen....15
3.8.1 Perustoiminta....15
3.8.2 Vaihtoehtoinen toiminta....15
3.9 Käyttötapauskaaviot....15

3.9.1 Ylläpitäjän käyttötapaukset....15
3.9.2 Äänestäjän käyttötapaukset....16
4. Järjestelmän sekvenssikaaviot....17
4.1 Äänestäminen....17
5. Tietokantamalli....18
6. Laatuvaatimukset....19
6.1 Oikeellisuus....19
6.2 Luotettavuus....20
6.3 Tehokkuus....20
6.4 Eheys....20
6.5 Ylläpidettävyys....20
6.6 Joustavuus....20
6.7 Todistettavuus....20
6.8 Käytettävyys....21
9. Suosituksia toteutukseen....21

1. Visio

1.1 Tarve

Opiskelijakunta SAMMAKKOn edustajiston vaalien järjestäminen Internetin välityksellä perinteisen vaalitavan sijaan tuo mukanaan etuja jotka hyödyttävät koko yhteisön toimintaa ja tulevaisuutta. Lippuäänestyksellä järjestetyissä vaaleissa äänestysprosentti on jäänyt usein alhaiseksi ja WWW-pohjaisen äänestysjärjestelmän käytön uskotaan parantavan osallistumista niin äänestykseen kuin koko yhteisön toimintaan.

1.2 Ongelma

Lippuäänestyksen järjestämisessä on monia ongelmia. Opiskelijakunnan pienien henkilöresurssien takia äänestystilaisuutta ei ole pystytty järjestämään kaikkialla samaan aikaan, vaan eri Satakunnan ammattikorkeakoulun toimipisteet on pitänyt porrastaa eri päiville, jotta vaalihenkilökunta ehtii kaikkialle. Tämä on luonut sekaannusta äänestäjien keskuudessa äänestysajasta. Äänestyspaikkojen aukiolo ei pysty noudattamaan optimaalista aikataulua kaikkien toimipisteen opiskelijaryhmien aikataulujen kanssa, vaan äänestys on voinut asua vapaapäiviin tai muihin ajanhetkiin, jolloin opiskelijat eivät pääse äänestämään. Lisäksi suurissa toimipisteissä äänestyspaikan näkyvyyttä ei välttämättä saada maksimoitua. Äänestyspaikka ei välttämättä rohkaise opiskelijakunnan toiminnasta tietämättömiä äänestämään, koska äänestyspaikalla on vaikea saada lisää tietoa toiminnasta. Tiedon jakaminen äänestyspaikoilla ei auta asiaan koska opiskelijoilla on päivän aikana tiukka aikataulu, eikä aikaa jää materiaalien lukemiseen.

1.3 Ratkaisu

WWW-pohjainen äänestysjärjestelmä ratkaisisi kaikki esitetyt ongelmat. Äänestys voi olla auki samanaikaisesti kaikille äänestäjille halutun ajanjakson verran, eli äänestäminen ei enää rajoitu yhteen päivään eikä koulupäivän pituuteen. Internetissä äänestyksen pystyy tekemään illalla tai viikonloppuna, tärkeimpänä valttina tämä antaa äänestäjälle mahdollisuus päättää, milloin hän haluaa äänestää. Tällöin opiskelijaryhmien aikataulueroot eivät vaikuta äänestysaktiivisuuteen. WWW-pohjainen äänestysjärjestelmä ei myöskään sido henkilöresursseja äänestyspaikalle vaalivirkailijoiksi, joten opiskelijakunnan toiminta voi jatkua normaalina vaalien aikanakin. Myöskään äänestyspaikan sijainti ei enää ratkaise vaalien näkyvyyttä tai saatavuutta. Äänestäjä myös pystyy tutustumaan ehdokkaiden taustamateriaaliin ja opiskelijakunnan esille laittamaan materiaaliin WWW-äänestyksessä. Äänestysprosentin noston lisäksi tämä materiaalin saatavuus parantaa myös yhteisön demokratiaa ja toimintaa, koska pelkän nimen sijaan äänestäjä saa paljon tietoa koko yhteisön toiminnasta ja ehdokkaanhaluamista teemoista. Äänestäjä voi hyvin lukea tunteja lähdemateriaalia ennen äänestyspäätöksen tekemistä. Tämä on paljon todennäköisempää

kuin että lippuäänestyksen yhteydessä lähtisi erikseen eri mediaa käyttäen tutkimaan ehdokkaan tai opiskelijakunnan WWW-sivuja.

1.4 Uhat

WWW-äänestyksen suurin uhka äänestysjärjestelmän tietoturvan murtuminen. Vaikka äänestystulosten tai äänestäjäluetteloiden manipulointi havaittaisiin ja vaalit uusittaisiin, luottamus vaalien järjestäjiin on tuhoutunut jopa vuosiksi. WWW-äänestysjärjestelmän tietoturva on oltava korkein prioriteetti järjestelmää rakennettaessa. WWW-äänestykseen liittyy myös äänestäjien ennakkoluulot Internetin käyttö kohtaan. Internetin käyttötaidoistaan epävarmat äänestäjät saattavat siksi jättää äänestämättä. Lisäksi perinteinen lippuäänestys on sosiaalinen tapahtuma, jossa äänestysvirkailija antaa opiskelijakunnalle kasvot ja muut äänestyspaikan äänestäjät luovat yhdessä vaikuttamisen henkeä. WWW-äänestys on sen sijaan täysin kasvoton ja epäsosiaalinen tapahtuma, joka ei välttämättä tunnu olevan suorassa yhteydessä yhteisön toimintaan. Äänestäjän on myös mahdoton mitenkään varmistua yksityisyydestään. Perinteisessä lippuäänestyksessä äänestäjä tietää ja voi tarkistaa, ettei hänen äänestyslippuaan voi erottaa muista tai myöhemmin yhdistää häneen. WWW-äänestyksessä äänestäjä ei voi varmistua tästä. Lähdekoodin ja määrittelydokumentaation julkinen saatavuus auttaa vain niistä jotain ymmärtäviä äänestäjiä, eikä äänestäjä voi silloinkaan varmistua, että äänestysjärjestelmän toiminta vastaa dokumentaatiota.

1.5 Yhteensopivuus muihin toimintaympäristöihin

Tämän määrittelydokumentaatio on tehty Satakunnan ammattikorkeakoulun opiskelijakunnan tarpeet huomioon ottaen ja sen toimintaa määrittävän lainsäädännön ehdoilla. Tämän johdosta määritys kelpaa myös muiden Suomen ammattikorkeakoulujen opiskelijakuntien äänestysjärjestelmien määrittelydokumentaatioksi. Ammattikorkeakoululainsäädännön mukaan opiskelijakunnan vaalien toimintatapoja määrää yhdistyslaki, joten tämä dokumentaatio on myös validi yhdistysten toimintaympäristöön. Vaikka yhdistyslaki on Suomen lainsäädäntöä, yhteisön vaalien toimintatavat noudattavat kaikkialla samoja periaatteita äänestäjän tunnistamisesta, annetun äänen anonymiteetistä ja vaalituloksen luotettavuudesta. Tämän ansiosta tätä dokumentaatiota voidaan käyttää äänestysjärjestelmän rakenteen pohjana tarkoitetun toimintaympäristön ulkopuolellakin.

1.6 Ohjelmiston yleiskuvaus

Ohjelmiston avulla on tarkoitus järjestää vaaleja WWW-ympäristössä. Vaalien järjestäjän kannalta tärkeitä ominaisuuksia ovat vaalien helppo ylläpito ja tietoturva. Ylläpidolla tarkoitetaan ehdokaslistojen ja äänestäjälistojen ylläpitoa sekä vaalien avaamista ja sulkemista. Koska äänestysjärjestelmä ei ole jäsenrekisteriohjelma, äänestäjälistoja pitää pystyä tuomaan äänestysjärjestelmään ulkopuolelta. Äänestäjien käyttäjätunnusten määrittelyyn ja äänestäjälle toimittamiseen pitää olla monia vaihtoehtoja. Tietoturvan kannalta järjestelmän tietoihin on oltava luku- ja

muokkausoikeus vain valituilla tahoilla ja järjestelmän antamaan vaalitulokseen on pystyttävä luottamaan. Ylläpitäjän kannalta äänestysjärjestelmän käytöstä on oltava saatavilla käyttöohjeet sekä tekninen dokumentaatio. Ohjelman käyttölisenssin on mahdollistettava lähdekoodin lukeminen tietoturvan varmistamiseksi.

Äänestäjän kannalta äänestysjärjestelmän vaatimuksena on helppokäyttöisyys ja järjestelmän tietoturvaan luottaminen. Äänestystapahtuma ei saa estyä liian vaikean käyttäjätunnusten saamisen tai kirjautumisen takia. Äänestystapahtuma on oltava selkeä ja äänestäjän on saatava selvä kuva siitä, mikä hänen äänestyspäätöksensä on. Äänestäjän on myös pystyttävä luottamaan järjestelmän anonymiteettiin ja luotettavuuteen.

2. Ohjelmiston toiminnot

2.1 Ylläpitäjä

2.1.1 Vaalien hallinta

Äänestysjärjestelmän ylläpitäjän oikeudet omaavan henkilön tulee ensiksi kirjautua järjestelmään. Vaalin luonnissa pitää antaa vaalin nimi, alkamispäivämäärä ja sulkeutumispäivämäärä.

2.1.2 Vaalin kysymysten hallinta

Kysymyksenä voi olla henkilön äänestäminen tai mielipiteen ilmaiseminen kysymykseen, esimerkiksi vaihtoehdoilla kyllä/ei tai a/b/c/d jne. Samassa vaalissa voi olla monta eri kysymystä. Henkilövaaleissa vaihtoehtoina on annettu ehdokaslista, kysymyksissä joko kyllä tai ei tai annettu lista muita vastauksia. Vain ylläpitäjän tunnuksilla voi muokata, lisätä tai poistaa kysymyksiä. Henkilövaaleissa pitää olla mahdollisuutena valita vaalitavaksi suora henkilövaali tai suhteellisena vaalina. Suhteellisessa vaalitavassa on saatava päättä yhdistyslain määrittelemän kolmen äänestystavan välillä. Kysymysten ja vastausvaihtoehtojen näkyvä järjestystä on pystyttävä hallitsemaan.

2.1.3 Äänioikeutettujen hallinta

Vain ylläpitäjän tunnuksilla voi hallita äänioikeutettujen listaa. Jokainen äänestäjä voi äänestää kaikissa niissä vaaleissa joihin hänen tunnuksilla on annettu äänioikeus. Vaalissa äänestäjällä on oikeus äänestää kaikissa kysymyksissä. Äänestäjistä pitää olla

tiedossa ainakin nimi, muut tiedot ovat ylläpitäjän päätettävissä. Jokaisella äänestäjällä on yksilölliset käyttäjätunnukset. Nämä voidaan luoda itse ohjelmassa poimimalla äänestäjän tiedoista tai luoda satunnaisesti ja tallentaa äänestäjän tietoihin. Listan äänioikeutetuista pitää pystyä tuomaan ohjelmaan järjestelmän ulkopuolelta ladattava tiedostona. Jos äänestäjän käyttäjätunnukset eivät ole äänestäjän tiedossa, äänestäjällä on oltava mahdollisuus tilata ne jotain tunnistetta vastaan ja tai pitää voida lähettää äänestäjän sähköpostiin. Äänestäjät kuuluvat aina johonkin äänioikeutettujen listaan, joita voi sitten kiinnittää vaaleihin.

2.1.4 Vaalien tuloksen laskeminen

Vaalin sulkeutumisen jälkeen tulos voidaan lasketaan automaattisesti. Äänestysliput pitää voida ladata järjestelmästä tiedostona, jotta ääntenlaskennan tulos voidaan varmistaa. Ääntenlaskutapoja ehdokasvaaleissa on kaksi: Suorassa vaalitavassa ääni menee suoraan ehdokkaalle. Suhteellisessa vaalissa on oltava valmiiksi kolme eri äänestystapaa (lainaus yhdistyslaista 26.5.1989/1503):

1) ehdokaslistoja käyttäen siten, että kukin ääni annetaan ehdokaslistalle kokonaisuudessaan, jolloin kullakin ehdokaslistalla ensimmäisenä oleva saa vertausluvukseen ehdokaslistan saaman koko äänimäärän, toisena oleva puolet äänimäärästä, kolmantena oleva yhden kolmasosan äänimäärästä ja niin edelleen ja valituiksi tulevat määräytyvät ehdokkaiden vertauslukujen mukaisessa järjestyksessä;

2) ehdokaslistoja käyttäen, mutta siten, että kukin ääni annetaan jollekin ehdokaslistassa olevalle ehdokkaalle, jolloin kullakin ehdokaslistalla ääniä eniten saanut saa vertausluvukseen ehdokaslistan saaman koko äänimäärän, toisena oleva puolet äänimäärästä, kolmantena oleva yhden kolmasosan äänimäärästä ja niin edelleen ja valituiksi tulevat määräytyvät ehdokkaiden vertauslukujen mukaisessa järjestyksessä;

3) ehdokaslistoja käyttämättä siten, että vaalissa jokainen annettu ääni jaetaan vaalilippuun merkittyjen ehdokkaiden kesken ensimmäisenä olevan ehdokkaan saadessa yhden äänen, toisena olevan puoli ääntä, kolmantena olevan yhden kolmasosan ääntä ja niin edelleen ja valituiksi tulevat määräytyvät ehdokkaiden saamien äänien mukaisessa järjestyksessä;

2.1.5 Vaalin tulosten julkistaminen ja hallinta

Ylläpitäjän tunnuksilla vaalituloksen pystyy julkistamaan ja piilottamaan. Vaalin tulos ei automaattisesti ole näkyvissä vaan se pitää erikseen julkistaa. Vaalituloksen piilottamisen jälkeen äänet jäävät talteen järjestelmään. Tulokset poistuvat vaalin poistamisen yhteydessä. Vaalituloksessa tulee näkyä äänet äänestäjittäin, kokonaistulokset ja muut tilastot (esim. äänestysprosentti) automaattisesti.

2.2 Äänestäjä

2.2.1 Äänestäminen

Äänestäjä kirjautuu äänestysjärjestelmään saamillaan tunnuksilla. Tunnukset voidaan lähettää sähköpostilla tai ne voi tilata sähköpostiinsa jollain tarkistustiedoilla. Samat tunnukset voivat toimia monissa eri vaaleissa. Hän pääsee äänestämään vain hänen tunnustensa käyttöoikeuksien sallimissa vaaleissa. Kun äänestäjä on äänestänyt jokaisen kysymyksen kohdalla, vaali sulkeutuu hänen kohdallaan. Jokaiseen kysymykseen pystyy äänestämään vain kerran, eikä äänestyspäätöstään pysty muuttamaan. Jos äänestäjä kirjautuu järjestelmään mutta ei äänestä, hän voi kirjautua uudestaan myös myöhemmin ja äänestää tällöin, kunhan vaali ei ole sulkeutunut. Kirjautumisilla ei ole lukumäärärajaa. Annettua ääntä ei saa pystyä yhdistämään äänestäjään.

2.2.2 Tuloksen katsominen

Äänestäjä näkee vaalin tuloksen kun se on julkaistu. Tulokseen tulee olla selkeä linkki vaalien sivuilla. -tuloksesta on näyttävä äänimäärät ja äänestysprosentti. Tulos on oltava näkyvillä vähintään 2 viikkoa äänestyksen loputtua.

3. Käyttötapaukset

3.1 Vaalin ylläpitäminen

Toimija: Ylläpitäjä

3.1.1 Perustoiminta

1. Ylläpitäjä luo uuden vaalin painamalla ”Luo uusi vaali” -painiketta
2. Ylläpitäjä syöttää vaalin nimen, aukeutumispäivämäärän ja sulkeutumispäivämäärän
3. Ylläpitäjä tallentaa uuden vaalin painamalla ”Tallenna”-painiketta
4. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.1.2 Vaihtoehtoinen toiminta

1a. Luodun vaalin muokkaaminen:

1. Ylläpitäjä painaa olemassa olevan vaalin kohdalla ”Muokkaa vaalia” -painiketta

2. Ylläpitäjä muuttaa vaalin nimeä, alkamispäivämäärää tai sulkeutumispäivämäärää
3. Ylläpitäjä tallentaa muutokset vaaliin painamalla ”Tallenna”-painiketta

1b. Luodun vaalin poistaminen:

1. Ylläpitäjä painaa olemassa olevan vaalin kohdalla ”Poista vaali” -painiketta
2. Järjestelmää pyytää vahvistusta poistoon ”Haluatko varmasti poistaa vaalin? Samalla poistuu tallennetut kysymykset, vastausvaihtoehdot ja annetut äänet!”
3. Ylläpitäjä painaa ”Kyllä, haluan poista vaalin”

2a. Ylläpitäjä ei syötä kaikki vaadittuja tietoja tai päivämäärä on virheellinen:

1. Järjestelmä pyytää puuttuvia tietoa eikä hyväksy tallentamista ennen kuin kaikki tiedot ovat kelvollisia.

3.2 Vaalin kysymysten ylläpitäminen

Toimija: Ylläpitäjä

3.2.1 Perustoiminta

1. Ylläpitäjä luo uuden vaalin painamalla ”Luo uusi kysymys vaaliin” -painiketta
2. Ylläpitäjä valitsee vaalin johon kysymys lisätään
3. Ylläpitäjä syöttää kysymyksen tekstin
4. Ylläpitäjä tallentaa kysymyksen painamalla ”Tallenna”-painiketta
5. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.2.2 Vaihtoehtoinen toiminta

3a. Luodun kysymyksen muokkaaminen:

1. Ylläpitäjä muokkaa olemassa olevaa kysymystä painamalla ”Muokkaa vaalin kysymyksiä” -painiketta
2. Ylläpitäjä valitsee vaalin jonka kysymystä haluaa muokata
3. Ylläpitäjä muokkaa kysymyksen tekstiä
4. Ylläpitäjä tallentaa muutokset painamalla ”Tallenna” -painiketta

3b. Luodun kysymyksen poistaminen:

1. Ylläpitäjä poistaa olemassa olevan kysymyksen painamalla ”Poista vaalin kysymyksiä” -painiketta
2. Ylläpitäjä valitsee vaalin jonka kysymyksen haluaa poistaa
3. Ylläpitäjä painaa kysymyksen kohdalla ”Poista” -painiketta

3c. Kysymysten näkyvän järjestyksen muuttaminen:

1. Ylläpitäjä painaa ”Näytä vaalien kysymykset” -painiketta
2. Ylläpitäjä valitsee vaalin jonka kysymykset hän haluaa listata
3. Ylläpitäjä painaa kysymyksen kohdalla ylöspäin osoittavaa nuolipainiketta siirtääkseen kysymystä ylemmäksi listassa tai alaspäin osoittavaa nuolipainiketta siirtääkseen kysymystä alemmaksi listassa

3.3 Vaalin kysymysten vastausvaihtoehtojen ylläpitäminen

Toimija: Ylläpitäjä

3.3.1 Perustoiminta

1. Ylläpitäjä painaa ”Lisää vastausvaihtoehto kysymykseen” -painiketta
2. Ylläpitäjä valitsee vaalin ja vaalin kysymyksen johon haluaa vastausvaihtoehdon lisätä
3. Ylläpitäjä syöttää vastausvaihtoehdon tekstin tekstikenttään.
4. Ylläpitäjä tallentaa vastauksen painamalla ”Tallenna”-painiketta
5. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.3.2 Vaihtoehtoinen toiminta

1a. Vastausvaihtoehdon muokkaaminen:

1. Ylläpitäjä painaa ”Muokkaa vastausvaihtoehtoa” -painiketta
2. Ylläpitäjä valitsee vaalin, kysymyksen ja vastausvaihtoehdon jota haluaa muokata
3. Ylläpitäjä muokkaa vastausvaihtoehdon tekstikentän sisältöä
4. Ylläpitäjä tallentaa muutokset painamalla ”Tallenna” -painiketta
5. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

1b. Vastausvaihtoehdon poistaminen:

1. Ylläpitäjä painaa ”Poista vastausvaihtoehto” -painiketta
2. Ylläpitäjä valitsee vaalin, kysymyksen ja vastausvaihtoehdon jonka haluaa poistaa
3. Ylläpitäjä painaa ”Poista” -painiketta
4. Järjestelmä kysyy vahvistusta poistoon, johon ylläpitäjä vastaa ”Kyllä, haluan poistaa vastausvaihtoehdon”
5. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

1c. Vastausvaihtoehdon näkyvän järjestyksen muuttaminen:

1. Ylläpitäjä painaa ”Näytä vaalien kysymysten vastausvaihtoehdot” -painiketta
2. Ylläpitäjä valitsee vaalin ja kysymyksen jonka vastausvaihtoehdot hän haluaa listata
3. Ylläpitäjä painaa vastausvaihtoehdon kohdalla ylöspäin osoittavaa nuolipainiketta siirtääkseen vastausvaihtoehtoa ylemmäksi listassa tai alaspäin osoittavaa nuolipainiketta siirtääkseen vastausvaihtoehtoa alemmaksi listassa

3.4 Äänioikeutettujen listojen ylläpitäminen

Toimija: Ylläpitäjä

3.4.1 Perustoiminta

1. Ylläpitäjä painaa ”Hallitse äänioikeutettujen listoja” -painiketta
2. Ylläpitäjä luo uuden äänioikeutettujen listan panamalla ”Luo uusi lista” -painiketta
3. Ylläpitäjä valitsee vaalin johon äänestäjien lista kiinnitetään
4. Ylläpitäjä painaa ”Tuo lista tiedostosta” -painiketta
5. Ylläpitäjä valitsee Excel-tiedoston koneen kiintolevyltä, jossa on lista äänioikeutetuista. Sarakkeet tulee olla järjestyksessä etunimi, sukunimi, sähköpostiosoite, käyttäjätunnus, salasana. Jos sarakkeita on vähemmän, puuttuviin luodaan automaattisesti satunnaista dataa.
6. Ylläpitäjä painaa ”Lataa lista palvelimelle” -painiketta
7. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.4.2 Vaihtoehtoinen toiminta

3a. Olemassa olevan listan muokkaaminen:

1. Ylläpitäjä painaa ”Muokkaa listaa” -painiketta
2. Ylläpitäjä valitsee vaalin, jonka äänestäjälistaa haluaa muokata
3. Ylläpitäjä lisää, poistaa tai muokkaa äänestäjätietoja tai muuttaa vaalia, johon lista on kiinnitetty
4. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3b. Äänestäjien poistaminen listalta:

1. Ylläpitäjä valitsee listalta äänestäjän tai äänestäjiä
2. Ylläpitäjä painaa ”Poista”-painiketta
3. Järjestelmä pyytää vahvistamaan poiston. Ylläpitäjä painaa ”Kyllä, haluan poistaa äänestäjän” -painiketta
4. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3c. Äänestäjän tietojen muokkaaminen:

1. Ylläpitäjä valitsee listalta äänestäjän
2. Ylläpitäjä painaa ”Muokkaa tietoja” -painiketta
3. Ylläpitäjä muokkaa äänestäjän tietoja
4. Ylläpitäjä painaa ”Tallenna muutokset” -painiketta
5. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

4a. Äänestäjien syöttäminen käsin:

1. Ylläpitäjä painaa ”Luo uusi äänestäjä” -painiketta
2. Ylläpitäjä syöttää äänestäjän etunimen, sukunimen, käyttäjätunnuksen ja salasanan

   2a. Ylläpitäjän syöttämät tiedot on epäkelpoja tai tietoja puuttuu:

   1. Järjestelmä ilmoittaa tietojen puuttumisesta
   2. Yläpitäjä korjaa puuttuvat ja virheelliset tiedot
3. Ylläpitäjä painaa ”Tallenna” -painiketta
4. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

4b. Äänestäjien tuominen toiselta listalta:

1. Ylläpitäjä painaa ”Tuo äänestäjiä toiselta listalta” -painiketta
2. Ylläpitäjä valitsee olemassa olevan vaalin äänestäjälistan, jonka äänestäjät liitetään myös tähän listaan
3. Ylläpitäjä painaa ”Hae äänestäjät” -painiketta
4. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.5 Äänioikeutettujen käyttäjätunnusten hallitseminen

Toimija: Ylläpitäjä

3.5.1 Perustoiminta

1. Ylläpitäjä painaa ”Hallitse äänioikeutettujen listoja” -painiketta
2. Ylläpitäjä valitsee vaalin, jonka äänestäjälistan haluaa nähdä
3. Ylläpitäjä painaa ”Luo äänestäjille tunnukset” -painiketta. Järjestelmä luo satunnaiset käyttäjätunnukset ja salasanat
4. Ylläpitäjä painaa ”Lähetä käyttäjätunnukset” -painiketta, joka lähettää tunnukset äänestäjän sähköpostiosoitteeseen
5. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.5.2 Vaihtoehtoinen toiminta

3a. Tunnuksia ei generoida:

1. Ylläpitäjä ei luo tunnuksia vaan pelkästään lähettää ne sähköpostiosoitteisiin
2. Ylläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.6 Vaalin tuloksen hallinta

Toimija: Ylläpitäjä

3.6.1 Perustoiminta

1. Ylläpitäjä valitsee ”Muokkaa vaalia” -painiketta
2. Ylläpitäjä painaa ”Julkaise vaalin tulos” -painiketta
3. Yläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.6.2 Vaihtoehtoinen toiminta

2a. Vaalin tulosta ei pysty julkaisemaan:

1. Ylläpitäjä painaa ”Julkaise vaalin tulos” -painiketta
2. Järjestelmä ilmoittaa, että vaali on yhä kesken eikä tulosta siksi voi vielä julkaista

2b. Vaalin tuloksen piilottaminen:

1. Ylläpitäjä painaa ”Piilota vaalin tulos” -painiketta
2. Yläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

2c. Vaalin äänien lataaminen:

1. Ylläpitäjä painaa ”Lataa vaalin äänet” -painiketta
2. Ylläpitäjä tallentaa Excel-tiedoston tietokoneelle
3. Yläpitäjä kirjautuu ulos ohjelmasta painamalla ”Kirjaudu ulos” -painiketta

3.7 Äänestäminen

Toimija: Äänestäjä

3.7.1 Perustoiminta

1. Äänestäjä valitsee vaalin jossa haluaa äänestää
2. Äänestäjä kirjautuu järjestelmään tunnuksillaan
3. Äänestäjä valitsee kysymyksen jossa haluaa äänestää ja hän voi äänestää
4. Äänestäjä painaa halutun äänestysvaihtoehdon kohdalla ”Äänestä” -painiketta
5. Äänestäjä kirjautuu ulos järjestelmästä painamalla ”Lopeta äänestys” -painiketta

3.7.2 Vaihtoehtoinen toiminta

2a. Annetut tunnukset eivät ole äänestäjän tunnukset:

1. Järjestelmä ilmoittaa virheellisistä tunnuksista ja pyytää syöttämään tunnukset uudelleen. Ennen oikeiden tunnusten syöttämistä ohjelman suoritus ei etene.

2b. Äänestäjä on jo äänestänyt tässä vaalissa kaikissa kysymyksissä:

1. Järjestelmä ilmoittaa ettei äänestäjä voi enää äänestää tässä vaalissa.

3.8 Kirjautuminen

Toimija: Äänestäjä, ylläpitäjä

3.8.1 Perustoiminta

1. Käyttäjä syöttää käyttäjätunnuksen ja salasanan
2. Ohjelman suoritus jatkuu

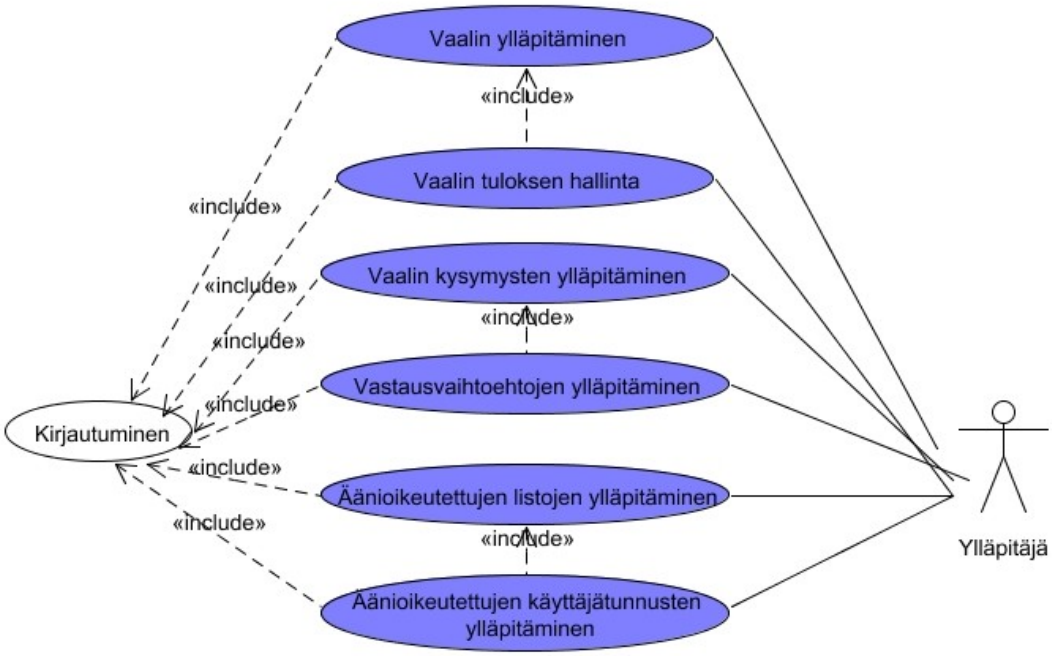
3.8.2 Vaihtoehtoinen toiminta

1a. Annetut tunnukset eivät ole äänestäjän tunnukset:

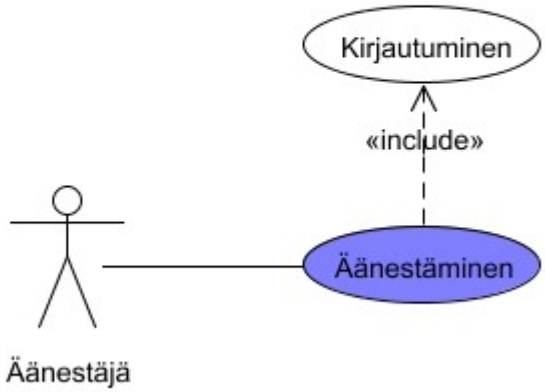
1. Järjestelmä ilmoittaa virheellisistä tunnuksista ja pyytää syöttämään tunnukset uudelleen. Ennen oikeiden tunnusten syöttämistä ohjelman suoritus ei etene.

3.9 Käyttötapauskaaviot

3.9.1 Ylläpitäjän käyttötapaukset

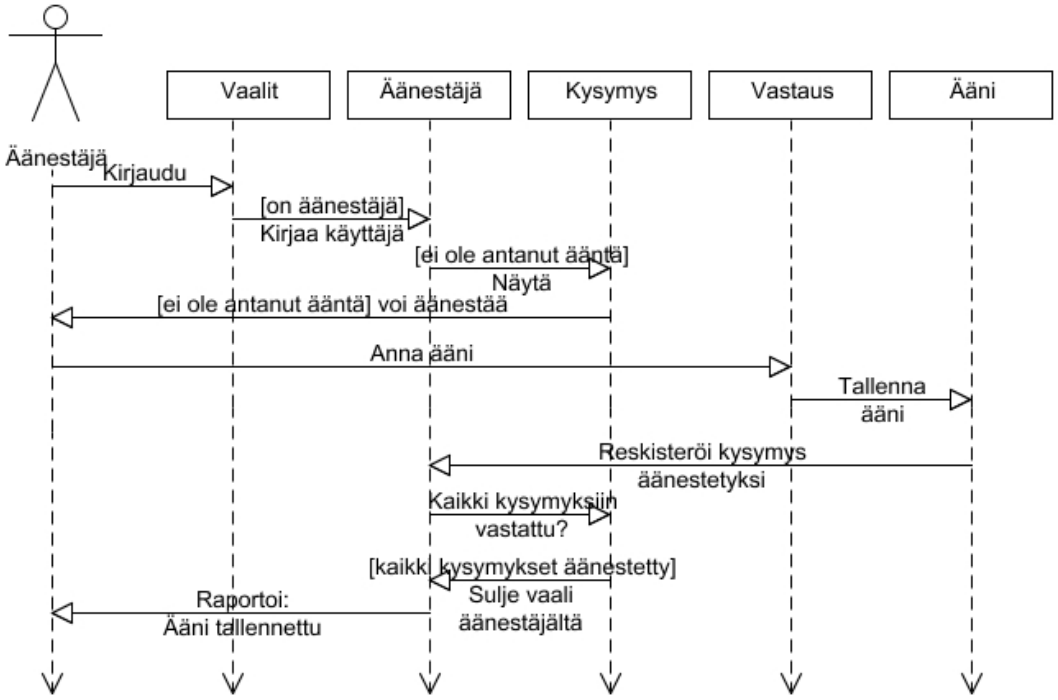


3.9.2 Äänestäjän käyttötapaukset

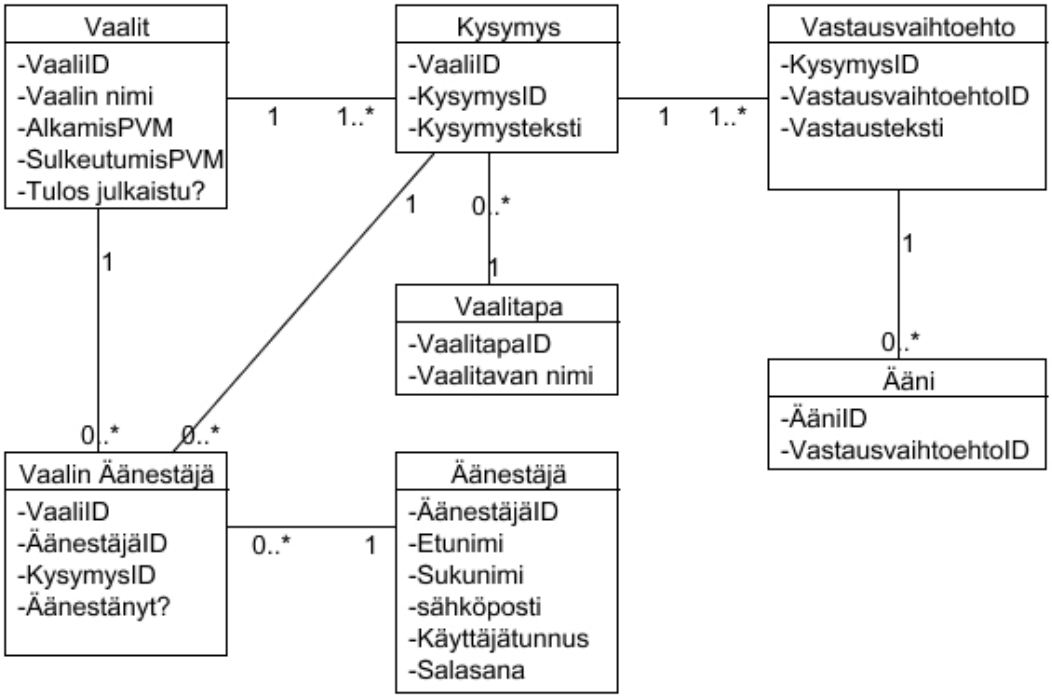

Kirjautuminen
«include»
Äänestäminen
Äänestäjä

4. Järjestelmän sekvenssikaaviot

4.1 Äänestäminen



5. Tietokantamalli



Kenttä	**Selite**
VaaliID	Vaalin yksilöllinen numero, kokonaisluku
Vaalin nimi	Vaalin nimi, esim. ”Edustajistovaalit 2007”
AlkamisPVM	Vaalin aukeutumispäivämäärä, esim. 12.11.2006
SulkeutumisPVM	Vaalin sulkeutumispäivämäärä, esim. 1.1.2007
Tulos julkaistu?	Onko vaalin tulos julkaistu? Joko kyllä tai ei
ÄänestäjäID	Äänestäjän yksilöllinen numero, kokonaisluku
Etunimi	Äänestäjän etunimi
Sukunimi	Äänestäjän sukunimi
Sähköposti	Äänestäjän sähköpostiosoite
Käytäjätunnus	Äänestämisen kirjautumiseen käytettävä käyttäjätunnus
Salasana	Äänestämisen kirjautumiseen käytettävä

	salasana
Äänestänyt?	Onko äänestäjä äänestänyt tässä vaalissa?
KysymysID	Vaalikysymyksen yksilöllinen numero, kokonaisluku
Kysymysteksti	Vaalinkysymyksen teksti, esim. ”Valitse henkilö jota haluat äänestää edustajistoon vuodelle 2007”
VaalitapaID	Vaalitavan yksilöllinen numero, kokonaisluku
Vaalitavan nimi	Vaalitavan nimi, esim. ”suhteellinen vaalitapa, listavaali vertausluvulla”
VastausvaihtoehtoID	Vastausvaihtoehdon yksilöllinen numero, kokonaisluku
Vastausteksti	Vastausvaihtoehdon yksilöllinen nimi, esim. ”kyllä, mielestäni jäsenmaksua on laskettava” tai ”Erkki Ehdokas, ehdokasnumero 8”. Vastaustekstikenttä on HTML-kenttä johon voi lisätä mm. kuvalinkkejä ja taulukoita.
ÄäniID	Äänen yksilöllinen numero, kokonaisluku

6. Laatuvaatimukset

6.1 Oikeellisuus

Sallittu virhemarginaali kaikissa laskutoimituksissa on nolla. Järjestelmän on pystyttävä havaitsemaan lähdetiedon virheellisyys seuraavissa tapauksissa:

1. Annettuja ääniä on jollain kysymyksellä enemmän kuin äänioikeutettuja kyseisessä vaalissa
2. Äänestäjän äänestänyt kysymystä jota ei ole olemassa
3. Ääni on rekisteröity vastausvaihtoehdolle jota ei ole olemassa

6.2 Luotettavuus

Ohjelmisto on satava toimintakuntoon vähintään seuraavana työpäivänä toimintakatkoksessa. Ohjelmisto on oltava ylläpitäjän asennettavissa.

6.3 Tehokkuus

Ohjelman vasteajan on oltava maksimissaan 2 sekuntia äänestäjälle näkyvissä toiminnoissa. Ylläpitäjän toiminnoissa vasteaika saa olla maksimissaan 4 sekuntia. Ohjelman suorituskyvyn on pysyttävä näissä rajoissa vaikka koko äänioikeutettujen joukko äänestäisi samalla ajanhetkellä.

6.4 Eheys

Vain ylläpitäjällä on pääsy muokkaamaan vaalien tietoja ja listoja äänioikeutetuista, sekä julkistamaan äänestystuloksen. Äänestäjillä on pääsy vain äänestykseen ja oikeudet äänen antamiseen. Muilla käyttäjillä ei ole mitään oikeuksia järjestelmään. Tiedon yksityisyyden kannalta kaikki tietoliikenne järjestelmän ja äänestäjän välillä tulee salakirjoittaa tehokkaasti.

6.5 Ylläpidettävyys

Ohjelmiston lähdekoodi tulee olla hyvien ohjelmointitapojen mukaan sisennettyä ja kommentoitua. Muuttujien ja funktioiden nimet tulee olla loogisia. Ohjelmiston toiminnasta, tietokannan tauluista ja oliomallista tulee olla täydellinen ja ajantasainen dokumentaatio. Ohjelmiston asennukseen tulee olla selkeät ohjeet.

6.6 Joustavuus

Ohjelman suunnittelussa on otettava huomioon laajennusmahdollisuudet uusien vaalitapojen lisäämiseksi sekä äänestäjätietojen säilyttämiseen ja tarkistamiseen ulkoisesta järjestelmästä.

6.7 Todistettavuus

Ohjelman rakenne tulee tukea tehokkaan ja kattavan testauksen mahdollisuutta. Lähdekoodin selkeys ja ajantasainen dokumentaatio on vaatimus staattisten tarkistusten onnistumiseksi. Dynaamisen testauksen onnistumiseksi ohjelman kaikki rajapinnat on oltava hyvin dokumentoitu.

6.8 Käytettävyys

Ohjelmistosta on oltava käyttäjille kolmen tason dokumentaatiota; käyttöopas äänestäjälle, laaja käyttöopas ylläpitäjälle vaali- ja äänestäjätietojen hallinnasta sekä asennusopas järjestelmän ylläpitoa varten. Käytettävyysvaatimuksena äänestäjän toiminnoille on että vähän Internettiä käyttänyt henkilö pystyy hoitamaan koko äänestysprosessin alle viidessä minuutissa. Ylläpitäjän toiminnoille käytettävyysvaatimuksena on selkeä kokonaiskuva tallennetun tiedon suhteesta muuhun tietoon sekä syötetyn tiedon eheys- ja oikeellisuustarkistukset. Järjestelmää ei saa saada sekaisin virheellisillä syötteillä. Asennusopas on oltava ylläpitäjän ymmärrettävissä ja asennuksen on oltava prosessina helposti opittava.

9. Suosituksia toteutukseen

Ohjelmiston ylläpitomalliin suositellaan avoimen lähdekoodin ylläpitomallia. Ohjelma on pystyttävä integroimaan eri käyttäjäympäristöihin ja sellaisten tahojen käyttöön, joilla ei ole resursseja käytettävissä ohjelmiston ylläpitoon kaupallisten tahojen toimesta. Avoin lähdekoodi auttaa myös jokaisen käyttäjätahon itse testata ohjelmiston luotettavuutta tehokkaammin.

Pohjajärjestelmäksi suositellaan jotain valmista WWW-pohjaista taustajärjestelmää, jossa olisi valmiina ainakin käyttäjien kirjautumiseen ja tiedostojärjestelmän turvallisuuteen liittyvät toiminnot. Esimerkkeinä PHP-pohjaiset Joomla! ja Drupal tarjoavat nämä toiminnot. Toteutuskielenä tulisi olla kieli jota yleisimmät webhostellit tukevat. Tällä hetkellä yleisin tuettu kieli on PHP ja tuettu tietokantaserveri MySQL.