TIETOTURVARISKIEN KARTOITUS

OIKEUSMINISTERIÖ — NETTIÄÄNESTYKSEN ESISELVITYS

Helsinki, 2017-05-26

Marko Buuri
Johtava riskienhallintakonsultti

Antti Vähä-Sipilä
Laadunvarmistus

F-Secure

Sisältö

RAPORTISTA

Tämän raportin on laatinut F-Secure Cyber Security Services osana nettiäänestyksen esiselvitystä Oikeusrekisterikeskuksen ja Oikeusministeriön toimeksiannosta. Kaikki raportissa oleva ja muutoin toimeksiannossa syntynyt aineisto on tarkoitettu työryhmän käytettäväksi osana esiselvityksessä muodostettavia johtopäätöksiä ja suosituksia.

Raportti ei ole aihealueen kattava yleisselvitys. Sen sisältöä rajoittavat valittu työmenetelmä, laadintaan käytettävissä ollut aika, käytettävissä ollut taustamateriaali, tiedot tulevan nettiäänestysjärjestelmän toimintaperiaatteista ja teknologioista, sekä työpajoihin osallistuneiden esiin tuomat näkemykset aiheesta.

Raportin jakelusta ja salassa pitämisestä päättää tilaaja.

1. JOHDANTO

Oikeusministeriö on asettanut työryhmän, joka valmistelee selvityksen nettiäänestyksen käyttöönotosta yleisissä vaaleissa. Yleisillä vaaleilla tarkoitetaan eduskunta-, kunta-, europarlamentti- ja presidentinvaaleja sekä valmistelussa olevia maakuntavaaleja. Nettiäänestyksellä tarkoitetaan äänestystapahtumaa, joka suoritetaan äänestäjän valitsemalla päätelaitteella internetin välityksellä.

Nettiäänestyksen edellytyksiä selvittänyt edellisen kerran työryhmä, joka jätti loppuraporttinsa 22.4.2015 (OM julkaisu 28/2015, asianumero 3/021/2013). Raportissa käsitellään nettiäänestyksen turvallisuuskysymyksiä useilta kannoilta. Järjestelmän on oltava sellainen, että se saa kansalaisten luottamuksen. Lisäksi äänestysjärjestelyillä on tehokkaasti varmistettava äänestyksen turvallisuus ja äänioikeutettujen vaalisalaisuuden sekä valinnanvapauden säilyminen. Varsinaisia tietoturva-uhkia raporttiin on kirjattu seuraavasti:

- Toimittajan mahdollisuudet toimittaa tietoturvallinen järjestelmä.
- Äänestäjän päätelaitteen ja sen ohjelmiston turvallisuus.
- Palvelunestohyökkäykset nettiäänestysjärjestelmään ja puutteet kyvyssä reagoida siihen kohdistuviin tietoturvahyökkäyksiin.
- Tietoturvallisuutta vaarantavat virheet vaalijärjestelmään liittyvissä asennuksissa ja ylläpidossa.
- Nettiäänestys on riippuvainen ulkopuolisista järjestelmistä, joiden toimintahäiriöt tai joihin kohdistuvat hyökkäykset voivat vaikuttaa myös nettiäänestykseen.
- Puutteet järjestelmän valvonnassa.

Parhaillaan meneillään olevan esiselvityksen tavoitteisiin kuuluu aiemmin tunnistettujen turvallisuusriskien käsittelyn laajentaminen, jotta riskien vaikutuksia ja hallintakeinojen kustannuksia olisi mahdollista arvioida. Tämä raportti kuvaa työn aikana tunnistettuja nettiäänestyksen tietoturvariskejä. Toimeksiannon aikana ei ollut tiedossa Suomeen valittavan nettiäänestysjärjestelmän tekninen toteutus. Tästä johtuen käsittelytapa perustuu ylätason riskien ja niiden mahdollisten seurausten sekä juurisyiden tunnistamiseen.

1.1. VAKAVIMMAT RISKIT

Seurauksiltaan vakavimpia riskiskenaarioita tunnistettiin kolme. Taloudellisilta ja yhteiskunnallisilta vaikutuksiltaan merkittävin riski koskee mahdollisuutta manipuloida äänestyksen tulosta nettiäänestysjärjestelmän turvallisuuspuutteita hyödyntämällä.

Muut vakavat skenaariot koskevat mahdollisuutta häiritä nettiäänestysjärjestelmää, sekä vaalisalaisuuden toteutumista nettiäänestyksessä. Häirinnällä voidaan estää yhtäläisen äänioikeuden toteutuminen. Jos tilanne johtaa vaalien uusimiseen, kustannukset yhteiskunnalle ovat kymmeniä miljoonia euroja; pelkästään Oikeusministeriön suorat kustannukset yleisissä vaaleissa ovat nykyisellään noin 18 miljoonaa euroa. Vaalisalaisuuden laajamittainen menettäminen, eli äänestäjien antamien äänien paljastuminen, voi puolestaan aiheuttaa huomattavaa inhimillistä kärsimystä, mutta myös yhteiskunnallista epävakautta.

Vakavimpia riskiskenaarioita käsitellään tarkemmin luvussa 3. Luku 4 käsittelee laajemmin toimeksiannon aikana syntyneen riskiaineiston ja mahdollisia hallintakeinoja.

1.2. SEURAAVAT VAIHEET

Tämä raportti on osa nettiäänestystä koskevan esiselvityksen tietoturvaa koskevia tehtäviä. F-Secure suosittelee, että raportti lähetetään kommentoitavaksi Oikeusministeriön valitsemille sidostahoille. Esiselvityksen myöhemmissä vaiheissa tuloksia on tarkoituksen mukaista käyttää nettiäänestysjärjestelmän toiminnallisten ja turvallisuusvaatimusten määrittämiseen, kustannus-hyöty –analyysiin, ja käyttöönottopäätöksen tukena.

2. KARTOITUKSEN TOTEUTUSTAPA

Tehty tietoturvariskien kartoitus liittyy Oikeusministeriön vetämään esiselvitykseen nettiäänestyksestä yleisissä vaaleissa. Riskikartoitustoimeksianto on yksi osa esiselvitystä, jossa pyritään avaamaan useita nettiäänestyksen kustannuksiin, riskeihin ja turvallisuuteen liittyviä kysymyksiä parlamentaarista päätöksentekoa varten. Esiselvityksen valmistumisen ajankohdaksi on asetettu lokakuu 2017.

Tietoturvariskien kartoitusta koskeva toimeksianto perustuu olemassa olevien dokumenttien katselmointiin sekä kahteen työpajaan, joihin kutsuttiin Oikeusministeriön valitsemien sidosryhmien edustajat. Toimeksiannon alainen työskentely ajoittui huhti- ja toukokuulle 2017. Tämä raportti pitää sisällään toimeksiannon aikana saavutetut tulokset.

Toimeksiannon toteutti ja tämän raportin laati johtava riskienhallintakonsultti Marko Buuri, F-Secure Cyber Security Services.

2.1. DOKUMENTAATIO

Seuraavat nettiäänestyksen tietoturvallisuuskysymyksiin liittyvät asiakirjat olivat käytettävissä tätä kartoitusta tehtäessä.

- Council of Europe E-voting recommendations (luonnos 2017)
- OSCE ODIHR Handbook for the Observation of New Voting Technologies (2013)
- The Future of Voting – End-to-end Verifiable Internet Voting, U.S. Vote Foundation (2015)
- Independent Report on E-voting in Estonia, University of Michigan (2014)
- Norjan, Sveitsin ja Viron nettiäänestysjärjestelmiä koskevaa dokumentaatiota

2.2. TYÖPAJAT

Toimeksiannon aikana järjestettiin kaksi saman sisältöistä työpajaa, joiden tarkoitus oli kartoittaa eri viranomaisten asiantuntijanäkemyksiä nettiäänestyksen riskeihin liittyen. Työpajojen työskentelytapana oli asiaan liittyvien uhkatoimijoiden, niistä aiheutuvien turvallisuuspoikkeamien, ja poikkeamiin mahdollisesti johtavien heikkouksien tunnistaminen. Työpajojen tulokset on eritelty luvussa 4 sekä liitteenä olevassa riskikaaviossa.

Työpajoihin osallistuivat seuraavat henkilöt.

Molemmat työpajat	
Arto Jääskeläinen	Oikeusministeriö, vaalijohtaja
Anneli Salomaa	Oikeusministeriö, esiselvitystyöryhmän sihteeri
Heini Huotarinen	Oikeusministeriö, esiselvitystyöryhmän sihteeri
Juha Mäenalusta	Oikeusrekisterikeskus, järjestelmäasiantuntija
Marko Buuri	F-Secure, työpajojen koordinaattori
Työpaja 2.5.	
Tero Muurman	Keskusrikospoliisi
Ismo Rossi	Keskusrikospoliisi
Anniina Tjurin	Oikeusrekisterikeskus
Pasi Koljonen	Puolustusvoimat
Juha Savolainen	Puolustusvoimat

Tuomo Kouhia	Valtori
Mikko Viitaila	Viestintävirasto
Mika-Jan Pullinen	Valtioneuvoston kanslia
Työpaja 5.5.	
Aarno Sandvik	Keskusrikospoliisi
Juha Tretjakov	Viestintävirasto
Kimmo Janhunen	Oikeusrekisterikeskus
Tommi Simula	Valtori
Jari Ylitalo	Valtioneuvoston kanslia

2.3. RAJOITUKSET

Tätä riskikartoitusta tai raporttia laadittaessa ei ollut tiedossa mikä äänestysjärjestelmä Suomeen tullaan valitsemaan, millainen kohdearkkitehtuuri siihen tullaan toteuttamaan, tai mitään teknisiä yksityiskohtia järjestelmän toiminnasta tai integraatioista. Tästä johtuen käsittelytavaksi valittiin taso, jossa teknologia-sidonnaiset kysymykset eivät olennaisesti vaikuta.

Riskikartoitusten tulosten laajuus riippuu aina käytettävissä olevasta ajasta. Riskien tunnistamiseen ja arviointia on tarkoituksen mukaista jatkaa alueilla, jotka mahdollisesti eivät tämän kartoituksen perusteella ole riittävän kattavia.

3. VAIKUTUKSILTAAN VAKAVIMMAT RISKIT

Tämä luku kuvaa toimeksiannon aikana vaikutuksiltaan vakavimmiksi tunnistetut riskiskenaariot.

3.1. VAALITULOKSEN LAAJA MANIPULOINTI

Nettiäänestysjärjestelmä luo uudenlaisen mahdollisuuden manipuloida yleisten vaalien tulosta. Muissa äänestystavoissa käytössä oleva ääntenlaskun hajauttaminen edellyttäisi laajaa laskentaan osallistuvien salaliittoa tuloksen merkittävään manipulointiin. Tällöin äänestyslippuja hävitettäisiin tai muokattaisiin huomattavia määriä, jotta tarkistuslaskennassa tulos ei muuttuisi. Nettiäänestyksen ollessa käytössä muiden vaihtoehtojen rinnalla vastaavan vaikutuksen saamiseen voi riittää tietojärjestelmän tietosisällön muokkaaminen niin, että annettuja ääniä poistetaan tai siirretään toisille ehdokkaille. Manipuloinnin mahdollisuudet ovat sitä laajemmat, mitä suurempi osuus äänistä annetaan netissä.

Nettiäänestysjärjestelmän tietosisällön manipulointi voi olla mahdollista uhkatoimijalle, joka on riittävän motivoitunut vaikuttamaan yleisvaalien tulokseen sekä omaa riittävän keinovalikoiman toimenpiteen toteuttamiseksi. Kuviteltavissa olevaan keinovalikoimaan kuuluu internetin kautta tapahtuvaan nettiäänestysjärjestelmään murtautumisen lisäksi esimerkiksi takaporttien ja toimintojen piilottaminen järjestelmään ennakolta, tietojärjestelmän valmistajan tai ylläpitohenkilöstön kiristys tai lahjonta, tai äänten manipulointiin tarkoitettujen haittaohjelmien toimittaminen ennakolta äänestäjien päätelaitteille. Tällaiset keinot tai niiden yhdistelmä voivat olla esimerkiksi vieraan vallan resursoimalla toimijalla.

Tietojärjestelmien sisäistä toimintaa on hankalaa tai mahdotonta luotettavasti havainnoida ulkoa päin. Kaikki tietojärjestelmän ulospäin näyttämät indikaatiot ovat yleensä sen itsensä tuottamia, ja tuolloin manipuloitavissa samoin perustein kuin muutkin osat järjestelmää. Erikoinen tai odotuksista poikkeava vaalitulos voi antaa aihetta epäillä järjestelmän manipulointia, vaikka sitä ei olisikaan tapahtunut. Samoin kuin vilpin todentaminen, myös kiistattoman vilpittömyyden näytön kerääminen voi olla hankalaa. Tämä saattaa asettaa yhteiskunnan vakauden vaaraan erityisesti, jos samaan aikaan on käynnissä muu informaatiovaikuttamisen operaatio.

Suomessa vaalitulos vahvistetaan aina ääntenlaskennan päätyttyä. Vahvistetun tuloksen perusteella vaaleissa valitut henkilöt saavat asemansa mukaiset valtuudet. Näin tapahtuu myös silloin, kun vaaleissa epäillään vilppiä. Vahvistetusta tuloksesta on mahdollista valittaa, ja vaalit voidaan uusia oikeuden päätöksellä, mikäli näyttöä epäselvyyksistä voidaan osoittaa. Tuloksen vahvistamisesta voi kulua kuitenkin kuukausia tai vuosia siihen, että riittävä tietotekninen näyttö on kerätty ja käsitelty eri oikeusasteissa, ja uudet vaalit järjestetty. Erikoinen tai odotuksista poikkeava vaalitulos ei itsessään ole näyttö vilpistä, eikä nettiäänestyksen tulosta ole mahdollista laskea uudelleen riippumatta saman tietojärjestelmän sisällöstä.

Ennen uusien vaalien järjestämistä vaaleissa valitut voivat käyttää asemansa mukaista valtaa. Kunnallisella tasolla valtuutetut voivat tehdä päätöksiä, joilla voi aiheutua merkittäviä taloudellisia hyötyjä tai haittoja joillekin tahoille. Eduskuntaan valitut kansanedustajat voivat säätää lakeja ja äärimmäisessä tapauksessa muuttaa perustuslakia kiireellisen säätämisjärjestyksen mukaisesti. Johtuen tästä, vaalituloksen laajamittainen manipulointi voi onnistuessaan olla äärimmäisen vahingollinen tapahtuma yhteiskunnan vakauden näkökulmasta.

Internetin toimintaympäristössä on tyypillistä, että tietojärjestelmiin murtautuneita henkilöitä ei pystytä varmuudella osoittamaan. Tämä on erityisen yleistä silloin, kun kyseessä on hyvin resursoidut kohdennetut hyökkäykset valtionhallintoon tai niiden kanssa toimiviin yrityksiin.

3.2. VAALIEN HÄIRINTÄ PALVELUNESTOHYÖKKÄYKSILLÄ

Vaalien häirintä tietoteknisillä keinoilla muodostaa uudenlaisen riskin demokraattiseen vaalijärjestelmään. Kaikki internetiin liitetyt palvelut altistuvat jollakin tasolla palvelunestohyökkäyksille. Näillä hyökkäyksillä tarkoitetaan tilannetta, jossa uhkatoimija synnyttää ylimääräistä tietoliikennettä, muuta kuormitusta tai

yhteyksien katkeamisen, aiheuttaen tilanteen, jossa palvelun luvalliset käyttäjät eivät voi ottaa yhteyttä palvelun toimintoihin.

Hyökkäysten toteuttaminen ei ole kallista ja niitä voi ostaa palveluna. Hyökkäysten torjunta on vaikeaa ja perustuu yleensä joko palveluun kohdistuvan tietoliikenteen tilapäiseen rajoittamiseen, esimerkiksi Suomen rajojen ulkopuolelta tulevan tietoliikenteen perille toimittamisen estämiseen, tai itse palvelun hajauttamiseen lukuisiin palveluympäristöihin.

Tilanne on ongelmallinen yhtäläisen äänioikeuden toteutumisen näkökulmasta. Yhtäläisellä äänioikeudella tarkoitetaan sitä, että jokaisella äänioikeutetulla on yhtäläinen oikeus vaikuttaa vaalin tulokseen. Nettiäänestyksen toteutuessa voidaan ajatella, että äänioikeutetulla on oikeus antaa äänensä nettiäänestysjärjestelmällä. Mikäli tämä ei toteudu palvelunestohyökkäyksen tai muun häiriön johdosta, ei äänioikeutetulla välttämättä ole mahdollisuutta antaa ääntä uudelleen muulla äänestystavalla.

Koska palvelunestohyökkäys määritelmällisesti voi estää äänestäjän yhteyden äänestysjärjestelmään, epäonnistuneista yrityksistä ei välttämättä jää mitään jälkiä. Vaaliviranomaisten ei välttämättä ole mahdollista jälkikäteen todentaa, kuinka monen äänioikeutetun äänestysyritys on tästä syystä epäonnistunut.

Koska palvelunestohyökkäysten toteutumista ei voida estää tai vaikutuksia täysin poistaa, vaalilakia uudistettaessa tulisi huomioida näiden tilanteiden mahdollisuus, ja niiden vaikutus vaalien tuloksen hyväksyttävyyden näkökulmasta. Jos häirintä johtaa vaalien uusimiseen, kustannukset yhteiskunnalle ovat kymmeniä miljoonia euroja. Oikeusministeriön suorat kustannukset yleisissä vaaleissa ovat nykyisellään noin 18 miljoona euroa. Ehdokkaiden kampanjointi ja yleisen tuottavuuden väheneminen vaalien järjestämisen sekä äänestäjien osallistumisen vuoksi aiheuttavat merkittävän taloudellisen kuluerän. Ehdokkaiden kyky käydä uusintavaalikampanjaa voi riippua voimakkaasti ehdokkaiden henkilökohtaisesta varallisuudesta.

Ulkoisen toimijan motivaatio palvelunestohyökkäykseen voisi olla tavoite estää vaalien järjestäminen tiettynä aikana, jos esimerkiksi poliittisista syistä voitaisiin vaalien tuloksen olevan hyökkääjän näkökulmasta edullisempi jonkin verran myöhempänä ajankohtana. Käytännössä palvelunestohyökkäys voidaan nähdä myös tapana estää Suomen valtiota järjestämästä vaaleja valitsemanaan ajankohtana.

3.3. VAALISALAISUUDEN MURTUMINEN AIHEUTTAA EPÄVAKAUTTA

Saatavilla olevien nettiäänestysjärjestelmien tekninen toteutustapa jättää mahdollisuuden vaalisalaisuuden murtamiselle. Huolimatta käytössä olevista salausalgoritmeista, osana nettiäänestystapahtuman eri vaiheita syntyy riittävä määrä tietoa, joita yhdistelemällä on mahdollista selvittää kunkin äänestäjän antama ääni. Tältä osin nettiäänestysjärjestelmissä ei saavuteta vaalipäivänä tapahtuvan äänestämisen tasoista vaalisalaisuutta.

Myös muissa äänestystavoissa on mahdollista selvittää yksittäisten äänestäjien antamia ääniä. Ennakko-, koti-, ja kirjeäänestyksessä tieto äänestäjästä sekä äänestyslippu joissakin prosessin vaiheissa yhdistettävissä toisiinsa. Nettiäänestys on kuitenkin äänestystavoista ainoa, jossa yhden keskitetyn pisteen turvallisuusongelma voi johtaa siihen, että kaikkien kyseistä äänestystapaa hyödyntäneiden äänet paljastuvat.

Oman erityispiirteensä vaalisalaisuuden säilymiseen muodostaa se, että salausalgoritmeilla on rajallinen elinkaari. Nettiäänestyksestä syntyy tietovarantoja, niiden varmuuskopioita, ja tietoliikenteen näytteitä, jotka ovat kokonaan tai osittain salattuja äänestyshetkellä. Käytettävissä olevan laskentatehon lisääntyminen (mukaan lukien kvanttilaskennan kehittäminen) ja salakirjoitusten avaamiseen (kryptoanalyysiin) liittyvät matemaattiset edistysaskeleet tarkoittavat, että nyt parhailla menetelmillä salakirjoitetut tiedot ovat avattavissa tulevaisuudessa. Salakirjoituksen elinkaari on perinteisesti ollut korkeintaan kymmeniä vuosia; tällä hetkellä voimassa olevat salaussuositukset on annettu tyypillisesti vuosiin 2030-2040 asti. Jos jollakin toimijalla on keinoja säilyttää salakirjoitettuja tietoja, jotka on hankittu tietoliikennettä tiedustelemalla tai itse nettiäänestysjärjestelmästä, voi olla mahdollista, että tämä toimija saa yhdistettyä äänet äänestäjiin vielä näiden elinaikana. Tämä voi aiheuttaa inhimillistä kärsimystä ja yhteiskunnallista epävakautta tavoilla, joita ei Suomessa nykyisen vaalisalaisuuden ja äänestämisen vapauden piirissä voida täysin ennakoida.

4. RISKILUETTELO

Tämä luku kuvaa toimeksiannon aikana tunnistetut riskit. Riskit on ryhmitelty seuraavissa luvuissa uhkatoimijoiden mukaisesti. Riskit on kuvailtu seuraavasti.

- Riskin kuvaus on kuvailu siitä, millaisia tavoitteita uhkatoimijalla on, mihin toimenpiteisiin toimija ryhtyy, ja mitä heikkouksia hän voisi käyttää hyväkseen toimenpiteiden saavuttamiseksi.
- Arvio riskin vaikutuksesta perustuu työpajoissa esille tulleisiin käsityksiin riskien haitallisista lopputulemista.
- Mahdolliset hallintakeinot kuvaavat tapoja rajoittaa kutakin riskiä. Esitetyt hallintakeinot eivät ole tyhjentävä luettelo, eivätkä ne välttämättä ole tehokkuudeltaan yksin riittäviä riskin mahdollisuuden poistamiseksi tai vaikutusten alentamiseksi.

Raportin liitteenä on lisäksi kaavio samoista riskeistä. Riskien R-tunnisteet ovat merkitty kaavioon.

4.1. VERKKORIKOLLINEN

Verkkorikollisella tarkoitetaan tässä yhteydessä yksittäistä henkilöä tai joukkoa henkilöitä, joilla on yhteinen motivaatio haitata tai vahingoittaa vaalien suorittamista nettiäänestysjärjestelmällä, sekä kyvykkyys toteuttaa hyökkäys internetin välityksellä.

	RISKIN KUVAUS	ARVIO RISKIN VAIKUTUKSESTA	MAHDOLLISIA HALLINTAKEINOJA
R1	Verkkorikollinen toteuttaa palvelunestohyökkäyksen nettiäänestysjärjestelmää kohtaan. Hyökkäyksen tavoitteena on äänestämisen estäminen tai häiritseminen. Mahdollisia motiiveja: • Maineen kasvattaminen rikollis- tai hakkeripiireissä • Rahan ansaitseminen hyökkäyksellä kiristämisellä • Kiusanteko • Poliittisen tai muun vakaumuksen toteuttaminen Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Internetiin liitetyt järjestelmät ovat luontaisesti alttiita palvelunestohyökkäyksille. • Kiinnijäämisen uhka tekijälle on pieni.	Tilanne on harmillinen ulkomailla asuville ja siellä oleskeleville, sillä nettiäänestyksen estäminen voi tarkoittaa, ettei heillä ole mahdollisuutta äänestää lainkaan, riippuen muista jäljellä olevista äänestysmahdollisuuksista. Hyökkäystä voidaan käyttää riistämään äänestyksen järjestäjältä mahdollisuus järjestää äänestys haluttuna ajankohtana. Mahdollinen uusintavaali aiheuttaa suoria kustannuksia sekä järjestäjälle että ehdokkaille. Riskiä on käsitelty raportin luvussa 3.2.	**Tietoliikenteen rajoittaminen** Palvelunestohyökkäysten vaikutusta on mahdollista pienentää rajoittamalla tietojärjestelmään kohdistuvaa tietoliikennettä. Tyypillinen toteutus on rajoittaa ulkomailta Suomeen kohdistuvaa liikennettä. Näin toimittaessa on kuitenkin todennäköistä, että samalla estetään ulkomailla asuvien ja olevien äänioikeutettujen mahdollisuus äänestää netissä. **Tietojärjestelmän hajauttaminen** Hajauttamalla tietojärjestelmä useiden palveluntuottajien ympäristöihin on mahdollista pienentää palvelunestohyökkäysten vaikutusta.

R2	Verkkorikollinen murtautuu nettiäänestysjärjestelmän toimittajan IT-ympäristöön asentaakseen äänestysjärjestelmään piilotettuja toimintoja. Toimintojen tavoitteena on vaalien tuloksen manipulointi. Mahdollisia motiiveja: • Oman edun tavoittelu vaalien tulokseen vaikuttamalla • Rahan ansaitseminen vaalien tulos myymällä Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Nettiäänestysjärjestelmän toimittajan omiin turvallisuusjärjestelyihin ei voida vaikuttaa. • Nettiäänestysjärjestelmään piilotettujen toimintojen havaitseminen voi olla vaikeaa.	Riskin seurauksena voi olla vaalituloksen laajamittainen manipulointi. Äärimmillään tilannetta voi kuvata vallankaappaukseksi. Vaalien tuloksesta on mahdollista valittaa, mutta tutkintaan, valituksen käsittelyyn ja vaalien uusimiseen voi nykyisen lain mukaan kulua esimerkiksi vuosi. Tuona aikana vaalien vahvistettu tulos on voimassa, ja vaaleissa valitut täysivaltaisia hoitamaan tehtäviään. Riskiä on käsitelty raportin luvussa 3.1.	**Edellytetään avointa lähdekoodia ja täysin eheä koodin tuotantoon vienti** Nettiäänestysjärjestelmään piilotettuja toimintoja on mahdollista havaita, jos sen lähdekoodi on saatavilla ja vapaasti tutkittavissa. Hallintakeinona tämä on kuitenkin tehokas vain, jos kaikki tietojärjestelmän lähdekoodit ovat avoimia – myös laiteajurit ja käyttöjärjestelmä – ja lähdekoodin ja suunnitteluperiaatteiden analysointiin on käytettävissä riittävästi ja riittävän osaavia asiantuntijoita. Pelkkä lähdekoodin oikeellisuus ei vielä kuitenkaan takaa, että itse järjestelmä käyttäisi (vain ja ainoastaan) tätä koodia, ja että tästä voitaisiin jälkikäteenkin varmistua. Ajettavan koodin oikeellisuuden varmentaminen on vaikea, mutta samalla olennainen osa luottamusketjun toteutumista. **Laaja tietoturvatestaus** Järjestelmän toimintojen oikeellisuutta on mahdollista varmistaa laajalla tietoturvatestaamisella, jossa yhdistyy lähdekoodin katselmointia ja erilaisia toiminnan luotettavuutta varmistavia testitapauksia.

4.2. AKTIVISTI TAI VAALEISSA HÄVINNYT

Tällä uhkatoimijalla tarkoitetaan tässä yksittäistä henkilöä tai joukkoa henkilöitä, joilla on yhteinen motivaatio haitata tai vahingoittaa nettiäänestysjärjestelmän yleistä uskottavuutta.

	RISKIN KUVAUS	ARVIO RISKIN VAIKUTUKSESTA	MAHDOLLISIA HALLINTAKEINOJA
R3	Uhkatoimija lietsoo epäluottamusta ja levittää vääriä tietoja äänestysjärjestelmästä. Vaaleissa hävinnyt voi väittää tietävänsä äänestysjärjestelmän manipuloinnista ja koittaa siten vaikuttaa äänestyksen uusimiseen oikeusistuimissa, lietsoa epäluottamusta valtaapitäviin tai kerätä kannatusta. Pienemmässä mittakaavassa riski voi toteutua siten, että yksittäiset henkilöt väärentävät tai muutoin väittävät netti-	Riskin seurauksena yleinen luottamus vaalien eheyteen ja poliittiseen järjestelmään sekä valtaapitäviin laskee. Tämä aiheuttaa epävakautta yhteiskunnassa, kuten mielenosoituksia, poliittista vastakkainasettelua ja muita tämän kaltaisia muutoksia sisäisessä turvallisuusympäristössä. Vaikutusten mittakaavaa on vaikea arvioida.	**Tapahtumien jäljitettävyys** Nettiäänestyksen eheyden varmistaminen edellyttää, että kaikista äänestämiseen ja järjestelmän ylläpitoon liittyvistä tapahtumista jää turvallisesti säilytettävät tapahtumalokit. Lokien osuus on keskeinen mahdollisten virheiden ja väärinkäytösten tutkinnassa. Mutta vaikka tarkat lokikirjaukset ovat keskeisiä äänestystu-

	äänestysjärjestelmän toimineen virheellisesti, esimerkiksi mahdollistaneen useiden äänten antamisen tai toisten antamien äänten paljastumisen. Mahdollisia motiiveja: • Poliittisen tai muun vakaumuksen toteuttaminen • Kannatuksen kerääminen • Kiusanteko Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Nettiäänestysjärjestelmän toiminnan luotettavuutta on vaikea perustella kansantajuisesti. • Nettiäänestyksen toimintaa ei voida suoraan havainnoida samoin kuin paperiin perustuvien äänestyslippujen käsittelyä ja laskentaa. • Nettiäänestyksen tulosta ei voida tarkastuslaskea riippumatta itse järjestelmän sisällöstä.	Riskiä on osittain käsitelty raportin luvussa 3.1 osana äänestysjärjestelmän eheyden toteennäyttöongelmaa.	loksen eheyden varmistamiseksi, ovat ne mahdollinen riskilähde vaalisalaisuuden paljastumiselle (ks. riskit R5, R10). **Järjestelmien monistaminen** Nettiäänestysjärjestelmä voisi toimia siten, että laskentaa suoritetaan usealla rinnakkaisella järjestelmällä, jotka olisivat kilpailevien puolueiden tai ehdokkaiden toimittamia tai erikseen tarkastamia. Tämä vastaisi käsitteellisesti eri puolueiden edustajia äänten laskutilanteessa. Tämä vaikuttaisi käyttökustannuksiin ja vaatisi, että tarkastukseen on käytettävissä riittävästi ja riittävän osaavia toisistaan riippumattomia asiantuntijoita. Tässä mallissa tulisi myös määritellä, mitä seuraisi siitä, jos rinnakkaisten järjestelmien tulokset poikkeaisivat keskenääni. Etenkin tahallisen häiriön mahdollisuus vaalien estämiseksi tai siirtämiseksi on huomioitava. **Edellytetään avointa lähdekoodia** Yleisen hyväksyttävyyden kannalta on kriittistä, että nettiäänestysjärjestelmän hankinnassa ja toteutuksessa pyritään mahdollisimman laajaan avoimuuteen. Nettiäänestysjärjestelmään piilotettuja toimintoja on mahdollista havaita, jos sen lähdekoodi on saatavilla ja vapaasti tutkittavissa. Hallintakeinona tämä on kuitenkin tehokas vain, jos kaikki tietojärjestelmän lähdekoodit ovat avoimia – myös laiteajurit ja käyttöjärjestelmä – ja lähdekoodin analysointiin on käytettävissä riittävästi ja riittävän osaavia asiantuntijoita. Lisäksi on pystyttävä jälkeen päin todistamaan, että äänestysjärjestelmissä äänten keräämisen ja laskennan aikana suorituksessa ollut koodi oli täsmälleen tämä oikein toimivaksi todettu.

4.3. EHDOKAS

Tällä uhkatoimijalla tarkoitetaan vaaleissa ehdolla olevaa henkilöä tai häntä kannattavia henkilöitä, joilla on yhteinen motivaatio edesauttaa ehdokkaan valituksi tulemista.

	RISKIN KUVAUS	ARVIO RISKIN VAIKUTUKSESTA	MAHDOLLISIA HALLINTAKEINOJA
R4	Nettiäänestäminen rinnastuu koti- ja kirjeäänestämiseen siinä, ettei äänestystapahtuma ole ympäristöltään valvottu ja turvattu. Näille äänestystavoille yhteistä on kohonnut mahdollisuus äänten ostamiseen, painostamiseen tai toisen nimissä äänestämiseen. Äänten ostaminen tulee mahdolliseksi siksi, että äänestystapahtuman voi suorittaa ostajan nähden. Painostaminen on mahdollista siksi, että fyysiset olosuhteet äänestämiselle eivät ole turvattu, ja painostaja voi seurata äänestystapahtumaa. Toisen nimissä äänestäminen voi olla mahdollista, jos äänestämisessä käytettäviä tunnisteita säilytetään huolimattomasta esimerkiksi kotona. Motiivi: • Ehdokkaan äänimäärän kasvattaminen Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Nettiäänestäminen ei tapahdu valvotuissa olosuhteissa	Riskin vaikuttavuutta rajoittaa sen fyysinen toteutettavuus. Voidaan ajatella, että yksittäisiä äänestystapahtumia altistuu nettiäänestyksen myötä vilpille. Isossa mittakaavassa näin olisi vaikea toimia ilman, että asia tulisi tavalla tai toisella ilmi. Koska teko on rangaistava, ilmiö tulee pysymään piilossa. Asialla voi olla vaikutusta lähinnä kunnallisvaaleissa, joissa erot äänimäärissä ovat pienet. Yksittäisiin ääniin vaikuttaminen voi tehdä eron valinnan ja ulos jäännin välillä. Sen sijaan esimerkiksi eduskuntavaaleissa on epätodennäköistä, että tällä tavoin ratkaistaisiin ehdokkaan läpimeno. Vaalisalasuutta koskevaa riskiä on käsitelty raportin luvussa 3.3.	**Mahdollisuus muuttaa ääntä sähköisesti** Nettiäänestyksen yhteydessä tapahtuvaa painostamista tai äänesten myyntiä voidaan rajoittaa mahdollistamalla nettiäänen antaminen uudelleen ennakkoäänestysajan puitteissa. Tällöin painostus tai ostaminen olisi tehokasta vain, jos se olisi mahdollista tehdä hyvin lähellä ennakkoäänestysajan päättymistä. Hallintakeinon toteuttaminen tarkoittaa, ettei sähköisesti annettuja ääniä voida sekoittaa heti niiden antamisen jälkeen. Sähköisesti aiemmin annettu ääni on pystyttävä poistamaan uurnasta. Tämä lisää riskiä sille, että äänet yhdistetään luvattomasti äänestäjiin (ks. riskit R5, R10). **Mahdollisuus antaa ääni vaalipäivänä** Nettiäänestyksen yhteydessä tapahtuvaa painostamista tai äänesten myyntiä voidaan rajoittaa mahdollistamalla nettiäänen korvaaminen vaalipäivänä annetulla äänellä. Uhkatoimijan tulisi tällöin varmistaa, etteivät hänen painostamansa tai lahjomansa henkilöt pääse äänestämään tuona päivänä. Tämän toteuttaminen suuressa mittakaavassa on vaikeaa ja teko on nykyisellään määritelty rikokseksi (vaalirikos). Hallintakeinon toteuttaminen tarkoittaa, ettei sähköisesti annettuja ääniä voida sekoittaa heti niiden antamisen jälkeen. Sähköisesti aiemmin annettu ääni on pystyttävä poistamaan uurnasta. Tämä lisää riskiä sille, että äänet yhdistetään luvattomasti äänestäjiin (ks. riski R5, R10).

4.4. VALTAAPITÄVÄ

Tällä uhkatoimijalla tarkoitetaan vallassa olevaa yksittäistä henkilöä tai joukkoa henkilöitä (esimerkiksi puolue tai hallitus), joilla on yhteinen motivaatio haitata tai vahingoittaa demokraattisen järjestelmän toimivuutta säilyttääkseen oman valtansa.

	RISKIN KUVAUS	ARVIO RISKIN VAIKUTUKSESTA	MAHDOLLISIA HALLINTAKEINOJA
R5 R6	Valtaapitävä on asemassa, jossa voi vaikuttaa nettiäänestysjärjestelmään. Hän väärinkäyttää asemaansa painostamalla tai määräämällä nettiäänestysjärjestelmään keskeisten vaaliperiaatteiden vastaisia toimintoja. R5. Valtaapitävä määrää nettiäänestysjärjestelmään toimintoja, joiden avulla voidaan selvittää äänestäjien antamat äänet. Tavoitteena toimijalla on tunnistaa hänen poliittiset vastustajansa, jotta heihin voidaan kohdistaa kosto- tai painostustoimenpiteitä. Nettiäänestysjärjestelmän toimintojen manipulointi on yksi tapa selvittää äänestäjien kantoja. Myös lippuäänestyksessä tämä on mahdollista vaikkapa käyttämällä erillisiä uurnia eri ehdokkaille, tai merkitsemällä äänestyslippu myöhempää tunnistamista varten. R6. Valtaapitävä määrää nettiäänestysjärjestelmään toimintoja, joiden avulla vaalitulosta voidaan muuttaa. Myös lippuäänestyksessä tämä on mahdollista, jolloin se edellyttää joko salaliittoa ääntenlaskijoiden kesken tai muutoin korruptoituneita vaaliviranomaisia. Mahdollisia motiiveja: • Vaalien tulokseen vaikuttaminen; oman valta-aseman vahvistaminen • Poliittisille vastustajille ja heidän kannattajilleen kostaminen Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Riski on luontaisesti mahdollinen, sillä tietojärjestelmän toimintoja on mahdollista kehittää aina halutulla tavalla	Riskien toteutuminen on nykyisessä yhteiskunnallisessa tilanteessa hyvin epätodennäköinen. Yritys tulisi luultavasti ilmi, sillä valtaapitävä tarvitsee järjestelmästä vastaavia sisäpiiriläisiä tuekseen toimenpiteen toteuttamiseksi. Jos yhteiskunnallinen tilanne muuttuu Suomessa siten, että valtaa keskittyisi harvemmille tahoille joiden otteet osoittautuisivat autoritaarisiksi, voi riskien toteutuminen muuttua todennäköisemmäksi. Tällöin yleinen ilmapiiri olisi luonteeltaan sellainen, että se alistaisi myös sisäpiiriläisiä noudattamaan käskyjä joko yleisen edun nimissä tai henkilökohtaisten seuraamusten pelossa. Vaalituksen muuttaminen johtaisi pahimmillaan vakaviin lopputuloksiin. Asiaa on käsitelty raportin luvussa 3.1.	Koska riskien juurisyyt on tietojärjestelmän toimintojen määrittelyssä, ei tietojärjestelmää koskevilla etukäteistoimenpiteillä ole käytännössä mahdollista hallita riskiä. Mahdollinen hallintakeino olisi sellainen, jossa nettiäänestysjärjestelmän muutoshallintamenettely tehtäisiin hyvin raskaaksi. Tämä olisi omiaan haittaamaan myös tavanomaista kehitystä ja ylläpitoa. Järjestelmiä täytyy laitteiden ja ohjelmistoalustojen kehityksen vuoksi ylläpitää lähes jatkuvasti, joten täysin muuttumaton järjestelmä ei todennäköisesti olisi enää seuraavissa vaaleissa käyttökelpoinen.

4.5.JÄRJESTELMÄN AVAINHENKILÖ

Tällä uhkatoimijalla tarkoitetaan nettiäänestysjärjestelmän kehittämiseen tai ylläpitoon osallistuvaa yksittäistä henkilöä tai joukkoa henkilöitä, joilla on yhteinen motivaatio manipuloida vaalien tulosta.

	RISKIN KUVAUS	ARVIO RISKIN VAIKUTUKSESTA	MAHDOLLISIA HALLINTAKEINOJA
R7	Järjestelmän avainhenkilö piilottaa nettiäänestysjärjestelmään toimintoja, joiden avulla voi manipuloida vaalien tulosta. Käytännössä tämä tapahtuisi muuttamalla tai poistamalla annettuja ääniä, tai lisäämällä ääniä sellaisille henkilöille, jotka eivät ole äänestäneet netissä tai muulla tavoin. Mahdollisia motiiveja: • Vaalien tulokseen vaikuttaminen; oman valta-aseman vahvistaminen • Poliittisille vastustajille ja heidän kannattajilleen kostaminen Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Riski on luontaisesti mahdollinen, sillä tietojärjestelmän toimintoja on mahdollista kehittää aina halutulla tavalla	Riskin seurauksena voi olla vaalituloksen laajamittainen manipulointi. Äärimmillään tilannetta voi kuvata vallankaappaukseksi. Vaalien tuloksesta on mahdollista valittaa, mutta tutkintaan, valituksen käsittelyyn ja vaalien uusimiseen voi nykyisen lain mukaan kulua esimerkiksi vuosi. Tuona aikana vaalien vahvistettu tulos on voimassa, ja vaaleissa valitut täysivaltaisia hoitamaan tehtäviään. Riskiä on käsitelty raportin luvussa 3.1. Toiminnon lisäämistä voidaan myös käyttää epäilysten lietsontaan äänestysjärjestelmää kohtaan. Mikäli järjestelmään lisätään toiminto, jolla on selvästi potentiaalia vaarantaa jokin äänestyksen perusvaatimuksista, eikä lisättyä tai poistettua toiminnallisuutta huomata järjestelmän tarkastuksessa, julkistamalla asian jälkikäteen usko järjestelmän tarkastuksen tasoon voi romuttua. Nettiäänestysjärjestelmän toteuttajat ovat periaatteellisella tasolla ne henkilöt, jotka lopulta välillisesti laskevat äänet. Riippuen toimittajasta, he eivät välttämättä ole Suomen kansalaisia. Riskiä on osittain käsitelty raportin luvussa 3.1 osana äänestysjärjestelmän eheyden toteennäyttöongelmaa.	**Vahva muutoshallinta** Nettiäänestysjärjestelmään tehtävien muutosten hallintaan on toteutettava riittävän vahva muutoshallintakäytäntö. Kehitys-, ylläpito- ja muut muutostoimenpiteet täytyy teknisten mahdollisuuksien mukaan hajauttaa useiden henkilöiden vastuulle niin, että yksittäisellä ohjelmistokehittäjällä tai ylläpitäjällä ei ole valtuuksia tehdä järjestelmää merkittävästi vaarantavia toimenpiteitä yksin. **Tapahtumien jäljitettävyys** Nettiäänestyksen eheyden varmistaminen edellyttää, että kaikista äänestämiseen ja järjestelmän kehitykseen ja ylläpitoon liittyvistä tapahtumista jää turvallisesti säilytettävät tapahtumalokit. Lokiin tulee kirjata kaikki järjestelmässä tehdyt koodimuutokset, ylläpito- ja käyttötoimenpiteet, tietotekniset häiriöt, sekä turvallisuustapahtumat, kuten luvattomat yritykset kirjautua järjestelmään. Lokien osuus on keskeinen mahdollisten virheiden ja väärinkäytösten tutkinnassa. **Edellytetään avointa lähdekoodia** Nettiäänestysjärjestelmään piilotettuja toimintoja on mahdollista havaita, jos sen lähdekoodi on saatavilla ja vapaasti tutkittavissa. Hallintakeinona tämä on kuitenkin tehokas vain, jos kaikki tietojärjestelmän lähdekoodit ovat avoimia – myös laiteajurit ja käyttöjärjestelmä – ja lähdekoodin analysointiin on käytettävissä riittävästi ja riittävän osaavia asiantuntijoita. Lisäksi on

			pystyttävä jälkeen päin todistamaan, että äänestysjärjestelmissä äänten keräämisen ja laskennan aikana suorituksessa ollut koodi oli täsmälleen tämä oikein toimivaksi todettu.

4.6. VIERAS VALTIO

Tällä uhkatoimijalla tarkoitetaan vierasta valtiota, joilla on yhteinen motivaatio haitata tai vahingoittaa Suomen demokraattisen äänestysjärjestelmän toimintaa.

	RISKIN KUVAUS	ARVIO RISKIN VAIKUTUKSESTA	MAHDOLLISIA HALLINTAKEINOJA
R8	Uhkatoimija murtautuu nettiäänestysjärjestelmän toimittajan IT-ympäristöön asentaakseen äänestysjärjestelmään piilotettuja toimintoja. Toimintojen tavoitteena on vaalien tuloksen manipulointi. Mahdollisia motiiveja: • Vaalien tuloksen manipulointi Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Nettiäänestysjärjestelmän toimittajan omiin turvallisuusjärjestelyihin ei voida vaikuttaa. • Nettiäänestysjärjestelmään piilotettujen toimintojen havaitseminen voi olla vaikeaa.	Riskin seurauksena voi olla vaalituloksen laajamittainen manipulointi. Äärimmillään tilannetta voi kuvata vallankaappaukseksi. Vaalien tuloksesta on mahdollista valittaa, mutta tutkintaan, valituksen käsittelyyn ja vaalien uusimiseen voi nykyisen lain mukaan kulua esimerkiksi vuosi. Tuona aikana vaalien vahvistettu tulos on voimassa, ja vaaleissa valitut täysivaltaisia hoitamaan tehtäviään. Riskiä on käsitelty raportin luvussa 3.1.	**Edellytetään avointa lähdekoodia** Nettiäänestysjärjestelmään piilotettuja toimintoja on mahdollista havaita, jos sen lähdekoodi on saatavilla ja vapaasti tutkittavissa. Hallintakeinona tämä on kuitenkin tehokas vain, jos kaikki tietojärjestelmän lähdekoodit ovat avoimia – myös laiteajurit ja käyttöjärjestelmä – ja lähdekoodin analysointiin on käytettävissä riittävästi ja riittävän osaavia asiantuntijoita. Lisäksi on pystyttävä jälkeen päin todistamaan, että äänestysjärjestelmissä äänten keräämisen ja laskennan aikana suorituksessa ollut koodi oli täsmälleen tämä oikein toimivaksi todettu. **Laaja tietoturvatestaus** Järjestelmän toimintojen oikeellisuutta on mahdollista varmistaa laajalla tietoturvatestaamisella, jossa yhdistyy lähdekoodin katselmointia ja erilaisia toiminnan luotettavuutta varmistavia testitapauksia.
R9 R10	Uhkatoimija kiristää tai lahjoo järjestelmän toimittajan tai ylläpidon henkilöstöä erilaisiin toimenpiteisiin. R9. Uhkatoimijan tavoitteena on piilottaa nettiäänestysjärjestelmään toimintoja, joiden avulla voi manipuloida vaalien tulosta. Käytännössä tämä tapahtuisi muuttamalla tai poistamalla annettuja ääniä, tai lisäämällä ääniä sellaisille henkilöille, jotka eivät ole äänestäneet netissä tai muulla tavoin. R10. Uhkatoimijan tavoitteena on saada sisäpiiriläiseltä nettiäänestysjärjestelmän tietosisältö. Uhkatoimijalla voi olla tapa purkaa tietosisällön salaus tai muutoin yhdistää äänet äänestäjiin, esimerkiksi järjestelmän eri tietosisältöjä	Riskin seurauksena voi olla vaalituloksen laajamittainen manipulointi. Äärimmillään tilannetta voi kuvata vallankaappaukseksi. Vaalien tuloksesta on mahdollista valittaa, mutta tutkintaan, valituksen käsittelyyn ja vaalien uusimiseen voi nykyisen lain mukaan kulua esimerkiksi vuosi. Tuona aikana vaalien vahvistettu tulos on voimassa, ja vaaleissa valitut täysivaltaisia hoitamaan tehtäviään. Riskiä R9 on käsitelty raportin luvussa 3.1 ja riskiä R10 luvussa 3.3.	**Tapahtumien jäljitettävyys** Nettiäänestyksen eheyden varmistaminen edellyttää, että kaikista äänestämiseen ja järjestelmän ylläpitoon liittyvistä tapahtumista jää turvallisesti säilytettävät tapahtumalokit. Lokiin tulee kirjata kaikki järjestelmässä tehdyt ylläpito- ja käyttötoimenpiteet, tietotekniset häiriöt, sekä turvallisuustapahtumat, kuten luvattomat yritykset kirjautua järjestelmään. Lokien osuus on keskeinen mahdollisten virheiden ja väärinkäytösten tutkinnassa.

	ja lokeja yhdistelemällä. Voidaan myös ajatella, että uhkatoimija haluaa kopion tietosisällöstä myöhempää käyttöä varten, vaikka sitä ei pystyttäisi avaamaan heti. Salauksen murtaminen voi tapahtua vasta myöhemmin. Mahdollisia motiiveja: • Vaalien tuloksen manipulointi • Äänten selvittäminen mahdollista jatkokäyttöä kuten painostamista varten tai muutoin demokraattiseen järjestelmään vaikuttamiseksi Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Riski on luontaisesti mahdollinen, sillä tietojärjestelmän toimintoja on mahdollista kehittää aina halutulla tavalla		**Vahva muutoshallinta** Nettiäänestysjärjestelmään tehtävien muutosten hallintaan on toteutettava riittävän vahva muutoshallintakäytäntö. Kehitys-, ylläpito- ja muut muutostoimenpiteet täytyy teknisten mahdollisuuksien mukaan hajauttaa useiden henkilöiden vastuulle niin, että yksittäisellä ylläpitäjällä ei ole valtuuksia tehdä järjestelmää merkittävästi vaarantavia toimenpiteitä yksin. **Edellytetään avointa lähdekoodia** Nettiäänestysjärjestelmään piilotettuja toimintoja on mahdollista havaita, jos sen lähdekoodi on saatavilla ja vapaasti tutkittavissa. Hallintakeinona tämä on kuitenkin tehokas vain, jos kaikki tietojärjestelmän lähdekoodit ovat avoimia – myös laiteajurit ja käyttöjärjestelmä – ja lähdekoodin analysointiin on käytettävissä riittävästi ja riittävän osaavia asiantuntijoita. Lisäksi on pystyttävä jälkeen päin todistamaan, että äänestysjärjestelmissä äänten keräämisen ja laskennan aikana suorituksessa ollut koodi oli täsmälleen tämä oikein toimivaksi todettu. **Laaja tietoturvatestaus** Järjestelmän toimintojen oikeellisuutta on mahdollista varmistaa laajalla tietoturvatestaamisella, jossa yhdistyy lähdekoodin katselmointia ja erilaisia toiminnan luotettavuutta varmistavia testitapauksia.
R11	Uhkatoimija toteuttaa ja levittää äänestäjien päätelaitteisiin haittaohjelmaa, jonka tarkoituksena on manipuloida äänestystapahtumaa. Haittaohjelma voi toimia siten, että äänestäjälle jää käsitys siitä, että hänen äänensä rekisteröidään halutulla tavalla. Todellisuudessa haittaohjelma lähettää nettiäänestysjärjestelmään äänen toiselle ehdokkaalle. Mahdollisia motiiveja: • Vaalien tuloksen manipulointi	Hyökkäyksen onnistumisen todennäköisyyttä rajoittaa se, että äänestäjät tulevat käyttämään erilaisia ja eri turvatasolla olevia päätelaitteita. Haittaohjelmien laajamittainen levittäminen eri päätelaitetyyppeihin siten, että jakelu onnistuu mutta tapahtuu huomaamatta, on hyvin epätodennäköistä. Riskin seurauksena voi olla vaalituloksen laajamittainen manipulointi. Äärimmillään tilannetta voi kuvata vallankaappaukseksi.	**Äänen varmistaminen toisesta kanavasta** Nettiäänestysjärjestelmään on mahdollista yhdistää toimintoja, joiden avulla äänestäjä voi tarkistaa, kenelle hänen äänensä on rekisteröity. Tällä keinolla on mahdollista lisätä luottamusta ja läpinäkyvyyttä nettiäänestämiseen. Hallintakeinon toteuttaminen tarkoittaa, ettei sähköisesti annettuja ääniä voida sekoittaa heti niiden antamisen jälkeen. Tämä lisää riskiä sille, että äänet yhdis-

	Riskiin vaikuttavat mahdolliset haavoittuvuudet tai heikkoudet: • Äänestäjien käyttämien päätelaitteiden turvallisuuteen ei käytännössä voida vaikuttaa ilman, että esimerkiksi joitakin päätelaitetyyppejä tai käyttöjärjestelmiä rajataan äänestämisen ulkopuolelle. Tämä voi olla ongelmallista yhtäläisen äänioikeuden näkökulmasta.	Vaalien tuloksesta on mahdollista valittaa, mutta tutkintaan, valituksen käsittelyyn ja vaalien uusimiseen voi nykyisen lain mukaan kulua esimerkiksi vuosi. Tuona aikana vaalien vahvistettu tulos on voimassa, ja vaaleissa valitut täysivaltaisia hoitamaan tehtäviään. Riskiä on käsitelty raportin luvussa 3.1.	tetään luvattomasti äänestäjiin (ks. riski R5, R10). Tällöin on myös määriteltävä, mitä tapahtuu, jos yksi tai useampia äänestäjiä ilmoittaa, että heidän äänensä on väärin rekisteröity (riippumatta siitä, onko näin todella tapahtunut).

5. JÄLKISANAT

Tämä raportti pitää sisällään tietoturvariskien kartoituksen aikana tehdyt havainnot. F-Secure suosittelee, että raportti lähetetään kommentoitavaksi Oikeusministeriön valitsemille sidostahoille. Esiselvityksen myöhemmissä vaiheissa tuloksia on tarkoituksen mukaista käyttää nettiäänestysjärjestelmän toiminnallisten ja turvallisuusvaatimusten määrittämiseen, kustannus-hyöty –analyysiin, ja käyttöönottopäätöksen tukena.

F-Secure ja toimeksiannon vastuukonsultti vastaavat mielellään kaikkiin toimeksiantoa ja raporttia koskeviin kysymyksiin.