Maiju Partamies

Tietoturvallisuus opiskelijajärjestöissä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan ko

Insinöörityö

11.05.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Maiju Partamies Tietoturvallisuus opiskelijajärjestöissä 23 sivua + 3 liitettä 11.5.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Ohjelmistotekniikka
Ohjaaja(t)	Lehtori Ilpo Kuivanen

Tietoturvallisuuden huomioonottaminen ja tietoturvallinen toiminta on tärkeää kaikkien organisaatioiden toiminnassa. Insinöörityön tavoitteena oli toteuttaa tietoturvasuunnitelma Wiipurilaiselle Osakunnalle. Toimeksiantajalla oli tarve toipumissuunnitelmalle, mutta tietoturvallisen toimintamallin puuttuessa päätettiin työn aiheeksi ottaa tietoturvasuunnitelma, johon sisällytettiin toipumissuunnitelma.

Teoreettinen viitekehys perustuu kirjallisuuteen ja Internet-lähteisiin tietoturvallisuudesta yritys- ja järjestötoiminnassa sekä tietoturvadokumenteista ja niiden toteuttamisesta. Työn konteksti koostuu Wiipurilaisesta Osakunnasta järjestönä ja tietoturvallisen toiminnan nykytilasta.

Työ toteutettiin soveltamalla yrityksien tietoturvallisen toiminnan ja dokumentoinnin malleja opiskelijajärjestötoimintaan. Tietoturvasuunnitelman todettiin pohjautuvan riskikartoitukseen ja tietoturvapolitiikkaan, joten ne toteutettiin ennen tietoturvasuunnitelmaa. Työssä hyödynnettiin myös järjestöjen tietoturvaan liittyvää teoriaa jäsenrekistereistä.

Suurimmiksi tietoturvapuutteiksi todettiin jäsenrekisterin ylläpito, käyttäjätilien kirjautumistietojen säilytys ja epätietoisuus käytettyjen ulkopuolisten palveluiden tietoturvapoikkeuksista. Tärkeänä ja riskejä pienentävänä tekijänä koettiin myös järjestön toimijoiden perehdytys virkailijoiden vaihtuessa vuosittain.

Lopputuloksena tuotettiin tietoturvasuunnitelma, jossa kuvataan tietoturvan nykytilaa tietoturvan osa-alueittain ja ohjeistetaan jokapäiväisessä toiminnassa. Tietoturvasuunnitelma sisältää myös tiedot, miten tietoturvallista toimintaa voidaan kehittää, ja toimet, jotka ovat suunnitteilla toteuttaa tulevaisuudessa. Dokumentin lopussa on toipumissuunnitelma, joka ohjeistaa, miten toimia eri riskien realisoituessa.

Työ toteutettiin onnistuneesti saavuttamalla asetetut tavoitteet. Työn haasteina olivat toteutuksen rajaus ja aikataulu, mutta hyödyllinen dokumentti saatiin toteutettua toimeksiantajan tarpeisiin lopulta ajallaan.

Avainsanat	tietoturva, tietoturvasuunnitelma, opiskelijajärjestö

Author(s) Title Number of Pages Date	Maiju Partamies Information Security at Student Organizations 23 pages + 3 appendices 11 May 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Software Engineering
Instructor(s)	Ilpo Kuivanen, Senior Lecturer

Information security must be taken into consideration in day to day processes of all organizations. The aim of this thesis was to implement an information security plan for a Finnish student nation, Wiipurilainen Osakunta. The client had a need for a recovery plan but in the absence of a proper model for information secure processes it was decided to create the information security plan in which the recovery plan was included.

The theoretical framework is based on literature and Internet sources about information security in business and volunteer organizations, as well as how to plan and execute the documents. The context of the study consists of Wiipurilainen Osakunta as an organization and the current state of information security in the processes used.

The study was carried out by applying the models of information security activities and documentation of companies to student organizations. The information security plan was found to be based on risk mapping and information security policy of a company, so they were done before the information security plan. The theory of member registers of organizations was also integrated to the study.

The biggest information security vulnerabilities were found in the management of the membership register, in the management of user account login information and in the lack of knowledge about possible security abstractions of the external services in use. Proper familiarization processes were considered as an important and risk-reducing factor.

The result was a security plan that describes the current state of information security and has instructions for every day operations. The information security plan also includes information on how to improve information security in the organization and actions planned to be implemented in the future. The paper also includes a recovery plan that guides how to act when different incidents occur.

The study was carried out successfully by achieving the goals set. The challenges were the framing and schedule of the implementation, but a useful document was finally completed on time for the needs of the client.

Keywords	information security, information security plan, student organization

Sisällys

Lyhenteet

HTK	Huoneistotoimikunta
HYY	Helsingin yliopiston ylioppilaskunta
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
WIO	Wiipurilainen Osakunta

1 Johdanto

Tietoturvallinen toiminta on yhä oleellisempaa alati kehittyvässä maailmassa ja, kun tietoa kerätään ja tallennetaan yhä enemmän. Jokaisen organisaation tulisi varautua riskeihin ja suunnitella toimintansa niin, että riskien toteutumiselta vältyttäisiin. Tietoturvallisen toiminnan tueksi voidaan laatia tietoturvasuunnitelma.

Tietoturvasuunnitelma perustuu riskianalyysiin ja organisaation tietoturvapolitiikkaan. Riskianalyysi tehdään kartoittamalla toiminnassa tunnistettavissa olevat riskit ja analysoimalla, kuinka riskien toteutumista voidaan ehkäistä. Tietoturvapolitiikassa linjataan tietoturvallista toimintaa ja kuvataan, miten organisaatio tukee sen kehitystä. Näiden perusteella toteutetaan tietoturvasuunnitelma, johon kirjataan konkreettiset menetelmät ja toimet organisaation tietoturvan kannalta. Tähän sisältyvät ohjeistukset päivittäiseen toimintaan ja suunnitelmat toiminnan kehittämiseen. Tietoturvan kannalta on tärkeää myös kirjata toimet toipumista varten, mikäli riskit realisoituvat, vaikka niitä pyritään ehkäisemään.

Tämän insinöörityön tavoitteena on toteuttaa tietoturvasuunnitelma helsinkiläiselle opiskelijajärjestölle, Wiipurilaiselle Osakunnalle. Osakunnalla oli tarve toipumissuunnitelmalle, jolloin havaittiin, ettei organisaatiolla ole muitakaan tietoturvadokumentteja. Näin päädyttiin toteuttamaan tietoturvasuunnitelma, johon sisällytettäisiin toipumissuunnitelma tunnistetuille riskeille. Työ hyödyttää välittömästi toimeksiantajaorganisaatiota, mutta se voi olla myös hyödyllinen muille järjestöille tulevaisuudessa, sillä tietoa vapaaehtois- tai opiskelijajärjestöjen tietoturvasta on vähän.

Insinöörityö esittelee ensin tieturvan perusteet, johon on sisällytetty sen merkitys, osa-alueet ja tietoturvalliseen toimintaan liittyvät dokumentit. Tämän jälkeen kuvataan tietoturvaa järjestötoiminnassa. Näistä muodostuu teoreettinen viitekehys. Osioissa selitetään keskeiset käsitteet ja sidotaan teoria työn tapaukseen. Konteksti koostuu Wiipurilaisesta Osakunnasta järjestönä ja sen tietoturvallisen toiminnan nykytilasta. Näiden jälkeen kerrotaan toteutetusta riskikartoituksesta ja toteutetuista dokumenteista, joita ovat tietoturvapolitiikka ja tietoturvasuunnitelma. Kaikki toteutetut dokumentit löytyvät työn liitteinä. Lopuksi reflektoidaan työn kulkua ja onnistumista.

2 Tietoturvan perusteet

Jokaisella organisaatiolla ja yksityishenkilöllä on tietoja, jotka halutaan turvata eli estää, etteivät tiedot päädy väärinkäytön kohteeksi. Niiden suojaamiseksi tarvitaan tietoturvaa. Tietoturvallisuus on nykyisin keskeinen osa yritysten ja kotitalouksien sekä muiden organisaatioiden turvallisuutta. Tässä luvussa käsitellään tietoturvallisuuden merkitystä ja esitellään tietoturvan osa-alueet ja dokumentointitavat.

2.1 Merkitys

Käsitteillä tietoturva ja tietosuoja tarkoitetaan eri asioita, mutta ne ovat yhteydessä toisiinsa. Tietosuoja merkitsee henkilön tiedollisen itsemääräämisoikeuden ja yksityisyyden suojaamista. Tietoturvalla tarkoitetaan menettelyjä ja toimenpiteitä tuon suojan ylläpitämiseen. Tietoturvassa suojattaviin asioihin sisältyvät myös tietojen käsittelyssä tarvittavat laitteistot tietoliikennejärjestelmineen. (Hakala, Vainio & Vuorinen 2006, 4; Laaksonen, Nevasalo & Tomula 2006, 17.)

Tietoturvan hallinta koostuu nykytilan kartoituksesta, tietoturvapolitiikan määrittelystä, tietoturvaohjelman ja suunnitelmien laatimisesta, riskien hallinnasta, tietoturva-asioiden huomioimisessa sopimuksissa sekä auditoinnista ja jatkuvasta seurannasta (Andersson & Koivisto 2013, 51).

2.2 Osa-alueet

Tietoturvallisuus koostuu osatekijöistä, joiksi on määritelty luottamuksellisuus, käytettävyys, eheys, kiistattomuus ja pääsynvalvonta. Luottamuksellisuudella tarkoitetaan, että tiedot ovat oikeutettujen henkilöiden käytettävissä. Käytettävyydellä taas tarkoitetaan, että tiedot tulee olla saatavissa tietojärjestelmästä nopeasti ja oikeassa muodossa. Tietojen tulee myös olla paikkaansa pitäviä, eikä niiden tule sisältää tahattomia tai tahallisia virheitä, ja tätä tarkoitetaan eheydellä. Kiistattomuus merkitsee sitä, että tietojärjestelmä kykenee tunnistamaan ja tallentamaan luotettavasti järjestelmää käyttävien henkilöiden tiedot. Pääsynvalvonnalla tarkoitetaan nimensä mukaisesti menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuuriin pääsyä ja sitä kautta sen käyttöä. (Hakala, Vainio & Vuorinen 2006, 4 - 5.)

Näiden lisäksi tietoturvallisuus on jaettu käsittelyn helpottamiseksi osa-alueisiin. Osat ottavat huomioon organisaatioiden tietyllä alueella tarvittavat tietoturvatoimet. Jaottelua pidetään keinotekoisena, koska osa-alueilla on vaikutusta toisiinsa ja niillä on yhteisiä tekijöitä. Jaottelu kuitenkin helpottaa esimerkiksi tietoturvasuunnitelman tekemistä ja dokumenttien jäsentelyä. (Hakala, Vainio & Vuorinen 2006, 10 - 12.) Osa-alueet ovat esiteltyinä seuraavaksi.

2.2.1 Hallinnollinen turvallisuus

Hallinnollisella turvallisuudella pyritään varmistamaan nimensä mukaisesti tietoturvan hallinnointia. Tietoturvaa tulee kehittää ja johtaa. Ylläpidon kannalta tulee pitää yhteyttä eri turvallisuudesta vastaaviin elimiin organisaation sisällä ja tarvittaessa ulkopuolella toimiviin viranomaisiin. Hallinnollisessa turvallisuudessa erityisen tärkeässä asemassa on lainsäädännön ja yksityisoikeudellisten sopimusten vaikutusten arviointi sisäisiin tietoturvakäytäntöihin. (Hakala, Vainio & Vuorinen 2006, 11.)

2.2.2 Fyysinen turvallisuus

Organisaatio tarvitsee fyysiset tilat toiminnalleen, ja ne luovat näin ollen perustan kaikille muille suojaustoimille. Kaikki organisaation tilat eivät ole fyysisen turvallisuuden kannalta samanarvoisia, sillä esimerkiksi laitetilat vaativat parempaa suojausta. (Laaksonen, Nevasalo & Tomula 2006, 125.)

Fyysisen turvallisuuden piiriin kuuluvat myös laitteistot. Sen uhkia ovat kaikki mikä voi aiheuttaa vahinkoa tiloille tai laitteistoille. Tällaisia ovat muun muassa murrot, vesivahingot, tulipalot ja järjestelmien toimintahäiriöt. Edeltävissä tilanteissa tulee tilanteesta riippuen ottaa yhteyttä kiinteistöhuoltoon tai vartiointiliikkeeseen, joka vastaa ylläpidosta. Organisaation kannattaa kuitenkin osallistua fyysisen turvallisuuden suunnitteluun ja ylläpitoon, ja se voi vaikuttaa esimerkiksi sisäisten tilojen suojauksen tasoon muun muassa lukkojen sijoittamisella. (Hakala, Vainio & Vuorinen 2006, 11.)

2.2.3 Henkilöturvallisuus

Henkilöturvallisuus merkitsee sitä, että hallitaan henkilöstön toimista aiheutuvia ja heihin kohdistuvia turvauhkia. Tietoturvan näkökulmasta näihin kuuluvat muun muassa tiedon väärinkäytöt ja inhimilliset virheet. (Laaksonen, Nevasalo & Tomula 2006, 138.)

Tämän osa-alueen suunnitteluun sisältyy henkilöiden toimintakyvyn takaaminen ja käyttöoikeuksien rajaaminen. Jatkuvuuden kannalta toimijoilla tulee mahdollisuuksien mukaan olla varahenkilöitä ja toimintakykyä voidaan parantaa sekä inhimillisiä virheitä välttää oikeanlaisella koulutuksella. (Hakala, Vainio & Vuorinen 2006, 11.) Virheisiin voidaan varautua jo rekrytointitilanteessa valitsemalla tehtäviin sopivia henkilöitä ja väärinkäytöksen mahdollisuutta voidaan pienentää tarvittaessa taustatarkastuksilla (Laaksonen, Nevasalo & Tomula 2006, 139).

2.2.4 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus tarkoittaa, että tiedot tulee säilyttää sopivalla tavalla, niiden säilyvyys tulee olla varmistettu, ja mikäli tietoa katoaa, on sen oltava palautettavissa. Tähän varaudutaan esimerkiksi säännöllisillä varmuuskopioilla. Jos tietoa tarvitsee lopullisesti poistaa, tulee se tuhota aineiston tiedon kriittisyyteen sopivalla tavalla. (Hakala, Vainio & Vuorinen 2006, 11.) Tietoaineisto tulee myös arkistoida sisällön kriittisyyden mukaan (Vahti 2009a).

Jotta aineiston käsittely voidaan tehdä oikein, tulee sille asettaa sopiva luokitus ja käyttöoikeusrajoitukset. Tiedolla tulee olla omistaja, joka päättää tiedon luokituksesta, käytöstä ja jakelusta. (Vahti 2009a.)

2.2.5 Ohjelmistoturvallisuus

Ohjelmistoturvallisuuteen kuuluvat ohjelmistoihin liittyvät uhat. Ohjelmistoturvallisuuden edistämiseksi pyritään varmistamaan, että sovellus sopii siihen tarkoitettuun käyttöön, ja se on yhteensopiva muihin jo olemassa oleviin ohjelmistoihin. Sen lisäksi tulee varmistaa ohjelmistojen toiminnan luotettavuus ja virheettömyys. Varmistus tapahtuu esimerkiksi kattavalla testauksella. Jotta ohjelmistojen toimivuus voidaan taata, on ohjelmistojen päivittäminen ja lisenssien uusinta tärkeää. (Hakala, Vainio & Vuorinen 2006, 11 - 12.)

2.2.6 Laitteistoturvallisuus

Laitteistoturvallisuuden edistämiseen kuuluu tietokoneiden ja muiden tietojärjestelmään kytkettyjen laitteiden hallinta. Tämä tarkoittaa käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyviä toimia. (Vahti 2009b.) Toimia ovat muun muassa laitteiden tarkoituksenmukainen mitoitus, toiminnan testaus, huolto tai sen järjestäminen ja varaosien hankinta sekä varautuminen laitteiden kulumiseen. Itse laitteisiin liittyvien toimien lisäksi on arvioitava ja pyrittävä minimoimaan laitteiden käytöstä aiheutuvat loukkaantumisvaarat. (Hakala, Vainio & Vuorinen 2006, 12.)

2.2.7 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen turvallisuudesta. Näitä ovat esimerkiksi lähi- ja laajaverkkoyhteyksien sekä viestintäjärjestelmien turvallisuus. (Hakala, Vainio & Vuorinen 2006, 12.) Turvallisuutta edistäviin menetelmiin kuuluvat laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen (Vahti 2009c).

2.3 Dokumentaatio

Kunnollinen dokumentointi on tietoturvallisuuden edellytys. Dokumentointi helpottaa tietoturvan edistämisen lisäksi teknistä ylläpitoa, tietojen käsittelyä ja tietohallintoa. Usein dokumentit ovat kuitenkin puutteellisia, vanhentuneita tai puuttuvat kokonaan. (Hakala, Vainio & Vuorinen 2006, 32.) Tähän voi olla syynä henkilöstön tai budjetin vajavaisuus. Ongelmia syntyy myös, jos kukaan organisaatiossa ei huolehdi tietoturva-asioista kokopäiväisesti. (Andersson & Koivisto 2013, 45.)

Tietoturvallisuuden kannalta oleellisin dokumentti organisaatiolle on tietoturvasuunnitelma. Tietoturvasuunnitelma pohjautuu organisaation tietoturvapolitiikkaan, joka määrittelee organisaation linjaukset tietoturvallisessa toiminnassa. Tietoturvapolitiikka pohjautuu riskikartoitukseen, jonka avulla voidaan määritellä organisaation nykytila ja toiminnan hyvät ja huonot puolet. Tietojen perusteella suunnitellaan tietoturvapolitiikka, joka tukee

tietoturvallisuuden kehitystä organisaatiossa. Tietoturvapolitiikkadokumentti ei sisällä teknisiä yksityiskohtia, ja sen tulee olla julkinen asiakirja, jonka voi tarvittaessa jakaa kaikkien saataville. Dokumentti tulee olla kirjoitettu niin, että kuka tahansa lukija ymmärtää lukemansa. Tietoturvapolitiikka tulee hyväksyttää organisaation korkeimmalla tasolla. Tietoturvapolitiikkaa laatiessa tulee ottaa huomioon sitä koskevat standardit ja lainsäädäntö. Näitä ovat esimerkiksi ISO/IEC 27001 ja ISO/IEC 27002 sekä arkistolaki ja henkilötietolaki. (Andersson & Koivisto 2013, 34 - 38.)

Tietoturvasuunnitelmaan määritellään konkreettiset menetelmät ja toimet organisaation tietoturvan kannalta. Suunnitelma laaditaan yleensä muutaman vuoden aikavälille. Dokumentaatiota tulee kuitenkin päivittää esimerkiksi, jos järjestelmiin tulee muutoksia tai käyttöön otetaan uutta teknologiaa. Muutostarpeiden seuraamiseksi tietoturvasuunnitelma kannattaisi katselmoida vuosittain. Koska tietoturvasuunnitelma kuvaa yksityiskohtaisesti käytettyjä menetelmiä ja järjestelmiä, on se yleensä luottamuksellinen tai salainen. (Hakala, Vainio & Vuorinen 2006, 9.)

Jotta tietoturvasuunnitelmaa noudatettaisiin koko organisaatiossa, voidaan tehdä erillinen tietoturvaohje käyttäjiä varten. Hyvin laadittu suunnitelma voi itsessään toimia ohjeistuksena, mutta se sisältää usein turhan teknisiä yksityiskohtia rutiinityöhön. Tietoturvasuunnitelma on turha, jos sitä ei seurata. Ohjeistuksessa tulee olla käyttäjän työhön liittyviä esimerkkejä ja käytännönläheisiä ohjeita. Käyttäjiä voi motivoida noudattamaan ohjeita sisällyttämällä ohjeisiin, miksi ohje on annettu ja mitä ohjeiden noudattaminen merkitsee käyttäjälle itselleen. Ohjedokumentin tulisi olla luottamuksellinen tai salainen. (Hakala, Vainio & Vuorinen 2006, 10.)

Jatkuvuuden kannalta organisaatiolla tulee olla myös toipumissuunnitelma ja valmiussuunnitelma. Toipumissuunnitelman avulla varaudutaan tunnettuihin riskeihin. (Hakala, Vainio & Vuorinen 2006, 98.) Tietoturvasuunnitelmaa tehdessä tulee tehdä riskianalyysi. Analyysin perusteella riskeiltä tulee suojautua, mutta kaikilta riskeiltä ei voi täysin suojautua ja suojautumisen jälkeenkin uhka voi toteutua. (Hakala 2006, 79.) Toipumissuunnitelma on ohjeistus, miten tulee toimia määrittelyvaiheessa löydettyjen riskien realisoituessa ja sellainen tulisi olla jokaista organisaation tietojärjestelmää kohti. (Hakala, Vainio & Vuorinen 2006, 98.)

Tietoturvallisuuden käsikirjan mukaan toipumissuunnitelmassa on hyvä käsitellä seuraavat asiat (Hakala, Vainio & Vuorinen 2006, 98.):

- Miten eri riskien realisoituminen havaitaan?
- Mihin muihin tietojärjestelmiin tapahtumalla on vaikutus?
- Miten organisaatiota ja sidosryhmiä informoidaan tapahtuneesta?
- Ketkä tarvitsevat tiedon tapahtuneesta?
- Mitä välittömiä vaikutuksia tapahtumalla on?
- Mitä välillisiä vaikutuksia tapahtumalla on?
- Mitä toimenpiteitä tarvitaan vahinkojen minimoiseksi?
- Mitä on tehtävä lisävahinkojen estämiseksi?
- Mitä henkilöresursseja toipumiseen tarvitaan ja miten työt jaetaan?
- Mitä aineellisia resursseja tarvitaan?
- Kuinka paljon toipumiseen tarvitaan aikaa?

Valmiussuunnitelmalla varaudutaan eri poikkeustilanteiden ja kriisien, kuten ympäristökatastrofeihin, taloudellisiin poikkeusoloihin tai sodan uhkan, vaikutuksiin organisaation toiminnan jatkumiselle (Hakala, Vainio & Vuorinen 2006, 99). Koska toimeksiantajana toimiva osakunta ei ole tuottoa hakeva organisaatio ja perustuu vapaaehtoistyölle eli sillä ei ole työllistävää vaikutusta, ei tässä työssä kuvata valmiussuunnitelmaa tarkemmin.

3 Tietoturva opiskelijajärjestötoiminnassa

Tietoturvallisuudesta saatavan tiedon hyödyntäminen pienimuotoiseen järjestötoimintaan ei ole täysin yksinkertaista. Ohjeita on yksityishenkilön arjen tietoturvaan sekä oman tietosuojan takaamiseen ja toisaalta yritysten tietoturvan toteuttamiselle. Vaikka järjestöllä ei olisi samanlaista organisaatiorakennetta kuin yrityksillä, voidaan vastuualueet jakaa järjestön toimijoiden kesken ja seurata yrityksille suunnattua teoriaa soveltaen.

3.1 Opiskelijajärjestöt

Opiskelijajärjestöt ovat opiskelijoiden vapaaehtoistoimintaan perustuvia yhdistyksiä tai lain määrittämiä julkisyhteisöjä, joiden jäseneksi liittyvät kyseessä olevaa järjestöä koskevan laitoksen, aineen tai kanta-alueen opiskelijat. Tällaisia ovat esimerkiksi ylioppilashallitukset, opiskelijakunnat, ainejärjestöt ja osakunnat. Nämä järjestöt kokoavat opiske-

lijat yhteen, järjestävät tapahtumia ja aktiviteetteja sekä pyrkivät edistämään opiskelijoiden asemaa pitämällä yhteyttä laitoksien hallintoon ja ympäröivään yhteiskuntaan. (Wikipedia 2017.)

Järjestötoiminta perustuu usein vapaaehtoistyölle. Opiskelijajärjestöissä toimiminen lopetetaan usein opintojen päättyessä ja työelämään siirtyessä. On mahdollista, että opiskelijajärjestöissä on myös muutama palkallinen työntekijä, mutta pääasiassa opiskelijajärjestöissä toimivien henkilöiden vaihtuvuus on tiheää. Tällöin perehdytys on kriittisen tärkeää, jotta inhimillisten virheiden uhka saadaan pidettyä minimissä. Toimijoiden vaihtuessa pitää ottaa myös huomioon, että edeltävälle henkilölle voi jäädä järjestölle tietoturvallisuuden kannalta tärkeää tavaraa ja tietoa. Vaihtoprosessissa tulee järjestölle kuuluvat tavarat palauttaa, kuten annetut laitteet ja avaimet, sekä käyttöoikeudet ja mahdolliset siirtyvät salasanat tulee päivittää.

3.2 Jäsenrekisteri

Opiskelijajärjestöt koostuvat jäsenistä, jolloin jokaisella järjestöllä tulisi olla jäsenrekisteri jossain muodossa. Järjestön koosta ja resursseista riippuen jäsentiedot voivat olla sähköisessä muodossa, esimerkiksi tietokannassa tai Excelissä, tai paperisena arkistona muun muassa hakemuslomakkeiden tai matrikkelin muodossa. On myös mahdollista, että jäsentietoja säilytetään monessa muodossa, esimerkiksi jos tiedot on mahdollista antaa paperisen hakemuslomakkeen kautta ja siitä ne siirretään sähköiseen muotoon.

Jäsenrekisteriä ylläpidettäessä on otettava huomioon lain asetukset. Henkilötietolaissa on asetettu, että rekisterinpitäjällä on velvollisuus määritellä rekisterin tarkoitus ja käyttö etukäteen, huolehtia tietojen oikeellisuudesta, huolehtia rekisterin ja sen tietojen asianmukaisesta suojaamisesta, mahdollistaa rekisteröidylle häntä koskevien tietojen tarkistus sekä noudatettava tietojen keräämisessä, tallentamisessa, käyttämisessä ja luovuttamisessa näitä asioita koskevia erillisiä säädöksiä. Laissa on myös säädetty, että henkilötietoja ei saa luovuttaa Euroopan unionin ulkopuolelle, ellei kohdemaassa voida taata riittävä tietosuojan taso. Mikäli jäsenrekisteri on sähköisessä muodossa, rekisteristä on laadittava rekisteriseloste, joka on kaikkien saatavilla. Rekisteriselosteen tulee sisältää rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot, henkilötietojen käsittelyn tarkoitus, kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä, mihin tietoja säännönmukaisesti luovutetaan sekä kuvaus rekisterin

suojauksen periaatteista. Jäsenrekisteri ja sen kautta sen sisältämät henkilötiedot tulee suojata asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä. (Finlex 1999.)

Jäsentietojen säilytystavoissa on hyvät ja huonot puolensa niin tietoturvan kuin yleisten käytäntöjen kannalta. Säilytystavassa tulee ottaa huomioon seuraavia asioita, jotka ovat osittain tärkeitä lain noudattamisen takia.

Kuten on kerrottu, tietojen tulee olla vain oikeutettujen henkilöiden saatavilla, mutta sen lisäksi täytyy varmistaa, että oikeutetuilla henkilöillä on myös helppo pääsy tietoihin. Jotta pääsy on vain oikeutetuilla henkilöillä, tulee säilytettyjen tietojen olla lukon tai salasanan takana. Tähän soveltuvat siis kaikki säilytystavat, sillä uhkana ovat murrot, ovat ne sitten hakkerointeja tai tiirikointeja. Molemmat, sekä avain että salasana, voivat myös kadota tai unohtua. Toisaalta salasanalle on yleensä tarjolla turvallinen palautuskeino, mikäli tietoja säilytetään jonkin palveluntarjoajan rekisterisovelluksessa. (Nevala 2014.) Salasanan unohtuminen on vakavampi vahinko, mikäli kyseessä on salasanalla kryptattu tiedosto, jolloin samanlaista palautuspalvelua ei ole tarjolla.

Säilytystavalla on enemmän merkitystä, kun mietitään, kuinka oikeutetut henkilöt pääsevät tietoihin helpoiten käsiksi. Jos tiedot ovat paperisena sijainnissa, jonne vain yhdellä henkilöllä on pääsy, on muiden oikeutettujen vaikeaa päästä katsomaan ja tarvittaessa muokkaamaan niitä. Tällaisia paikkoja ovat esimerkiksi lukollinen kaappi, jonne on vain yksi avain, tai yksityinen asunto. Jos vain yksi henkilö on vastuussa jäsenrekisteristä, on paperinen muoto silti hankala, koska tiedot eivät saata olla käsillä tarvittaessa. Jos tietoja säilytetään esimerkiksi Excel-muodossa yksityisellä koneella, vastaava henkilö ei pääse tietoihin käsiksi, mikäli tietokone on pysyvästi tai jäänyt eri sijaintiin, jossa kyseinen henkilö on. Tietoihin pääsyn kannalta verkossa tarjottava rekisteripalvelu tai pilvipalvelu, jonka käyttö on salasanan takana, olisi paras ratkaisu. Tiedon tulee olla myös ajantasaista, joten koska parempi saatavuus helpottaa muokkaamista, on tietojen ajan tasalla pitäminenkin helpompaa. Palveluntarjoajilla saattaa olla myös ratkaisuja, joilla rekisterissä oleva jäsen pääsee itse tarkastelemaan ja muokkaamaan omia tietojaan verkossa. On kuitenkin otettava huomioon, että kaikilla tarvittavilla henkilöillä on tieto käyttäjätunnuksistaan ja kuinka palvelua käytetään. (Nevala 2014.)

Nettipalvelu voisi olla myös paras tapa tietojen katoamisen ja tuhoutumisen uhan minimoimiseksi. Paperinen arkistoinnin uhkana ovat tulipalot, vesivahingot tai inhimillinen virhe, kuten juoman kaataminen paperille niiden kanssa työskennellessä. Paikallisella koneella säilyttäessä uhkana on laitteen hajoaminen ja mahdollisesti sen johdosta tallennettujen tiedostojen ja tietojen menettäminen. Mikäli jäsenrekisteriä päätetään säilyttää verkossa, on tietenkin otettava huomioon palvelun luotettavuus ja tiedetyt tietoturvapoikkeukset. (Nevala 2014.) Verkossa säilytettävän jäsenrekisterin uhkana on myös tietojen leviäminen EU:n ulkopuolelle. Tieto ei olisi enää vain lokaalisti Suomessa vaan tietoturvapoikkeuksen tai hakkeroinnin sattuessa tieto voi levitä maailmalle. Tarkistettava on myös pilvipalvelujen palveluntarjoajan omistusoikeudet tietoihin. Vahinkoa ei käy, mikäli verkossa säilytettävä tieto ei ole yhdistettävissä suoraan henkilöihin vaan nimien sijaan tietoa voidaan hakea esimerkiksi identikoivan numeron avulla. Tällaisia ovat esimerkiksi jäsen- tai opiskelijanumero.

Verkossa tarjottujen palvelujen hyöty saattaa kuitenkin olla haittoja suurempi. Jotta tieto pysyisi kiistämättömänä, tulee muokkaamisesta olla merkintä, kuka tietoa on muokannut. Näin muokkaaja ja syy voidaan jäljittää, jos tiedot eivät ole oikein. Jos vastuuhenkilöitä, joilla on oikeus muokata jäsenten henkilötietoja, on vain yksi, voidaan olettaa, että muokkaaja on aina sama. Kuitenkin on vaikea todistaa, että esimerkiksi arkistonavain on ollut viimeisenä kyseisen henkilön hallussa. Muokkaushistoriaa voidaan tietenkin pitää paperisen ja Excel-muotoisen jäsenrekisterin kohdalla manuaalisesti, mutta sen päivittäminen muokkauksen yhteydessä voi helposti unohtua ja merkinnät on helppo väärentää. Jäsentietojen ylläpitoon tarkoitetut palvelut pitävät usein automaattisesti muokkaushistoriaa, jota ei voi itse muokata. Merkinnät perustuvat siihen, että muokkaajan tiedot otetaan sisään kirjautuneelta käyttäjältä. (Nevala 2014.) Vertailun pohjalta suurin riski verkkopohjaisissa palveluissa tietoturvapoikkeusten lisäksi on, ettei käyttäjä kirjaudu toimien jälkeen ulos ja poistuu koneen ääreltä, jolloin asiaton henkilö saattaa päästä katsomaan ja muokkaamaan tietoja. Tällöin edes automaattinen muokkaushistoria ei auta.

3.3 Tiedottamistavat

Nykypäivänä on tavallista, että opiskelijajärjestöillä on toiminnasta tiedottamista varten omat verkkosivut, sähköpostilista ja tilejä erilaisissa sosiaalisissa medioissa, kuten Facebook, Instagram, Twitter ja/tai Snapchat.

Verkkosivujen tietoturvauhkana ovat erilaiset hyökkäykset. Sivuille voidaan hakkeroitua, jotta sille saadaan näkyville poliittinen mielipide tai mainosviestejä. Opiskelijajärjestöjen toiminta on usein niin pientä, että hyökkäys ei todennäköisesti ole suoraan järjestöä kohtaan, vaan kohde on valikoitunut tietoturva-aukon takia. Hyökkäyksen motiivina voi olla myös käyttäjätietojen kerääminen rikollisten toimesta, mutta järjestöillä on vähän käyttäjiä sivustoille ja käyttäjätiedot eivät yleensä sisällä hyödyllisiä henkilötietoja, kuten yhteys- tai luottokorttitietoja. (Kanava.to 2014.)

Sivujen ylläpitoon voidaan käyttää sisällönhallinta- ja julkaisujärjestelmää, kuten WordPress ja Joomla!, ja nämä valikoituvat hyökkäyksen kohteiksi, koska niillä on haavoittuvuuksia, joita voidaan hyödyntää laajalla skaalalla. Esimerkiksi järjestelmään voidaan kohdentaa brute force -hyökkäys, jossa automaattisesti syötetään järjestelmähallinnan kirjautumislomakkeelle yleisiä käyttäjätunnusyhdistelmiä, kuten admin / admin, ja koitetaan päästä arvatulla yhdistelmällä sisään. Verkkosivujen tietoturvasta huolehtiessa tulee huomioida, että verkkosivujen julkaisuun käytettyjen järjestelmien päivitykset ovat ajan tasalla ja asetuksissa on mahdollisuuksien mukaan määritelty sallittujen kirjautumisyrityksien määrä tietyllä aikavälillä ja piilotettu järjestelmän versiotiedot julkaistulta sivulta. (Kanava.to 2014.)

Sähköpostilistojen avulla tiedotteet saa yhdellä lähetyksellä toimitettua kaikille listalla oleville jäsenille. Siksi opiskelijajärjestöt liittävät jäsenensä tai kertovat, kuinka liittyä omalle sähköpostilistalleen. Sähköpostilistoja ja niiden hallintaa tarjoavia palveluita on monia. Sähköpostilistojen kohdalla on tärkeintä, ettei välitä roskapostia jäsenille. Tämän takia kannattaa valita palvelu, joka ei päästä kaikkia viestejä suoraan läpi. Järjestön sisältä voidaan valita sähköpostilistasta vastaava henkilö joka hallinnoi viestejä tarjotusta hallintapaneelista. Osalta sähköpostilistoilta viestit, jotka on lähettänyt joku listalla olevista, lähtevät heti listalla oleville, mutta ulkopuoliset viestit tulee hyväksyä. Tämä ei kuitenkaan takaa, ettei listalle pääse henkilö, joka lähettää roskapostia, mutta todennäköisyys, että huijausviestejä päätyy jäsenille, on pienempi. Sähköpostilistan hallinnointi käyttäjätunnukset tulee pitää muiden käyttäjätunnusten tavoin hyvässä tallessa ja vain tarpeellisten henkilöiden tiedossa, ettei kukaan pääse aiheuttamaan haittaa suoraan hallintapaneelin kautta.

Järjestöt käyttävät myös sosiaalista mediaa eli somea ajankohtaisten tiedotteiden jakamiseen ja tapahtumista tiedottamiseen. Se on myös hyvä tapa saada näkyvyyttä järjestöille ja sitä kautta saada uusia jäseniä. Kuvilla välitetään, mitä toimintaa järjestöllä on ja millainen tunnelma tilaisuuksissa on.

Petteri Järvinen on kirjassaan Arjen tietoturva kirjoittanut, että sosiaalinen media ja tietosuoja ovat täysin vastakkaisia käsitteitä, sillä some perustuu tiedon jakamiseen ja tietosuoja sen piilottamiseen (Järvinen 2012, 294). Järjestöt luovat kuitenkin mahdollisuuksien mukaan yritystilejä tai jos tili luodaan jonkun järjestössä toimivan nimiin, voi käytössä olla opiskelijajärjestön toimintaa varten luotu sähköposti. Käyttäjätiedoissa tai jaetussa sisällössä ei tulisi siis olla henkilötietoja. Tietoturvan merkitystä sosiaalisen median käytössä tässä tapauksessa ei kuitenkaan saa unohtaa. Julkaisuja tekee järjestössä toimiva henkilö ja inhimillisiä virheitä voi tapahtua.

Julkaisuja tehdessä tulee harkita, antavatko ne jotain tietoa järjestön jäsenistä tai toiminnasta, jota joku voi käyttää laittomalla tavalla hyödyksi. Valokuvia jakaessa, etenkin jos kuviin merkitään jäseniä, tulee varmistaa, että henkilöt haluavat olla kuvissa. Julkaisuissa ei saa levittää jäsenten henkilötietoja. Nimien sisältyminen on kuitenkin yleistä. Esimerkiksi opiskelijajärjestön sisäisissä vaaleissa ehdokkaat halutaan asettaa näkyville mahdollisimman monessa kanavassa, ja jos joku jäsenistä on saanut kunniamaininnan tai palkinnon, saatetaan häntä onnitella. Myös järjestön yhteyshenkilöitä halutaan esitellä. Koko nimeä käytettäessä on hyvä olla asianomaisen suostumus. Muiden henkilötietojen jakamista tulee harkita tarkkaan ja pyytää lupa asianomaiselta. Tarvittaessa jaettavia tietoja ovat yleensä aktiivisten toimijoiden puhelinnumerot ja sähköpostit. Nämä voivat olla yksityisiä, jollei järjestöllä ole tarjota niitä toiminnan ylläpitämiseen. Sosiaalisen median tileiltä tulee muistaa kirjautua ulos käytön jälkeen.

4 Tietoturvasuunnitelman toteutus

Tämän työn toimeksiantona on toteuttaa teorian pohjalta tietoturvasuunnitelma Wiipurilaiselle osakunnalle. Seuraavassa esitellään toimeksiantajana toimiva järjestö ja sen nykytila tietoturvan näkökulmasta. Tähän sisältyvät hallinnoitavat tiedot ja niiden säilytys, käytetyt palveluntarjoajat ja ohjelmistot, henkilöstö, laitteet ja tilat. Luvussa kerrotaan

myös toiminnan tietoturva riskeistä, joiden avulla toteutetaan osakunnalle tieturvapolitiikka ja sen pohjalta tietoturva- ja toipumissuunnitelma.

4.1 Toimeksiantajan nykytila ja tarpeet

Wiipurilainen osakunta (WiO) on opiskelijajärjestö, joka kuuluu Helsingin yliopiston alaisuuteen. Osakunnat pyrkivät edistämään opiskelijoiden, jotka ovat usein opiskelupaikkakunnan ulkopuolelta, sosiaalisia oloja sekä tukemaan ja kehittämään jäsentensä henkisiä harrastuksia (Finlex 2009). Jäsenet on ennen kerätty opiskelijan kanta-alueen perusteella eli missä hän on kirjoittanut ylioppilaaksi, mutta nykyisin kotipaikkakunnalla ei ole väliä.

WiO:lla on itsehallinto ja jäsenistä, hallinnosta, taloudenpidosta ja muusta toiminnasta määrätään osakunnan säännöissä. Jäsenet ovat velvollisia maksamaan jäsenmaksun vuosittain joko Helsingin ylioppilaskunnan lukuvuosi-ilmoittautumisen yhteydessä tai yliopiston ulkopuolisten jäsenten tapauksessa suoraan osakunnan tilille. Maksuvelvollisuudesta määrätään myös virallisissa säännöissä. Jäsenet kirjaavat nimensä, tiedekuntansa, lukionsa ja valmistumisvuotensa osakunnanmatrikkeliin. Jokainen uusi jäsen täyttää jäsenlomakkeen, joka arkistoidaan. Arkistoon menevät myös ulkojäsenenhakemukset, jotka vaaditaan Helsingin yliopiston ulkopuolisilta opiskelijoilta. Jäsenistä kerätään lomakkeilla seuraavat tiedot: nimi, syntymäpaikka ja -aika, osoite, puhelinnumero, sähköpostiosoite, vakituinen osoite, ylioppilaaksitulovuosi ja -koulu, tiedekunta ja pääaine, harrastukset, luottamustehtävät muissa järjestöissä ja osakuntaan tulovuosi. Lomakkeen yhteydessä pyydetään myös suostumus liittämisestä WiO:n sähköpostilistalle.

Lukuvuosi-ilmoituksen yhteydessä maksaneista jäsenistä pyydetään sihteerin toimesta Excel-muodossa lista vuosittain. Koska lista ei sisällä jäseniä, jotka ovat suorittaneet tilisiirron, ei tätä tiedostoa voida pitää jäsenrekisterinä. WiO:n jäsentiedot ovat kokonaisuudessaan paperisessa muodossa. WiO on muihin opiskelijajärjestöihin verraten pieni, joten jäsenten tietojen säilyttäminen ja hallinnointi on helpompaa.

4.1.1 Palveluntarjoajat

Kaikki uudet jäsenet lisätään WiO:n sähköpostilistalle, jota ylläpidetään Majordomo-ohjelmistolla. Sähköpostilista on luotu Helsingin yliopiston listaksi ja sitä voivat hallita vain

Helsingin yliopiston tunnukset omistavat henkilöt. Sähköpostilistan ylläpitäjänä toimii WiO:n neuvoston sihteeri. Mikäli sihteeri on ulkojäsen eli jonkun muun oppilaitoksen kuin Helsingin yliopiston opiskelija, määrätään tehtävään joku toinen, kuten varakuraattori.

WiO:lla on verkkosivut www.wiipurilainenosakunta.fi, joilla on tietoa osakunnasta. Sisältöön kuuluvat muun muassa ajankohtaiset ilmoitukset, tietoa liittymisestä, toiminnasta ja tapahtumista sekä yhteystiedot ja sijainti. Verkkosivujen julkaisualustana käytetään WordPressiä. Se on ilmainen ja ylläpito voidaan hoitaa verkkoselaimella. Osakunnan verkkosivuilta pääsee myös selaamaan kuvia tapahtumista. Valokuvien näyttämiseen on käytetty verkkoselain pohjaista Gallery Open Source -sovellusta.

Verkkosivut ovat julkiset, mutta osakunnan sisäiseen tiedon säilyttämiseen käytetään Dokuwikiä, ilmaista Open Source -wikisovellusta. Sisältöön kuuluu perehdytysmateriaalia virkailijoille, vinkkejä ja sääntöjä. Varakuraattori hallinnoi käyttäjätunnuksia, jotta vain asianomaisilla on pääsy materiaaleihin.

WiO:lla ei ole omaa palvelinta, vaan kiintolevytila on hankittu webhotellin muodossa Zonerilta. Edeltävien ohjelmistojen ollessa ilmaisia tämä on ainoa maksullinen palvelu, joka osakunnalla on käytössä verkkopuolella. Webhotellipalvelussa on kotisivutila, sähköpostipalvelu, oma verkkotunnus, tietokantoja ja hallintapaneeli, jonka avulla hallinnoidaan webhotellin toimintoja ja ominaisuuksia. Vaikka WiO:n virallinen sähköpostilista on luotu Majordomossa, on osakunnan seniorijäsenten sähköpostilista tehty webhotellin kautta ja sitä hallinnoidaan webhotellin käyttöliittymältä.

Jokaisen palveluntarjoajan kohdalla on omat tietoturvauhkansa ja sovelluksissa mahdollisia tietoturvapoikkeuksia. Nämä jätetään kuitenkin tietoturvasuunnitelman ulkopuolelle ja keskitytään käyttäjätilien hallinnointiin ja uusimiseen liittyviin riskeihin sekä inhimillisistä virheistä johtuvaan sisällön katoamiseen ja sen palauttamiseen varmuuskopioista tai palveluntarjoajien palveluiden avulla.

4.1.2 Tilat ja laitteisto

Wiipurilainen osakunta toimii Domus Gaudiumin osakuntahuoneistossa, joka sijaitsee keskeisellä paikalla Helsingissä. Tilat sijaitsevat huoneiston kellarikerroksessa. Katutason ulko-ovet ovat lukollisia ja niistä kulkevat kaikki rakennuksen toimijat. WiO jakaa toimitilansa kahden osakunnan ja muutaman muun järjestön kanssa. Domus Gaudiumin

osakuntahuoneiston hallinnasta ja käytöstä vastaa DG:n osakuntien yhteinen huoneistotoimikunta (HTK), jonka virat jaetaan osakuntien kesken siten, että jokaisesta tilojen osakunnasta on edustajia toimikunnassa. Osakuntatiloihin on kaksi ovea, jotka pidetään aina lukittuina. Oven saavat auki järjestöjen toimijat, jotka ovat hakeneet kulkulupaa ja se on hyväksytty. Kulkuluvat ladataan opiskelija- tai matkakorteille ja ne on jaettu päivälupiin (8 -22) ja vuorokausilupiin (24 h). Kulkuluvattomat pääsevät sisään soittamalla ovisummeria ulko-ovella ja tarvittaessa vielä tilojen sisäänkäynnillä. Tapahtumien aikana sisään päästetään tilaisuudesta riippuen henkilöt, joilla on näyttää opiskelijakortti tai osakuntatarra ja heidän seuralaisensa.

Tilat koostuvat aulasta, salista, lehtihuoneena toimivasta oleskelutilasta, keittiöstä ja toimistosta. Toimiston ovi on lukollinen, sillä siellä säilytetään järjestöjen asiadokumentteja ja arvotavaroita. Toimistossa sijaitsee myös yhteiskäyttöinen pöytätietokone ja tulostin. Pöytäkoneen lisäksi tiloissa on kannettavatietokone niin ikään yhteiskäyttöön ja sitä säilytetään lehtihuoneessa numerolukolliseen vaijeriin kiinnitettynä. Tiloissa on langaton verkkoyhteys, jonka kirjautumistiedot ovat saatavilla lehtihuoneen ilmoitustaululta.

4.1.3 Virkailijat

Wiipurilaisen osakunnan toimintaan osallistutaan hakemalla virkoihin ja toimikuntaan kerran vuodessa (Wiipurilainen Osakunta 2017a). Pääasiallisesti virkakausi on vuoden muutamaa poikkeusta lukuun ottamatta. Kahden vuoden virkoja ovat muun muassa kuraattorin, taloudenhoitajan ja Willin päätoimittajan virat. (Wiipurilainen Osakunta 2017b.) Virkoihin voivat hakea sekä vanhat ja uudet jäsenet. Virat voivat siis vaihtua jäsenten kesken tai joku voi uusia virkansa, mutta kaiken kaikkiaan vaihtuvuus on tiheää.

Tietoturvan osa-alueiden vastuut ovat tällä hetkellä tietoisesti ohjaamatta jakautuneet karkeasti seuraavasti: Hallinnollisesta turvallisuudesta eli tietoturvan hallinnoinnista ja yhteydenpidosta eri tietoturvavastaaviin vastaa kuraattorin johtama neuvosto. Fyysisestä turvallisuudesta eli tiloista ja laitteista vastaa HTK yhdessä kiinteistöhuollon, vartiointiliikkeen ja HYY:n kanssa. Henkilöturvallisuudesta tietoturvan kannalta vastaavat virkailijat perehdyttämällä omat seuraajansa sekä verkkovastaava kouluttamalla ja tukemalla tarvittaessa ohjelmistojen käytössä. Tietoaineistoturvallisuudesta vastaa jäsentietojen osalta sihteeri, arkistoinnin osalta arkiston- ja kirjastonhoitaja ja sähköisistä varmuuskopioista verkkovastaava. Ohjelmistoturvallisuudesta vastaa verkkovastaava, laitteistoturvallisuudesta ja tietoliikenneturvallisuudesta vastaa HTK.

Verkkovastaava toimii ohjelmistojen ylläpitäjänä ja vastaa teknisestä hallinnoinnista. Kuten mainittu Verkkovastaava auttaa järjestön toimijoita ja tarvittaessa jäseniä ohjelmistojen käytössä. Verkkovastaava hoitaa yhteydenpidon palveluntarjoajiin ja valvoo, että lisenssit ja päivitykset ovat ajan tasalla. Verkkovastaavan virkakausi on vuoden pituinen. Verkkosivujen ja sosiaalisen median sisällöstä vastaa tiedotusneuvos. Tarvittavilla virkailijoilla on käyttäjätunnukset Wordpress-, Dokuwiki- ja Gallery -sovelluksiin. Sosiaalisen median tileille on yksi tunnus joka tilille, jotka on jaettu tiedotusneuvoksen harkinnanvaraisesti tiedotustoimikunnalle. Tällä hetkellä WiO:lla on sosiaalisen median tilit sovelluksissa Facebook, Instagram ja Snapchat.

4.2 Tietoturvallinen toiminta ja riskienhallinta

Toimeksiantajan organisaatiolla ei aiemmin ole ollut tietoturvasuunnitelmaa eikä riskejä oltu kokonaisvaltaisesti kartoitettu. Jotkut asiat hoidetaan tietoturvan periaatteiden mukaisesti kokemuksen ja muilta saatujen mallien mukaan. Asiapaperit, arvotavarat ja kassat pidetään lukkojen takana. Tilojen ovissa on lukot asiattoman oleskelun välttämiseksi ja ne tulee pitää lukittuina tai tapahtumien aikaan tulee olla kulunvalvonta. Keittiössä on yksi yhteinen katkaisin lämpölaitteille tulipalon riskin pienentämiseksi. Vuonna 2016 HTK laati turvallisen tilan ohjeistuksen HYY:n antamasta aloitteesta. Siinä keskitytään siihen, miten tiloissa saa käyttäytyä ja miten toimia, jos havaitsee epäilyttävää käytöstä. Ohjeistuksesta on tiedotettu kaikkia tilan toimijoita ja ne on asetettu esille tilojen seinille. Ohjeet rajoittavat luvattomien ja haitallisten henkilöiden oloa tiloissa. Tiloissa on myös esillä hätänumerot sekä vartiointiliikkeen yhteystiedot.

Koska riskianalyysiä ei ennalta ollut ja tietoturvadokumenttien tulisi pohjautua riskikartoitukseen, toteutettiin sellainen pienimuotoisesti järjestön toiminta, tilat ja laitteisto huomioon ottaen (liite 1).

Uhat liittyivät pääasiassa ihmisten käytökseen, teknisiin vikatilanteisiin ja onnettomuuksiin. Riskejä voi hallita eli uhkien toteutumista voidaan ennalta ehkäistä ja jos riskeihin on varauduttu, voi niiden tuottamat vahingot pitää minimissä ja toipuminen tapahtuu nopeammin.

Tärkeintä on varautua tietosisällön säilymiseen. Verkossa olevat tiedot voidaan turvata varmuuskopioita ottamalla ja pitämällä ohjelmistot ajan tasalla. Varmuuskopiointi ja päivitysten tarkistus tulee suorittaa säännöllisesti. Parhaiten tämä toteutuu määrittelemällä toiminnoille säännöllinen aikaväli.

Inhimillisiä virheitä voidaan vähentää asianmukaisella koulutuksella ja ohjeistuksella. Tämä toteutuu hyvällä perehdytyksellä. Perehdytykseen sisältyy virkaan liittyvä koulutus ja sen yhteydessä tulee varmistaa, että perehdytettävä tietää ohjeistuksien sijainnit, hänellä on pääsy sinne ja hän lukee ne. Jotta verkossa olevaan tietoon ei ole asiattomilla henkilöillä pääsyä, virkailijoiden perehdytykseen pitää myös sisällyttää eteenpäin siirtyvien käyttäjätunnuksien salasanojen vaihto. Salasanan tulee olla vahva eli mahdollisimman pitkä, suositus yli kahdeksan merkkiä, ja sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Salasana tulisi vaihtaa yleisien suositusten mukaan kolmen kuukauden välein, mutta ainakin viran vaihtuessa tulee salasana uusia, jotta vain virassa olevalla on pääsyoikeudet kyseiselle käyttötilille. Tämä pienentää väärinkäytön riskiä ja edistää muutoshistorian paikkaansa pitävyyttä esimerkiksi verkkosivuilla.

Ulkopuoliset voivat päästä käyttäjätileille myös inhimillisen huolimattomuuden takia. Käyttäjätileiltä ja hallintapaneeleista pitää aina kirjautua ulos heti, kun lopettaa käytön. Konetta ei saa jättää valvomatta ollessa kirjautuneena jossain, missä on osakunnan sisältöä tai jos käsittelee jäsenten henkilötietoja. Uloskirjautumisen jälkeen tulee sivuhistoria tyhjentää julkisilla, mukaan lukien osakunnan tiloissa sijaitsevilla, koneilla työskennellessä. Jäseniä tulee ohjeistaa samoin myös tilanteissa, joissa he kirjautuvat yksityisille tileilleen (sähköposti, some, verkkopankit) osakunnan yhteiskäyttöisillä koneilla.

Tiloihin ja laitteisiin liittyvät riskit ovat HTK:n vastuulla. Vikatiloja voidaan estää laitteistojen säännöllisellä tarkistuksella ja huollolla. Varkauksia voidaan rajoittaa varmistamalla lukkojen toimivuus. Kaikkia toimijoita tulee myös ohjeistaa pitämään ovet lukittuina, jotta esimerkiksi jäsentietoja sisältävät asiakirjat säilyvät tallessa. Hyvällä ohjeistuksella voidaan vaikuttaa myös siihen, että paperinen jäsenrekisteri pysyy omalla paikallaan ja näin ollen tallessa ja asianomaisten saatavilla.

4.3 Toteutetut dokumentit

Riskikartoitus kirjattiin taulukkomuodossa (liite 1). Sen jälkeen lähdettiin toteuttamaan sen pohjalta, ja Anderssonin ja Koiviston teoksen ”Tietoturvaa toteuttamassa” tietoturvapolitiikan sisältöä mukaillen, Wiipurilaisen Osakunnan tietoturvapolitiikka-asiakirjaa (liite 2). WiO:n tietoturvapolitiikka sisältää tietoturvapolitiikan tavoitteet, tietoturvallista toimintaa ohjaavat tekijät, tietoturvan merkityksen osakunnalle, kuvauksen vastuiden jakautumisesta ja kuinka tietoturvallista toimintaa valvotaan sekä linjauksen ohjeistuksista, koulutuksesta ja tiedottamisesta. Politiikkaan tuli sisällyttää, että WiO sitoutuu tietoturvaan ja jäsentietoihin liittyvien säädöksien noudattamiseen. WiO linjaa politiikkassa, että virkailijat vastaavat omien vastuualueidensa tietoturvallisesta toiminnasta, koulutusta järjestetään perehdytyksien yhteydessä vuosittain ja valvontaa suoritetaan päivittäisen toiminnan ohessa sekä riskikartoituksia ja auditointia tehdään tarvittaessa neuvoston koordinoimana. Tietoturvapolitiikan tulee olla neuvoston hyväksymä, ja sen jälkeen se on vapaasti jaettavana ja julkaista WiO:n verkkosivuilla.

Tietoturvapolitiikan dokumentoinnin jälkeen siirryttiin yksityiskohtaisempaan tietoturvasuunnitelmaan (liite 3). Asiakirjan jaottelu päädyttiin tekemään tietoturvan osa-alueittain. Sisältöön lisättiin myös omat kohtansa vastuualueiden jakautumiselle eritahoille ja kehityskohteille, jotka vaativat tietoturvaa parantavia toimia tulevaisuudessa. Lopuksi lisättiin toipumissuunnitelmat eri tilanteille, jolloin ennustetut riskit ovat toteutuneet. Toipumissuunnitelman pohja pyrittiin suunnittelemaan niin, että dokumentti vastaa aiemmin teoriassa esiteltyihin kysymyksiin, jotka ovat oleellisia WiO:n kannalta. Suunnitelmassa pyrittiin kuvaamaan tietoturvan osa-alueiden sisältöä ja nykytilaa lyhyesti ja selkeästi, sekä antamaan helposti noudatettavia ohjeita tietoturvalliseen toimintaan. Seuraavassa on keskeisimpiä asioita, joita tieturvasuunnitelmaan sisällytettiin.

Hallinnollinen turvallisuus on tavallisen tapaan organisaation johdon eli WiO:n neuvoston vastuulla. Alueen osalta todettiin riittäväksi kirjata vastuu taho ja luettelemaan hallintaan kuuluvaksi toiminnan valvonnan, tietoturvan kehittämisen ja korjaavien sekä kehttävien toimien koordinoinnin.

Kuten aiemmin on kuvattu, WiO:n jäsentiedot on kerätty kansioon ja niiden tulee aina olla lukkojen takana. Tämä tieto ja jäsentietoihin liittyvää ohjeistusta sisällytettiin tietoaineistoturvallisuusosioon. Toipumissuunnitelmassa otettiin kantaa jäsentietojen palauttamiseen. Mikäli jäsentiedot katoavat tai vahingoittuvat, voidaan Helsingin yliopiston kautta

kirjautuneista jäsenistä saada tiedot sihteeriltä, tai jos nämä tiedot vahingoittuvat, voidaan ne pyytää uudelleen. Loput tiedot on jossain määrin mahdollista kerätä itse jäseniltä sähköpostilistalle välitetyn tai puuteiden kartoituksen jälkeen asianomaisille suoraan lähetetyn ilmoituksen avulla. Katoamisesta tilanteessa on joka tapauksessa tiedotettava jäseniä, mikäli on syytä epäillä, että tiedot ovat joutuneet asiattomille henkilöille.

Käytetyistä tietoteknisistä palveluista vastaa osakunnalla verkkovastaava. Verkkosivuista, gallerian sisällöstä ja tietokannasta tulee ottaa varmuuskopiot säännöllisesti. Näin toimitaan, jotta sisällöt voi vikatilanteessa palauttaa. Palautus tehdään Zonerin palvelimelle purkamalla pakattu tiedosto oikeaan sijaintiin. Mikäli palautus ei onnistu, palveluntarjoajaan voi olla suoraan yhteydessä, koska heillä tulisi olla varmuuskopiot kaikesta asiakkaan sisällöstä. Tämä on kuvattu toipumissuunnitelmassa. Riippuen sisällön katoamisen syystä, palauttaminen Zonerin toimesta on joko ilmaista tai maksullista.
Aikaisemmin toiminnan ohessa on todettu, että verkkosivut voivat toimia virheellisesti myös sopimattoman päivityksen takia. Mikäli verkkosivut hajoavat, mutta sisältö ei katoa, voi syy olla viimeisimmät teemapäivityksestä ja sen riippuvuudesta WiO:n teemaan Wordpressissä. Wordpressiin on asennettu lisäosa, jolla päivitykset voi tarvittaessa peruuttaa aikaisempaan tilaan. Koska riski on tiedossa, on toipumissuunnitelmaan sisällytetty myös ohjeistus tällaiseen tilanteeseen.

Tietoturvallisen toiminnan piirissä kyseessä olevassa organisaatiossa on myös paljon asioita, jotka eivät ole WiO:n käsissä. Etenkin laitteiston ja tilojen ongelmatilanteissa vastaava taho on HTK. Tällä yhteisosakuntalaisella toimikunnalla on omat prosessinsa, joihin WiO:n tietoturvasuunnitelmassa ei oteta kantaa vaan tyydytään ohjeistamaan ottamaan tietyissä tilanteissa yhteyttä HTK:aan. Uhkaavissa tilanteissa ja vakavissa onnettomuustilanteissa tulee kuitenkin ensin ottaa yhteyttä hätänumeroon.

Tietoturvasuunnitelman alkuun lisättiin taulukko, johon voidaan kirjata dokumentin muutoshistoria, sillä suunnitelmaan tulee katselmoida ja tarvittaessa muuttaa säännöllisesti. Muutoshistoria sivu koostuu päivitystaulukosta, johon kirjataan, milloin päivitys on tehty, kuka sen on tehnyt ja mitä päivitys koskee. Katselmointitaulukkoon merkitään katselmoija ja aika jokaisen muutoksen jälkeen sekä vuotuisen katselmoinnin yhteydessä.

5 Yhteenveto

Teoriaan nojautuen saatiin hyödyllinen dokumentaatiokokonaisuus aikaiseksi toimeksiantajana toimineen Wiipurilaisen Osakunnan käyttöön ja tietoturvallisen toiminnan tueksi. Työn aikana koettiin onnistumisia, mutta toteutuksessa oli myös haasteita.

Kahden vuoden verkkovastaavana olo helpotti työn tekoa, sillä taustat olivat selvillä, mutta tämä vaikuttaa usein negatiivisesti tekemisen objektiivisuuteen. Suuremmissa yrityksissä tietoturva-analyysit ja toteutukset tehdään yhteistyössä ulkopuolisen konsultin kanssa, jotta hän voi tuoda esille riskejä, jotka ovat jääneet huomaamatta jokapäiväisessä toiminnassa. Toisaalta henkilöstö tuntee toiminnan parhaiten ja tiedostaa monia riskejä kokemuksen kautta. Silti organisaation toimijat voivat pitää joitain asioita itsestäänselvyytenä tai organisaatiolla ei ole edes riittävästi resursseja toteuttaa tietoturvasuunnitelmaa itse, jolloin työtä ei tehdä kunnolla. Tätä työtä toteuttaessa tekijällä ei ollut virkaa osakunnalla, joten resursointi oli kohdallaan. Tietotaidossa oli puutteita, sillä työ toteutettiin insinöörityönä eli osana opintoja. Objektiivisuus ei kärsinyt liikaa, sillä osakuntaurat pysyvät työuriin verraten lyhyinä ja osa-aikaisina, joten asiaan oli tuoretta näkemystä, missä osa-alueissa olisi parannettavaa.

Haasteiksi nousivat aikataulussa pysyminen ja itse tietoturvasuunnitelman sisältö. Insinöörityön aihetta etsittiin ja varmisteltiin vielä tammi-helmikuun vaihteessa, kun valmistuminen oli suunniteltu toukokuulle. Toteutusta työstettiin osa-aikaisen työn ohessa, ja kun joku osa ei valmistunut suunnitellussa aikataulussa, aiheutti se heti painetta aikataulun pitämiseen. Toteutukseen ei kuulunut kurssisisällön puolesta aikataulutettuja tapaamisia tai deadlineja kypsyyskoe ja esiintymispäiviä lukuun ottamatta, joten työ vaati paljon itsenäistä työskentelyä ja itsekuria. Toimeksiantajan puolelta vastuuviroissa ei ollut kokeneita virkailijoita juuri vaihtuneen virkavuoden johdosta, joten työn toteuttajan kykyihin luotettiin suunnitelman toteuttamisessa, joten ohjausta ei ollut toimeksiantajan puolelta.

Tietoturvasta järjestötoiminnassa ei ollut paljoa lähdemateriaalia, vaan suurin osa teoriasta koskee tuottavia liiketoimintoja. Soveltaminen onnistui hyvin, ja työn tekeminen oli näin opettavaista, mutta työn sisältöä oli vaikea rajata, koska ei ollut sopivaa ennakkotapausta. Näin ollen oli hankalaa päättää mikä on oleellista kyseessä olevassa tapauksessa ja mikä ei. Myöskään tietoturvasuunnitelman rakenteesta ei löytynyt malleja, koska ne on suunniteltava tapauskohtaisesti, koska organisaatioita ja niiden tarpeita on

niin erilaisia esimerkiksi koon ja toiminnan puolesta. Oletettavasti tästä syystä teoreettista mallia ei ole toteutettu. Esimerkkejä oli myös hankala löytää, sillä tällaiset asiakirjat ovat usein salaisia.

Toteutuksen aikana esille tuli asioita, jotka olisi hyvä toteuttaa jatkotoimina ja jotka soveltuvat myös opinnäytetyöksi. Työn ulkopuolelle jätettiin palveluntarjoajien sovelluksissa olevat tietoturvapoikkeukset. Nämä on hyvä tulevaisuudessa käydä läpi ja selvittää miten niihin voi vaikuttaa omalla toiminnalla. Tärkeää on myös tehdä säännöllisin väliajoin vertailu muiden palveluntarjoajien välillä ja varmistaa, että tämän hetken käyttötarkoitukseen parhaat palvelut ovat käytössä.

Työn aikana kävi myös ilmi, että jäsenrekisterissä on paljon puutteita. Jäsenrekisteriä voidaan tietysti pitää myös paperisena, mutta riskejä analysoidessa huomattiin, että tässä muodossa tiedot on kaikista vaikein palauttaa niiden vahingoittuessa tai kadotessa. Nykypäivänä sähköistä jäsenrekisteriä on harkittava vakavasti ja vaihtoehtojen vertailu ja rekisterin toteuttaminen soveltuvat opinnäytetyöksi.

Insinöörityöprosessin aikana onnistuttiin soveltamaan aiemmin opittua ja oppimaan uutta. Teoria saatiin sidottua käytäntöön ja tietoa onnistuttiin yhdistelemään selkeiksi kokonaisuuksiksi. Vaikka prosessi ei aina sujunut toivotulla tavalla, pystyttiin työskentelemään paineen alla ja etsimään uutta tietoa, jota soveltaen työtä voitiin viedä eteenpäin. Kaiken kaikkiaan työ saatiin vietyä loppuun onnistuneesti.

Lähteet

Andersson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tietosanoma Oy. Helsinki.

Finlex 1999. Henkilötietolaki. Luettavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523#L7P32. Luettu 30.3.2017.

Finlex 2009. Yliopistolaki. Luettavisssa: http://www.finlex.fi/fi/laki/ajantasa/2009/20090558. Luettu: 24.03.2017.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo. Jyväskylä.

Järvinen, P. 2012. Arjen tietoturva. Vinkit ja ratkaisut. Docendo. Jyväskylä.

Kanava.to 2014. Verkkosivujen tietoturvauhat ja niihin varautuminen. Luettavissa: http://www.kanava.to/blogi/tietoturvauhat-ja-niihin-varautuminen/. Luettu: 02.04.2017

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy. Helsinki.

Nevala, S. 2014. Missä jäsentietonne majailevat? 6 asiaa yhdistyksen tietoturvasta, jotka eivät ole käyneet mielessäsi. Luettavissa: http://blog.avoine.fi/kirjoitukset/missa-jasentietonne-majailevat-6-asiaa-yhdistyksen-tietoturvasta-jotka-eivat-ole-kayneet-mielessasi/. Luettu: 31.03.2017.

Vahti 2009a. Tietoaineistoturvallisuus. Luettavissa: https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus. Luettu: 03.03.2017.

Vahti 2009b. Laitteistoturvallisuus. Luettavissa: https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus1. Luettu: 03.03.2017.

Vahti 2009c. Tietoliikenneturvallisuus. Luettavissa: https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus. Luettu: 03.03.2017.

Wiipurilainen Osakunta 2017a. Wiipurilainen osakuntavuosi. Luettavissa: http://wiipurilainenosakunta.fi/osakuntavuosi/. Luettu: 06.03.2017.

Wiipurilainen Osakunta 2017b. Virkaesittely. Luettavissa: http://wiipurilainenosakunta.fi/osakunta/virkaesittely/. Luettu: 06.03.2017.

Wikipedia 2017. Opiskelijajärjestö. Luettavissa: https://fi.wikipedia.org/wiki/Opiskelijaj%C3%A4rjest%C3%B6. Luettu: 24.03.2017.

Riskikartoitus

Riski	Seuraus	Vastuuhenkilö	Ehkäisevät toimet
Murto/varkaus	Ulkopuolisen pääsy käsiksi luottamuksellisiin tietoihin, tietojen ja/tai laitteiden katoaminen, taloudelliset kulut korjauksiin	HTK	Kulunvalvonta, lukot, hälytysjärjestelmät
Asiaton oleskelu	Ulkopuolisen pääsy käsiksi luottamuksellisiin tietoihin, tietojen ja/tai laitteiden katoaminen, taloudelliset kulut korjauksiin	HTK/Tapahtuman järjestäjä	Kulunvalvonta, lukot, koulutus/ohjeistus
Tulipalo	Tiedon ja laitteiden tuhoutuminen tulipalossa, taloudelliset kulut korjauksiin	Kiinteistöhuolto/HTK	Palovaroittimet, sammuttimet, laitteiden sammuttaminen, keskuskytkin lämpölaitteille
Vesivahinko	Tiedon ja laitteiden tuhoutuminen, taloudelliset kulut korjauksiin	Kiinteistöhuolto/HTK	Viemärit, putkien huolto, pesukoneen oikea oppinen käyttö, "hanojen" sulkeminen
Sähkövika	Laitteiden vioittuminen, taloudelliset kulut korjauksiin	Kiinteistöhuolto/HTK	Säännöllinen tarkistus ja huolto
Virus	Laitteiden sisältämien tietojen katoaminen/tuhoutuminen	Verkkovastaava	Tuntemattomien linkkien avaamisen ja ohjelmien asentamisien välttäminen
Hakkerointi	Tilien/Laitteiden tietojen leviäminen/katoaminen/tuhoutuminen	Verkkovastaava/Tiedotusneuvos	Vahva salasana ja sen vaihtaminen säännöllisesti, sekä sen säilyttäminen oikeaoppisesti
Asiaton henkilö saa käyttötilin salasanan	Tilien väärinkäyttö ja mahdollinen luotettavien tietojen lukeminen, muokkaaminen, levittäminen ja/tai kadottaminen	Käyttötilistä vastaava/Tilin omistaja	Koulutus/ohjeistus (miten salasanoja saa säilyttää)
Inhimillinen virhe laitteiden/ohjelmistojen käytössä	Tietojen leviäminen/katoaminen/tuhoutuminen	Verkkovastaava	Koulutus/ohjeistus
Inhimillinen virhe asiapapereiden käsittelyssä	Tietojen leviäminen/katoaminen/tuhoutuminen	Sihteeri	Koulutus/ohjeistus
Palvelinvika	Tietojen tuhoutuminen	Palveluntarjoaja	Varmuuskopiot
Jäsentietoja sisältävän laiteen tekninen vika	Tietojen tuhoutuminen (tiedot saatavissa uudelleen)	Laitteen omistaja	Säännöllinen tarkistus ja huolto
Yhteiskäyttöisten tietokoneiden tekninen vika	(Eivät sisällä osakunnalle tärkeitä tietoja) Laitetta vaativien toimien väliaikainen seisahtuminen, taloudelliset kulut korjauksiin	HTK	Säännöllinen tarkistus ja huolto

Wiipurilaisen Osakunnan tietoturvapolitiikka

Johdanto

Tämä asiakirja sisältää Wiipurilaisen Osakunnan (WiO) tietoturvapolitiikan eli järjestön linjauksen tietoturvallisesta toiminnasta. WiO on opiskelijajärjestö, joka koostuu opiskelijajäsenistä ja valmistuneista senioreista. WiO:lla on arkistoituna jäsentensä henkilötietoja.

Tietoturvapolitiikka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot. Se annetaan tiedoksi kaikille WiO:n virkailijoille tietoturvan perusasiakirjana. Tietoturvallista toimintaa tarkennetaan politiikan pohjalta luodussa tietoturvasuunnitelmassa sekä ohjeissa ja perehdytyksissä, jotka koskevat WiO:a.

Tietoturvapolitiikan tavoite

Tietosuoja merkitsee henkilön tiedollisen itsemääräämisoikeuden ja yksityisyyden suojaamista. Tietoturvalla tarkoitetaan menettelyjä ja toimenpiteitä tuon suojan ylläpitämiseen. Tietoturvassa suojattaviin asioihin sisältyvät myös tietojen käsittelyssä tarvittavat laitteistot tietoliikennejärjestelmineen. Tiedon tulee olla luotettavaa, eheää ja käytettävissä.

WiO:n tavoitteena yhdessä yhteistyötahojen kanssa on turvata riittävällä ja tarkoituksenmukaisella tasolla luottamukselliset ja toiminnalle oleelliset tiedot, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta sekä estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon vääristyminen tai tuhoutuminen. Tietojen turvallisuudesta tulee huolehtia manuaalisesti ja tietotekniikan avulla tapahtuvassa tietojenkäsittelyssä, tietojen kaikissa olomuodoissa ja tietojen koko elinkaaren ajan.

Tietoturvatyö on jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa. Sillä pyritään ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeustilanteisiin. Tietoturva politiikka tukee näiden tavoitteiden tietoturvallisen toiminnan saavuttamista.

Tietoturvatoimintaa ohjaavat tekijät

WiO:n tietoturvallisuudesta huolehditaan Suomessa voimassa olevien kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti.

Tietoturvallisuuden merkitys osakunnalle

WiO ottaa vuosittain vastaan uusia jäseniä. Tietoturvallisuus tulee toteutua etenkin jäsentietojen käsittelyprosesseissa. Uusien jäsenten tiedot tulee arkistoida oikeaoppisesti ja vanhojen jäsenten tiedot tulee pitää ajan tasalla. Tietoja käsittelevät vain siihen valtuutetut henkilöt ja ne eivät tule olla muiden saatavilla. WiO:lla on myös toiminnan kannalta oleellisia käyttäjätilejä, jotka tulee pitää turvassa. Kaikki toiminnan kannalta luottamuksellinen tieto tulee olla vain asianomaisten saatavilla.

Toiminnan muutoksiin ja palveluiden tai järjestelmien hankintoihin tulee sisällyttää tietoriskien arviointi ja tietoturvavaatimusten määrittely jo suunnitteluvaiheessa.

Tietoturvavastuut

Tietoturvallisuus toteutuu tehokkaimmin, kun toimintaa ohjaavat nimetyt vastuuhenkilöt ja kaikki tiedon käsittelijät huolehtivat oman osa-alueensa turvallisuudesta parhaalla mahdollisella tavalla. Jokaisella WiO:n virkailijalla on vastuu tietoturvallisuuden toteuttamisesta ja valvonnasta sekä velvollisuus noudattaa WiO:n antamia tietoturvallisuuteen liittyviä sääntöjä ja ohjeita.

Vastuu WiO:n toiminnasta ja tietoturvasta on WiO:n neuvostolla. Suunnitelma, ohjeistus ja toteutus tehdään yhdessä eri osa-alueiden virkailijoiden ja toimikuntien kanssa.

Tietoturvatoimien riittävä ja oikea taso varmistetaan tietoturvallisuuden riskienhallinnalla. Toimintaan, palveluihin ja järjestelmiin kohdistuva riskien arviointi tulee toteuttaa säännöllisesti toimintaan sopivin aikavälein sekä merkittävien muutosten yhteydessä. Korjaavien ja ehkäisevien toimenpiteiden suorittamisesta vastaavat tietojen ja järjestelmien omistajat.

Tietoturvakoulutus ja -ohjeet

Tietoturvakoulutus sisältyy uusien virkailijoiden perehdyttämiseen jokaisen vuoden vaihteessa. Tietoturvasuunnitelma ja muut tietoturvaa koskevat ohjeistukset ovat luettavissa virkailijoille tarkoitetussa wikissä. Lisäkoulutuksen tarpeessa voidaan erillinen koulutus järjestää neuvoston päätöksestä.

Tietoturvallisuudesta tiedottaminen

WiO:n tietoturvallisuutta koskevat asiat eivät ole aktiivisen ulkoisen tiedottamisen aihe. Tarvittavia virkailijoita tiedotetaan sisäisesti, jos tietoturvassa havaitaan poikkeuksia tai ohjeistukseen tulee muutoksia. Järjestettävistä koulutuksista tiedotetaan kaikkia virkailijoita ja tarvittaessa kaikkia jäseniä. Mikäli on aihetta uskoa, että arkaluontoisia jäsentietoja on päässyt vuotamaan ulkopuolisille, tiedotetaan kaikkia jäseniä asiasta.

Valvonta

Tietoturvallisuudesta huolehtiminen edellyttää jatkuvaa seurantaa sekä turvallisuustason ja poikkeamien raportointia. Seurantaa toteutetaan normaalin toiminnan ohessa. Kunkin tietojärjestelmän, aineiston tai palvelun turvallisuuden valvonnan toteutumisesta on vastuussa sen omistaja. Jokainen virkailija on velvollinen raportoimaan tietoturvan tasosta, poikkeamista, puutteista ja epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista tiedon tai tietojärjestelmän omistajalle sekä WiO:n neuvostolle. Neuvosto voi tarvittaessa käynnistää tietojen käsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi.

Hyväksynyt

Päiväys

Wiipurilaisen Osakunnan tietoturvasuunnitelma

Sisällysluettelo

Päivityshistoria

Versio	Päivämäärä	Päivittäjä	Päivitys
1.0	23.4.2017	Maiju Partamies	Luotu uutena

Katselmointi ja hyväksyntä

Versio	Päivämäärä	Hyväksyjä
1.0		

1 Johdanto

Tämä tietoturvasuunnitelma on yleinen tietoturvadokumentti Wiipurilaisen Osakunnan sisäiseen käyttöön. Dokumentissa esitellään ja ohjeistetaan tietoturvallista toimintaa osa-alueittain. Dokumentista löytyvät myös vastuu toimikunnat/virkailijat, joihin olla yhteydessä ongelmatilanteissa. Nykytilanteen pohjalta on suunniteltu toimia tietoturvallisuuden kehittämiseksi ja parantamiseksi. Tietoturvasuunnitelma tulee tarkistaa vuoden välein, jotta se pysyy ajantasaisena ja kehitystoimien etenemistä voidaan seurata.

2 Hallinnollinen turvallisuus

Hallinnollisesta turvallisuudesta eli tietoturvan hallinnoinnista ja yhteydenpidosta eri tietoturvavastaaviin, sekä tietoturvallisesta toiminnasta vastaa kuraattorin johtama neuvosto. Tähän sisältyy toiminnan valvonta ja kehittävien sekä korjaavien toimien koordinointi.

Osakunnalle toteutettiin tietoturvadokumentaatiokokonaisuus keväällä 2017, johon kuuluu sen hetkinen riskikartoitus, tietoturvapolitiikka ja tietoturvasuunnitelma. Neuvoston tulee katselmoida mainitut dokumentit vuoden välein aina virkavuoden alussa ja toteuttaa tai delegoida tarvittavat päivitykset.

3 Fyysinen turvallisuus

Fyysisestä turvallisuudesta eli tiloista ja laitteista vastaa huoneistotoimikunta (HTK) yhdessä kiinteistöhuollon, vartiointiliikkeen ja HYY:n kanssa. Osakuntatilat koostuvat eteisaulasta, tilanjakajalla kahteen jaettavasta salista, oleskelutilana toimivasta lehtihuoneesta, keittiöstä ja toimistosta. Lukolliset sisäänkäynnit sijaitsevat aulassa ja keittiössä. Ovet tulee aina pitää lukittuina. Aulan ovea voi pitää poikkeuksellisesti auki tapahtumien aikana, mikäli ovella on henkilöitä suorittamassa kulunvalvontaa.

HTK on toteuttanut vuonna 2016 turvallisen tilan ohjeistuksen, joka on nähtävillä tiloissa. Ohjeistukseen tulee tutustua ja sitä on noudatettava.

4 Henkilöturvallisuus

Henkilöturvallisuus merkitsee sitä, että hallitaan henkilöstön toimista aiheutuvia ja heihin kohdistuvia turvauhkia. Tietoturvan näkökulmasta näihin kuuluvat muun muassa tiedon väärinkäytöt ja inhimilliset virheet. Henkilöturvallisuudesta tietoturvan kannalta vastaavat virkailijat perehdyttämällä omat seuraajansa sekä verkkovastaava kouluttamalla ja tukemalla tarvittaessa ohjelmistojen käytössä. Kunnollisella perehdyttämisellä pyritään varmistamaan, että virkailijat osaavat toimia oikein, ettei väärinkäytöksiä ilmenisi ja vähennettäisiin toiminnassa sattuvia virheitä.

5 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudesta vastaa jäsentietojen osalta sihteeri, arkistoinnin osalta arkiston- ja kirjastonhoitaja ja sähköisistä varmuuskopioista verkkovastaava. Säilytettävät tiedot tulee pitää eheinä ja saatavilla. Virkailijoita tulee perehdytyksessä ohjeistaa mitä, miten ja missä tietoja tulee säilyttää ja miten tarpeeton tieto pitää hävittää.

5.1 Jäsentiedot

Kaikkien jäsenien jäsenlomakkeet tulee säilyttää lukitussa toimistossa niille varatussa kansiossa. Älä kuljeta jäsentietopapereita mukanasi ellei sille ole pakottavaa tarvetta. Näin pystytään paremmin välttämään jäsentietojen katoaminen tai tuhoutuminen sekä niiden joutuminen vääriin käsiin.

Paperisilla lomakkeilla ei ole varmuuskopiota, mutta jäsenmaksun HYY:n vuosimaksun yhteydessä maksaneista voi saada Helsingin yliopistolta sähköisessä muodossa. tiedostoa pyytää, säilyttää ja hallinnoi sihteeri. Jos täydelliset jäsentiedot vahingoittuvat tai katoavat, voidaan kyseessä olevaa tiedostoa käyttää väliaikaisesti huomioon ottaen, että siitä puuttuvat ainakin ulkojäsenten tiedot ja ne pitää kerätä uudelleen. Listaa henkilöistä, jotka ovat maksaneet jäsenmaksun suoraan tilille pyydetään taloudenhoitajalta ja tämän pohjalta voidaan kerätä tietoja sähköisestä tiedostosta puuttuvilta henkilöiltä.

Jäsentietojen keräys- ja käsittelyohjeet ovat tarkemmin kuvattuna sihteerin perehdytysmateriaaleissa.

Kuten kerrottu, eheä jäsenrekisteri on vain paperisessa muodossa ja näin vaikeasti kopioitavissa. Sähköisessä jäsenrekisteritiedostossa on puutteita, koska se sisältää vain HYY:n jäseninä olevia osakuntalaisia. Jäsenrekisterin ylläpidon helpottamiseksi ja riskien pienentämiseksi, tulisi jäsenrekisteri tulevaisuudessa muuttaa kokonaisuudessaan myös sähköiseksi.

5.2 Käyttäjätunnus- ja salasanaohjeistus

Wiipurilaisen osakunnan virkailijalla on varakuraattorin toimesta käyttäjätunnukset Virkailijawikiin. Tämän lisäksi virkailijalla voi olla virkaan liitetyt tai toimikunnan kautta jaetut käyttäjätunnukset WordPressiin, Zonerin hallintapaneeliin, tilanvarauskalenteriin, Galleriaan, Facebookiin, Instagramiin ja/tai Snapchattiin. Uusi virkailija saa käyttäjätunnukset wikiin varakuraattorilta ja muihin palveluihin perehdytyksen yhteydessä. Pidä huoli, että säilytät käyttäjätunnuksia fiksusti. Älä kirjoita niitä ylös esim. kalenteriin tai tallenna niitä kännykkään tai tietokoneellesi salaamatta. Tarvittaessa voit tallentaa ne salasanasovellukseen, kuten KeyPass. Älä jaa käyttäjätunnustasi ja salasanaasi kenellekään.

Perehdytyksen yhteydessä salasana tulee päivittää uuden virkailijan toimesta. Salasanan tulee olla vähintään kahdeksan merkkiä pitkä ja sisältää isoja ja pieniä kirjaimia, numeroita sekä erikoismerkkejä (mikäli palvelu sen sallii). Mitä pidempi salasana, sitä

vaikeampi se on hakkeroida. Pyri välttämään selkokielisiä sanoja salasanana. Tästä voit joustaa, jos käytät salasanana lausetta ja se on erityisen pitkä. Salasana tulee vaihtaa myös, jos epäilet, että se on jonkun toisen tiedossa. Ilmoitathan muutoksesta asianomaisille virkailijoille, jos käyttäjätili on monen virkailijan vastuulla (sosiaalisen median tilit).

5.3 Puhtaan pöydän periaate

Kun käsittelet osakunnalla tai arkistossa asiakirjoja, etenkin jos ne sisältävät henkilötietoja, älä jätä niitä levälleen näkyville, mikäli poistut tilasta. Palauta asiakirjat aina asianmukaiselle paikalle. Osakuntatiloissa on kaksi vapaassa käytössä olevaa konetta. Oman yksityisyytesi ja osakunnan tietojen takia kirjaudu ulos käyttäjätileiltä ja sulje auki olevat asiakirjat aina kun poistut koneen ääreltä. Sivuhistoria on myös hyvä tyhjentää internetin käytön lopettaessasi.

5.4 Varmuuskopiointi

Varmuuskopiointi on aina verkkovastaavan vastuulla. Varmuuskopioitavia asioita ovat verkkosivujen sisältö ja osakunnan kuvat Galleriassa. Ne sijaitsevat palveluntarjoaja Zonerin palvelimella. Tiedostot sisältävät kansiot tulee pakata ja ladata palvelimelta pakattuina tiedostoina kerran kuussa. Palvelimelle pääsyyn tarvitaan käyttäjätunnukset, jotka ovat verkkovastaavan hallussa. Varmuuskopion voi ottaa monella tapaa, kuten manuaalisesti Putty:n tai WinSCP:n avulla tai aiemman verkkovastaavan luomalla Python scriptillä. Ohjeistus varmuuskopioiden ottamiseen ovat verkkovastaavan saatavilla VirkailijaWikissä.

5.5 Sosiaalinen media

Tällä hetkellä WiO:lla on sosiaalisen median tilit sovelluksissa Facebook, Instagram ja Snapchat. Käyttäjätunnuksista ja tilien vastaa tiedotusneuvos ja hän delegoi hallinnoin tarpeen mukaan tiedotustoimikunnalle.

Käyttäjätiedoissa tai jaetussa sisällössä ei tulisi olla yksityisiä henkilötietoja. Julkaisuja tehdessä tulee harkita, antavatko ne jotain tietoa järjestön jäsenistä tai toiminnasta, jota joku voi käyttää laittomalla tavalla hyödyksi. Valokuvia jakaessa, etenkin jos kuviin merkitään jäseniä, tulee varmistaa, että henkilöt haluavat olla kuvissa. Julkaisuissa ei saa levittää jäsenten henkilötietoja. Nimien sisältyminen on sallittua, jos mainitulta henkilöltä on siihen lupa. Virkailijoilla tulee olla tiedossa, että toimenkuvaan kuuluu yhteyshenkilönä oleminen ja tätä kautta heidän nimiään ja verkkosivuille annettuja yhteystietoja saatetaan käyttää julkaisuissa. Muiden jäsenien yhteystietojen ja kaikkien yhteystiedoista poikkeavien henkilötietojen jakaminen sosiaalisen median julkaisuissa on kielletty. Mikäli

tämä on tarpeellista, on jakaminen perusteltava ja lupa kysyttävä asianomaiselta henkilöltä erikseen. Sosiaalisen median tileiltä tulee muistaa kirjautua ulos käytön jälkeen.

6 Ohjelmisto-, tietoliikenne- ja laitteistoturvallisuus

Osakuntatilojen laitteistoista vastaa HTK. Osakuntatiloissa on yhteiskäytössä pöytätietokone, tulostin ja silppuri toimistossa sekä kannettavatietokone lehtihuoneessa.

Yhteiskäyttöisten tietoteknisten laitteiden yhteisistä ohjelmistoista vastaa HTK. WiO:n käyttämistä ohjelmistoista vastaa verkkovastaava. Vastuisiin kuuluu pitää ohjelmistot ajantasaisina ja toiminnassa. Päivitykset tulee tarkistaa ja suorittaa säännöllisesti. Käytössä tulee olla vain sellaisia ohjelmistoja, joissa on voimassa oleva lisenssi. Tietokoneissa tulee olla ajantasainen virustentorjunta ja palomuuri käytössä. Laitteistot tulee tarkistaa ja huoltaa soveltuvin aikavälein.

Tietoliikenneturvallisuudesta, eli osakunnan tapauksessa Internet-yhteyksistä, vastaa HTK.

7 Vastuut ja yhteystiedot

Kaikkien osakunnan toimijoiden vastuulla on ilmoittaa vastuutaholle, jos he huomaavat tietoturvapoikkeuksen tai epäilevät sitä. Tietoturvapoikkeuksiin sisältyy kaikki tässä dokumentissa käydyt alueet eli ilmoitus voi liittyä esimerkiksi viallisiin laitteisiin ja ohjelmistoihin, epäilyttäviin henkilöihin, puutteisiin tiloissa tai kadonneisiin tavaroihin ja tietoihin.

Vastuualue	**Vastuutaho/hlö**	**Yhteystieto***
Toiminta	Neuvosto/ Kuraattori	wio-neuvosto@helsinki.fi/ kuraattori@wiipurilainenosakunta.fi
Jäsenrekisteri	Neuvosto/ Sihteeri	wio-neuvosto@helsinki.fi/ sihteeri@wiipurilainenosakunta.fi
Tilat	HTK/ puheenjohtaja	htk-list@helsinki.fi
Laitteet	HTK/ puheenjohtaja	htk-list@helsinki.fi
Tietokoneiden paikalliset ohjelmistot	HTK/ puheenjohtaja	htk-list@helsinki.fi
WiO:n käyttämät verkkopalvelut (Verkkosivut/WordPress, DokuWiki, Galleria)	Verkkovastaava	verkkovastaava@wiipurilainenosakunta.fi
Tietoliikenne	HTK/ puheenjohtaja	htk-list@helsinki.fi
Wiki käyttäjä- ja sisällönhallinta	Varakuraattori	Ella.Kaplas@helsinki.fi
WordPress käyttäjähallinta	Verkkovastaava	verkkovastaava@wiipurilainenosakunta.fi

Sosiaalinen media	Tiedotustoimikunta/ Tiedotusneuvos	juho.myyrylainen@helsinki.fi
Osakunnan sähköposti-lista	Sihteeri	sihteeri@wiipurilainenosakunta.fi
Senioreiden sähköposti-lista	Verkkovastaava	verkkovastaava@wiipurilai-nenosakunta.fi

*) Kiirellisissä tapauksissa ajantasainen yhteyshenkilön puhelinnumero on löydettävissä Wiipurilaisen osakunnan verkkosivuilta (www.wiipurilainenosakunta.fi) Yhteystiedot/Virkailijat osiosta. Mikäli puhelinnumeroa sopivalle henkilölle ei löydy, ota yhteyttä kuraattoriin.

8 Kehityskohteet tietoturvallisuudessa

Kehityskohteisiin liittyvät toimet listattuna alla. Listaus sisältää asioista, joissa on havaittu puutteita tietoturvakartoituksen yhteydessä, ja jotka tulee toteuttaa/korjata seuraavana mahdollisena ajankohtana. Vastuuvirkailijat määritetään neuvoston toimesta ennen syksy kauden alkua (viimeistään syksyn ensimmäisessä kokouksessa).

- Jäsentietojen käsittelyn ja jäsenrekisterin ohjeistuksen päivitys (vuoden 2017 loppuun mennessä)
- Palveluntarjoajien riskikartoitus ja tietoturvapoikkeuksien dokumentointi (vuoden 2018 loppuun mennessä)
- Uusi jäsenrekisteri (vuoden 2019 loppuun mennessä)
- Palveluntarjoajien vertailu ja mahdolliset vaihdokset (vuoden 2020 loppuun mennessä)

9 Toipumissuunnitelma

9.1 Verkkosivujen ja/tai gallerian sisältö kadonnut

Toipumisaika havaitsemisesta: Tunnista vuorokauteen. Päivittäinen toiminta voi jatkua.

Havaitseminen: Sisältö puuttuu verkkosivuilla tai galleriassa vieraillessa

Vaikutus: Ei vaikuta muihin järjestelmiin tai laitteisiin. Tiedon saaminen verkkosivujen kautta mahdotonta väliaikaisesti, joten voi vaikuttaa siltä, ettei osakunta ole enää toiminnassa. Tämä voi johtaa potentiaalisten jäsenien liittymiseen. Jäsenet eivät saa tietoa, jota olivat etsimässä, joten saattavat myöhästyä esimerkiksi tapahtumasta, asuntohausta tai stipendihausta. Tämän realisoituminen kaikkien jäsenien kohdalla on kuitenkin epätodennäköistä, sillä tiedot tapahtumista ja hauista lähetetään myös sähköpostilistan kautta.

Tiedotus: Havaitsija tiedottaa verkkovastaavaa puhelimitse. Jos verkkovastaava ei ole tavoitettavissa, on hänelle syytä lähettää viesti puhelimen kautta ja sähköpostilla. Talvikaudella voi jäseniä tiedottaa vikatilasta sähköpostilistan kautta. Kesäkaudella tämä ei ole tarpeellista, sillä kävijämäärä ja -tiheys on kohteissa kesäisin pieni.

Toimenpiteet ja tarvittavat resurssit:

Verkkovastaava:

1. Palauta varmuuskopioidut tiedostot joko WinSCP:n tai Puttyn avulla. Pura pakatut tiedostot palvelimelle oikeille sijainneille:

    - /home/wiipurilai/domains/wiipurilainenosakunta.fi/public_html

    - /home/wiipurilai/gallery_data

2. Palauta tietokanta wiipurilai_i

3. Jos varmuuskopioiden palauttaminen ei korjaa ongelmaa tai epäonnistuu, ota yhteys palveluntarjoaja Zoneriin: tuki@zoner.fi

9.2 Sivujen asettelu hajonnut

Toipumisaika havaitsemisesta: Tunnista muutamaan vuorokauteen. Toiminta voi jatkua.

Havaitseminen: Verkkosivuilla vierailija huomaa vikoja asettelussa

Vaikutus: Ei vaikutusta järjestelmiin tai laitteistoihin. Ei vaikutusta tiedon jakamiseen. Saattaa vaikeuttaa verkkosivujen käyttämistä tai lukemista. Ei vakavia seuraamuksia, saattaa vaikuttaa osakunnan imagoon.

Tiedotus: Havaitsijan tulee olla yhteydessä Verkkovastaavaan. Jos virhe ei ole kriittinen, ota yhteyttä sähköpostitse.

Toimenpiteet ja tarvittavat resurssit:

Verkkovastaava:

1. Tarkista asettelu eri selaimilla. Jos vika on selain kohtainen, kehota ilmoittajaa käyttämään toista selainta ja ota selvitystyö ja korjaus tehtävälistalle.

2. Jos asettelussa on selkeästi vikaa selaimesta riippumatta, kirjaudu WordPressin hallintapaneeliin ja katso kuka on viimeksi muokannut virheellistä sivua. Palauta aikaisempi asettelu ja ilmoita tilanteesta muokkaajalle. Käykää läpi mikä meni vikaan ja ohjeista käytössä.

3. Jos vika on kokonaisvaltainen ja muutoksia ei ole tehty sivuihin, tarkista päivitykset. Mikäli teemoihin on virheen havaitsemista ennen tehty päivityksiä, pohjateema ei saata olla enää yhteensopiva räätälöityyn teemaan. Tee päivityksen peruuttaminen asennetun Rollback lisäosan avulla.

4. Raportoi vian aiheuttanut päivitys ja toimiva versio.

5. Varmista, että päivitys oli tehty toimestasi ja jos ei, ohjeista päivityksen tehnyttä henkilöä, että päivitys on vastuullasi.

6. Mikäli aiemmat toimet eivät auttaneet, korjaa virheitä manuaalisesti seuraavien päivien kuluessa. Pyri samalla selvittämään juuri syy ja päivittämään toipumissuunnitelmaa. Ota tarvittaessa yhteyttä WordPress tukeen. Voit käytää Googlea apuna selvittääksesi ovatko muut törmänneet samankaltaisiin ongelmiin, jos viasta löytyy selkeitä piirteitä

9.3 Jäsentiedot kadonneet/tuhoutuneet

Toipumisaika havaitsemisesta: Päivästä viikkoon. Toiminta voi jatkua.

Havaitseminen: Jäsenkansio on kadonnut tai sen sisältö on viallinen.

Vaikutus: Ei vaikuta järjestelmiin tai laitteisiin. Jäsentiedot ovat voineet joutua väärinkäyttäjän haltuun ja tästä voi koitua haittaa jäsenille esimerkiksi yhteydenottoina, joilla on laittomat tarkoitusperät.

Tiedotus: Asiasta on tiedotettava ensisijaisesti sihteeriä puhelimitse. Sihteeri tiedottaa tarvittaessa kuraattoria ja neuvostoa. Jäsenille on lähetettävä tiedote sähköpostilistan kautta, mikäli on tarvetta uskoa, että tiedot ovat vuotaneet asiattomille henkilöille.

Toimenpiteet ja tarvittavat resurssit:

Jos tietojen puuttuminen koskee vain yhtä henkilöä ja henkilöllisyys tiedetään, tiedotetaan vain häntä asiasta ja pyydetään häntä täyttämään jäsenlomake uudelleen.

Sihteeri:

1. Lähetä jäsentietojen pyynnön Helsingin yliopistolle, mikäli sinulla ei jo ole ajantasaista tietoa sähköisessä muodossa. Ohjeet wikissä.

2. Pyydä taloudenhoitajalta lista suoraan tilille maksaneista jäsenistä.

3. Ole mahdollisuuksien mukaan yhteydessä taloudenhoitajan listaamiin henkilöihin ja pyydä puuttuvat tiedot. Lisää ne saamaasi sähköiseen tiedostoon.

4. Arkiston pitämistä paperisena jatketaan uusien jäsenien kohdalla.

9.4 Tulipalo/vesivahinko

Toipumisaika havaitsemisesta: Vuorokaudesta määrittelemättömään vahingon suuruudesta riippuen

Havaitseminen: Palovaroitin tai aistihavainnot

Vaikutus: Asiakirjojen tuhoutuminen, laitteistojen ja tilojen vioittuminen, henkilövahingot, taloudelliset tappiot. Palvelin ja verkkopalvelut säilyvät, sillä ne on hankittu ulkoisilta palveluntarjoajilta.

Tiedotus: Tilanteen mukaan soitto palokunnalle tai kiinteistöhuoltoon. Ilmoitus HTK:lle ensisijaisesti puhelimitse puheenjohtajalle. Tiedote jäsenille sähköpostilistan kautta mahdollisesta tilojen käyttökatkosta ja toiminnan peruuntumisesta. Ilmoitus tilanteesta kaikkien tiloissa toimivien järjestöjen yhteyshenkilöille (HTK:n toimesta).

Toimenpiteet ja tarvittavat resurssit:

Havaitsija:

1. Tyhjennä tilat ja pyri sammuttamaan palo/tukkimaan vuoto/estämään veden leviäminen. Poistu tiloista, jos alkusammutusvälineet eivät riitä palon sammuttamiseen.

2. Soita palokunnalle tai kiinteistöhuoltoon.

3. Tiedota HTK:ta

HTK: Vahinkojen korjausten koordinointi.

Sihteeri: Toimi tarvittaessa jäsentietojen tuhoutumisen toipumisohjeen mukaisesti.

9.5 Sähkövika

Toipumisaika havaitsemisesta: Tunnista pariin vuorokauteen

Havaitseminen: Sähkölaitteet eivät toimi tai kipinöivät.

Vaikutus: Mahdollinen laitteistojen vioittuminen ja välillisesti taloudelliset tappiot. Henkilövahingot. Toiminnan seisahtuminen.

Tiedotus: Ilmoitus HTK:lle ja heidän ohjeidensa mukaan mahdollisesti kiinteistöhuollolle. Ilmoitus tilanteesta kaikkien tiloissa toimivien järjestöjen yhteyshenkilöille (HTK:n toimesta).

Toimenpiteet ja tarvittavat resurssit:

Havaitsija:

1. Sammuta sähkölaitteet ja sähköt katkaisimista.
2. Tiedota paikalla olijoita tilanteesta.
3. Kysy neuvoa HTK:lta

HTK: Vahinkojen korjausten koordinointi. Korjaajan tilaaminen ja korjauksen valmistumisajankohdasta tiedottaminen.

9.6 Murto

Toipumisaika havaitsemisesta: Määrittelemätön. Riippuu varkauden arvosta ja osakuntien taloudellisesta tilanteesta sekä vakuutuksen kattavuudesta. Toiminnan jatkamiseen mahdollisine rajoitteineen toipuminen vuorokaudessa.

Havaitseminen: Murtojälkiä lukoissa. Kadonneita tavaroita tai rahaa.

Vaikutus: Tietojen, arvotavaroiden ja laitteiden katoaminen. Korvaamattomien asioiden menettäminen. Toiminnan väliaikainen seisahtuminen. Tietojen mahdollinen leviäminen väärinkäyttäjille.

Tiedotus: Poliisi ja HTK puhelimitse heti havaitsemishetkellä. Tarvittaessa myös vartiointiliike. Jäsenien tiedottaminen, mikäli tilat on laitettava tutkinnan ajaksi käyttökieltoon. Ilmoitus tilanteesta kaikkien tiloissa toimivien järjestöjen yhteyshenkilöille (HTK:n toimesta).

Toimenpiteet ja tarvittavat resurssit:

Havaitsija: Tiedotus ja paikalle jäänti

Neuvosto ja HTK: Menetettyjen tavaroiden korvaamisen koordinointi

9.7 Unohtunut tai vuotanut salasana

Toipumisaika havaitsemisesta: Tunti, pahimman tapauksen realisoituessa tilin palauttamiseen parivuorokautta. Toiminta voi jatkua.

Havaitseminen: Kirjautuminen ei onnistu tai käyttäjätilille on tehty muutoksia jonkun muun kuin valtuutetun toimesta.

Vaikutus: Ei vaikutusta järjestelmiin tai laitteisiin. Salasanan unohtumisella ei kriittisiä vaikutuksia. Mahdollisen tiedottamisen tai päivittämisen hetkellinen viivästyminen. Salasanan ollessa asiattomassa käytössä, mahdollinen sisällön menettäminen tai jäsenille haittaa, mikäli ulkopuolinen henkilö on ehtinyt esimerkiksi kalastella tietoja lisäämällään sisällöllä.

Tiedotus: Ilmoitus asiasta muille käyttäjille, mikäli tunnus on jaettu. Mikäli tilin kautta on lisätty sisältöä (wikiin, verkkosivuille, someen), joka on lukijalle haitallista tai ei pidä paikkaansa, tiedote asiasta kyseessä olevaan kanavaan.

Toimenpiteet ja tarvittavat resurssit:

Palauta tai vaihda salasana palvelun ohjeistuksen mukaisesti. Mikäli tili on joutunut väärinkäytön kohteeksi ja salasana sekä sen palautusyhteystieto on muutettu, ota yhteyttä palveluntarjoajaan ja tiedota neuvostoa ja verkkovastaavaa asiasta.