Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2014

Mikko Oinonen

TIETOTURVARISKIEN KARTOITUS SOPIMUSPALOKUNTA-YHDISTYKSELLE

– case Turun Vapaaehtoinen Palokunta ry

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

Toukokuu 2014 | 81 sivua

Ohjaaja Esko Vainikka

Mikko Oinonen

TIETOTURVARISKIEN KARTOITUS SOPIMUSPALOKUNTAYHDISTYKSELLE

Opinnäytetyön tarkoituksena on selvittää sopimuspalokuntatoimintaan liittyvät tietoturvariskit sekä analysoida niiden vaikutus yhdistyksen toimintaan.

Tietoturvariskien kartoittaminen suoritettiin lähettämällä kyselylomake yhdistyksen hallitukselle sekä yhdistyksen toiminnan avainhenkilöille. Lomakkeessa pyydettiin listaamaan yhdistykselle arvokasta tieto-omaisuutta, kertomaan käytössä olevista tietoturvamenetelmistä sekä listaamaan, millaista vahinkoa syntyisi jos tieto-omaisuuden eheys, luottamuksellisuus tai saatavuus vaarantuisi. Lisäksi toimitiloissa suoritettiin itsenäistä havainnointia tietotekniikan ja tietoturvan osalta.

Riskianalyysissä tarkasteltiin tietoturvariskejä jakamalla ne kuuteen eri osa-alueeseen ja muodostamalla havaituille riskeille riskikerroin, jota yhdistys voi käyttää hyväkseen keskittyessään eniten huomiota ja toimenpiteitä vaativiin tietoturvariskeihin.

Vaikka yhdistyksellä ei olisi tarkkaa tietoa arvokkaasta tieto-omaisuudesta, on tietoturvan taso yleisesti ottaen hyvällä tasolla. Tietoturvan tärkeys ymmärretään ja yhdistyksen päivittäisissä toiminnoissa on otettu käyttöön monia yleisesti hyväksi todettuja tietoturvaratkaisuja ja toimenpiteitä. Yhdistykselle laadittiin kirjallinen yhteenveto mahdollisista uhkaskenaarioista sekä niiden muodostamista riskeistä toimenpidesuosituksineen.

ASIASANAT: Tietoturva, Tietoturvariski, Tietoturvallisuus, Tietoturvariskianalyysi, Hallinnollinen tietoturva, Riskienhallinta.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

May 2014 | 81 pages

Instructor Esko Vainikka

Mikko Oinonen

SECURITY RISK ASSESSMENT FOR A VOLUNTEER FIRE BRIGADE ASSOCIATION

The purpose of the present bachelor's thesis is to explore potential IT security risks involved within the activities of the volunteer fire brigade. The thesis also analyses the impacts on the activities if the risks come true.

The analysis of the threats and risks was conducted by sending a question form to the board of directors and to the key personnel of the association. The personnel were asked to list valuable assets to the association, to tell about the safety mechanisms the assets were protected with and to list the damages caused to the fire brigade if the confidentiality, integrity or availability of the assets would be compromised. A walk-through within the premises was also conducted to gather additional information.

The security risks were analyzed by dividing them into six groups. Each individual risk was given a risk factor which enables the association to list risks in such a way that the most critical risks with the highest factor would top the list, and thus giving the association a ranking list to react to.

Although the association lacks the understanding of their assets, the IT security is generally at a good level. The association understands the importance of IT security and it has implemented several established security practices into their daily activities. The association was given a written summery of the potential threat scenarios and the risks they include as well as the suggested measures to reduce them.

KEYWORDS: Information security, Security risk, Security risk assessment, Administrative security, Risk management.

SISÄLTÖ

LIITTEET

Liite 5: Markkinointipäällikön vastauslomake (salattu).
Liite 6: Aluepelastuslaitoksen viestiliikennesuunnittelijan sähköpostihaastattelu (salattu).
Liite 7: Yhdistykselle laadittu tietoturvariskien yhteenveto (salattu).

TAULUKOT

1 JOHDANTO

Tässä opinnäytetyössä keskitytään selvittämään sopimuspalokuntayhdistyksen tietoturvariskejä sekä laatimaan yhdistykselle yhteenveto, jossa löydetyt riskit on eritelty ja niihin on esitetty korjausehdotuksia.

Sopimuspalokuntayhdistykset suorittavat päivittäin keskimäärin 200 hälytystehtävää joko yksin tai yhteistyössä pelastuslaitoksien ammattipelastajien kanssa (Suomen Sopimuspalokuntien Liitto 2013).

Jokaisesta suoritetusta hälytystehtävästä sekä yhdistystoiminnan ylläpidosta muodostuu sivutuotteena dokumentteja, joita ei ole tähän mennessä analysoitu kattavasti tietoturvan näkökannalta. Lisäksi edellä mainittujen toimien suorittamiseksi sopimuspalokuntayhdistykset usein käyttävät tietokonetta, johon palokunnan jäsenistöllä on vapaa pääsy. Tämä muodostaa selkeän tietoturvariskin.

Riskikartoitus saatiin toimeksiantona Turun Vapaaehtoinen Palokunta ry:ltä, joten tämä opinnäytetyö keskittyy kyseisen palokuntayhdistyksen tietoturvariskeihin. Työssä on keskitytty toimiston, markkinoinnin sekä hälytysosaston osalta keskeisimpiin riskitekijöihin.

Tieto-omaisuuden sekä sen suojauksen tason kartoittamista varten laadin kyselylomakkeen, joka lähetettiin yhdistyksen hallitukselle, toimistosihteerille, markkinointipäälliköllе sekä isännöitsijälle. Kyselylomakkeen kysymykset kerättiin manuaalisesti Octave-S -materiaalista valikoimalla sekä käyttämällä avuksi Douglas J. Landollin kirjaa ”The Security Risk Assesment Handbook” (2011). Yhdistyksen hallitus koordinoi vastauslomakkeen täyttämisen sekä lomakkeen palauttamisen.

Lomake annettiin hallitukselle käsiteltäväksi ja täytettäväksi vuoden 2014 tammikuussa. Lomakkeita palautettiin neljä kappaletta: hallituksen puheenjohtajalta (liite 2), isännöitsijältä (liite 3), päällystön edustajalta (liite 4) sekä markkinointipäälliköltä (liite 5). Vastaukset painottuivat siten, että jokainen vastaaja vastasi oman vastuualueensa puitteissa kysymyksiin.

Lisäksi naisosaston edustaja ilmoitti suullisesti vastauksensa. Näistä vastauksista ei tieto-omaisuuden kartoittamisessa ollut juurikaan hyötyä vastausten ollessa joko ”ei ole” tai ”en osaa sanoa”.

Luvuissa 9 ja 11 on käsitelty lyhyesti Turun VPK:n lähiverkon rakennetta sekä liitteinä olevien kyselylomakkeiden vastauksia tietoturvallisuuden eri osa-aluejaon mukaan.

Lisäksi suoritin toimitiloissa omatoimista havainnointia erilaisten järjestelmien turvallisuudesta sekä turvallisuuden tasoista.

Kyselylomakkeiden vastauksista sekä omatoimisesta havainnoinnista laadittiin yhdistykselle tietoturvariskien yhteenveto, joka on liitteenä.

2 TURUN VAPAAEHTOINEN PALOKUNTA RY:N ESITTELY

Turun Vapaaehtoinen Palokunta ry (myöhemmin ”VPK”) on Suomen ja pohjoismaiden vanhin edelleen toiminnassa oleva vapaaehtoinen palokunta. Vuonna 1838 perustettu palokunta toimii Varsinais-Suomen Aluepelastuslaitoksen sopimuspalokuntana sitoutuen miehittämään kaksi sammutusautoa ja yhden säiliöauton sammutussopimuksessa määrätyn ajan puitteissa ympäri vuorokauden vuoden jokaisena päivänä.

Palokunta omistaa ensimmäisen lähdön sammutusauton ja säiliöauton sekä miehistönkuljetusauton. Palokunnan toisen lähdön sammutusauto on Aluepelastuslaitoksen omistama. Palokunnan toiminnan keskuksena toimii vuonna 1892 valmistunut palokunnantalo Turun Eerikinkadun ja Eskelinkadun risteyksessä (Soiri-Snellman 2012, 52). Palokunnantalon juhlasalia vuokrataan erilaisten yksityisten ja julkisten tapahtumien järjestämiseen. Palokunnan autokalusto on sijoitettuna talon Kauppatorin puoleiseen päätyyn vuonna 1952 rakennetun lisärakennuksen pohjakerrokseen.

Palokunnan jäsenmäärä vuoden 2012 lopulla oli 275 henkilöä (Turun VPK 2012, 14). Jäsenet kuuluvat johonkin palokunnan kuudesta osastosta.

Hälytysosasto

Hälytysosaston jäsenet vastaavat palokunnalle osoitettujen sammutus- ja pelastustehtävien suorittamisesta. Osa jäsenistöstä on erikoiskoulutettu erityiseen tehtävään hälytystilanteissa. Tällaisia erikoiskoulutettuja henkilöitä ovat yksikönjohtajat, savusukeltajat, kuljettajat, korkean paikan työskentelijät sekä pintapelastajat.

Hälytysosasto hälytetään Turun Hätäkeskuksen kautta tekstiviestillä ja robottipuhelulla joko päivystävän palomestarin pyynnöstä tai automaattisesti osana hälytysvastetta.

Nuoriso-osasto

Nuoriso-osaston jäsenet harjoittelevat palokuntataitoja, osallistuvat palokunta-kilpailuihin sekä vuosittain järjestettäville palokuntanuorten leireille. Osaston ikärakenne vaihtelee yhdentoista ja kuudentoista ikävuoden välillä. Nuoriso-osasto toimii yhtenä tärkeimmistä kanavista ylläpitää hälytysosaston riittävää jäsenmäärää tulevaisuudessa.

Naisosasto

Naisosasto tukee palokunnan toimintaa suorittamalla hälytysmuonitusta, turvallisuusvalistusta sekä kouluttamalla jäseniään paloturvallisuusasioissa.

Veteraaniosasto

Veteraaniosasto ylläpitää ja vaalii VPK:n palokuntaperinteitä, järjestää vuosittain joulumyyjäiset sekä avustaa palokunnantalolla järjestettävissä palokunnan tapahtumissa tarpeen mukaan.

Järjestöosasto

Järjestöosastoon kuuluvat ne palokunnan jäsenet, jotka eivät kuulu oletusarvoisesti muihin osastoihin. Järjestöosasto suunnittelee ja toteuttaa joka vuosi pidettävän jäsenillan.

Puhallinorkesteri

VPK:n puhallinorkesteri on Suomen vanhin edelleen toiminnassa oleva amatöörisoittokunta. Orkesteri on perustettu vuonna 1873 ja se on julkaissut kolme äänitettä. Puhallinorkesteri järjestää vuosittain kahvikonsertin palokunnantalolla sekä esiintyy useissa tapahtumissa ympäri Suomea sekä Eurooppaa.

Henkilökunta

Tavallisesta sopimuspalokunnasta poiketen VPK:lla on neljä palkattua henkilöä, joista kaksi on kuukausipalkkaisia ja kaksi osa-aikaisia työntekijöitä. Kuukausipalkkaisia työntekijöitä ovat markkinointipäällikkö sekä toimistonhoitaja. Osa-aikaisia työntekijöitä ovat vahtimestari sekä kapellimestari.

3 TIETOTURVA YHDISTYSTOIMINNASSA

European Network and Informaton Security Agencyn vuonna 2012 julkaisemassa tietoturvan uhkaraportissa listattiin, miten mahdolliset tietoturvauhat tulevat lisääntymään tai vähentymään. Huolestuttavaa on, että raportin mukaan ainoastaan roskapostin muodostama uhka tulisi pienenemään kun vastaavasti muut uhat olisivat nousussa. (European Network and Information Security Agency 2012, 3.)

Tietoturva mielletään yleisesti yritysten huolenaiheeksi. Yrityksien olemassaoloa varjostavat taloudelliset riskit, joista suurimpana ja viimeisenä voidaan mainita konkurssi, tila jossa velallisen omaisuus käytetään kokonaisuudessaan velkojien saatavien perimiseksi (Oikeuslaitos 2013). Yhdistystoiminta sekä sen tietoturvariskit ovat kuitenkin yhtä vakavasti otettavia kuin yrityksenkin. Yhdistys voi kärsiä yhtäläisiä vahinkoja, jos se ei ota jollain tasolla kantaa tietoturvariskeihin.

Yhdistyksellä on käytössään tieto-omaisuutta (eng. assets), joka on yhdistykselle rahallisesti tai yhdistystoiminnallisesti tärkeää. Tieto-omaisuus voi olla esimerkiksi tekstitiedosto yhdistyksen jäsenten yhteystiedoista tai yhdistyksen käytössä olevalla palvelimella sijaitseva sisäverkon tietokanta. Yhteistä tieto-omaisuudelle on se, että vaikka niiden rahallinen arvo on vaikeasti määriteltävissä, on tieto-omaisuuden hyödyntämisellä yhdistykselle selkeää rahallista tai toiminnallista hyötyä (Jordan & Silcock 2006, 17).

Esimerkkeinä yhdistyksen tieto-omaisuudesta voidaan mainita

- jäsenrekisteri
- asiakasrekisteri
- reskontra-ohjelma sekä sen tiedot
- yhdistystoiminnan tuottamat dokumentit.

4 TIETOTURVAN PERUSTEET

Tietoturvan tarkoituksena on yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) mukaan turvata organisaation arvokkaita resursseja kuten tietoa, laitteistoa sekä ohjelmistoja (NIST 1995).

Yhdistyksen tietoturvallisuuden tason arvioiminen lähtee ajatuksesta, jonka mukaan yhdistyksellä on olemassa tieto-omaisuutta, jota yhdistyksen on suojeltava. Sen jälkeen yhdistyksen on mietittävä, mitkä asiat uhkaavat yhdistyksen tieto-omaisuutta. Lopuksi yhdistyksen on mietittävä, miten näitä uhkia vastaan voidaan suojautua. (Stallings & Brown 2008, 7.)

Yksinkertaisimmillaan tieto-omaisuuden turvallisuus katsotaan turvatuksi, kun niin sanottu CIA-triadi toteutuu (Andress 2011, 4). Tämä tarkoittaa tilannetta, jossa tietoturvallisuuden hyväksyttävä taso on saavutettu, kun tieto-omaisuuden luottamuksellisuus, eheys sekä saatavuus täyttyvät hallittavassa kompromississa.

Hallittava kompromissi tarkoittaa, ettei täydellistä tietoturvaa voida saavuttaa koskaan. Täydellinen tietoturva tarkoittaisi äärimmilleen vietynä sellaista tilannetta, jossa tieto-omaisuus – esimerkiksi palvelin – lukittaisiin paloturvalliseen, ilmatiiviiseen maanalaiseen kassakaappiin, joka peitettäisiin betonilla ja jota vartioimaan asetettaisiin täysipäiväisesti kaksi aseistettua vartijaa. Tällöin saavutettaisiin ideaalitilanne, jossa palvelimen sisältämät tiedot olisivat turvassa.

Vastaavasti kukaan ei voisi hyödyntää palvelimen tietoja, kuten jäsenrekisteriä, jolloin yhdistyksen hallinnolliset toimet muuttuisivat mahdottomiksi. Yhdistyksen on siis sallittava pääsy tietokoneen sisältämiin tietoihin. Yhdistys ottaa tällöin riskin, jossa myös joku ulkopuolinen henkilö pääsee tietoihin käsiksi. Riskienhallinnan tarkoituksena on pyrkiä minimoimaan tällainen riski sellaiselle tasolle, jonka yhdistys voi hyväksyä (Landoll, 2011, 4).

CIA-triadin lisäksi tietoturvallisuuden osa-alueiksi voidaan lukea Parkerin heksadin mukaisesti myös hallinta (control), aitous (authenticity) sekä hyödyllisyys

(utility) (Andress 2011, 6). Vaikka Parkerin heksadi laajentaa tietoturvallisuuden käsitettä, tullaan tässä opinnäytetyössä keskittymään pelkästään CIA-triadiin.

Luottamuksellisuus

Luottamuksellisuus (Confidentiality) tarkoittaa tieto-omaisuuden sisältämän sanoman tahallisen tai tahattoman paljastamisen estämistä (Krutz & Vines 2003, 3). Sillä myös tarkoitetaan tilannetta, jossa tieto-omaisuus on suojattu asiattomalta käsittelyltä (Stallings & Brown 2008, 8). Luottamuksellisuus pyritään saavuttamaan käyttämällä salasanoja sekä käyttäjätunnuksia suojauksen kohteena oleviin tietojärjestelmiin (Hakala ym. 2006, 4).

Eheys

Eheys (Integrity) tarkoittaa, että tietojärjestelmän sisältämä tieto on paikkansa pitävää ja virheetöntä (Hakala ym. 2006, 4). Tämä saavutetaan varmistamalla muun muassa, että

- valtuuttamattomat henkilöt eivät pääse muokkaamaan tietoa
- valtuutetut henkilöt tai prosessit pääsevät tekemään ainoastaan sellaisia muutoksia, joihin heillä on valtuudet
- tiedot ovat yhdenmukaisia keskenään ja ulkoisen todellisuuden kanssa. (Krutz & Vines 2003, 3.)

Eheyteen pyritään mahdollisimman vikasietoisilla järjestelmillä, varmuuskopioinnilla (Jordan & Silcock 2006, 167) sekä ohjelmistoteknisillä ratkaisuilla, joissa ohjelmistoihin voidaan määrittää syöttörajoituksia tai syötteen tarkistuksia (Hakala ym. 2006, 5). Valtuutuksien suhteen toimitaan käyttämällä käyttäjätilejä, joilla on pääsy vain kaikkein välttämättömimpään dataan, kaikkein välttämättömimmillä työkaluilla varustettuna. Tätä kutsutaan pienimmän oikeuden periaatteeksi. (Andress 2011, 34.)

Saatavuus

Saatavuuden (Availability) osa-alue tarkoittaa järjestelmän tai tiedon olevan valtuutettujen henkilöiden tai tietoprosessien käytettävissä silloin, kun tietoon tai järjestelmään on päästävä käsiksi (Andress 2008, 6).

Tällaisena esimerkkinä voidaan mainita verkkosivu, jonka tieto on täysin julkista, mutta samalla sen tulee olla ehdottoman totta sekä vielä tarvittaessa saatavilla. Tällöin verkkosivun luottamuksellisuudella ei ole suurta merkitystä, mutta sen saatavuudella ja luotettavuudella puolestaan on.

Kyseisen verkkosivun hallintaan ja muokkaamiseen tarvittavien käyttäjätilien osalta puolestaan kaikkien kolmen osa-alueen olemassaololla on suuri merkitys. Jos käyttäjätilin saatavuus poistetaan kokonaan joko poistamalla käyttäjätili tai rajoittamalla sen oikeuksia muokata sivua, ei kyseisellä sivulla olevaa, mahdollisesti virheellistä tietoa päästä korjaamaan välittömästi.

Jos taas verkkosivun käyttäjätilin luottamuksellisuus vaarantuu siten, että käyttäjätilin tunnus ja salasana päätyvät ulkopuolisen henkilön käsiin, ei sivun sisältämän tiedon voida katsoa olevan enää yhtä luottamuksellista. Tässä tapauksessa verkkosivun tekstin kirjoittajasta ei ole täyttä varmuutta. Jos verkkosivun käyttäjätilin luottamuksellisuus vaarantuu, vaikuttaa se myös verkkosivulla olevan tiedon ja käyttäjätilin sisältämien tietojen eheyteen.

5 RISKI, UHKA JA HAAVOITTUVUUS

Tietoturvariski on NIST:n mukaan uhan hyväksikäyttämä haavoittuvuus, jolla pyritään luomaan haittavaikutuksia organisaation toimintaan (NIST 2006, 85). Riskin suuruus voidaan määritellä yhtälömuotoon:

Riski = Tieto-omaisuus x Uhka x Haavoittuvuus

Yhtälössä riskin suuruus määrittyy organisaation tieto-omaisuuden arvolla, uhkien todennäköisyydellä sekä haavoittuvuuksien kriittisyydellä (Landoll 2011, 366). Riskin arviointi vaatii uhkien huolellista analysointia sekä tietoa olemassa olevista haavoittuvuuksista, jotta voidaan päätellä, mitkä tilanteet tai tapahtumat voisivat vaikuttaa organisaatioon sekä todennäköisyys miksi näin tapahtuisi (NIST 2012, 6).

Kuten luvussa neljä kerrottiin, tietoturva koostuu kolmesta osa-alueesta: luottamuksellisuudesta, eheydestä ja saatavuudesta. Tietoturvauhka on jokin näiden kolmen vastakohdasta: paljastuminen, muuttuminen tai tuhoutuminen (Krutz & Vines 2003, 3), kuten taulukossa 1 on esitetty. Tietoturvauhaksi voidaan määritellä myös mikä tahansa tapahtuma, jolla on tieto-omaisuuteen ei-haluttuja vaikutuksia (Landoll 2011, 27).

Taulukko 1. Tietoturvallisuuden osa-alueet ja niihin kohdistuvat uhat.

Tietoturvallisuuden osa-alue	**Vastaava tietoturvauhka**
Luottamuksellisuus	Paljastuminen
Eheys	Muuttuminen
Saatavuus	Tuhoutuminen

Tietoturvauhkaan liittyy uhka-agentiksi kutsuttu itsenäinen kokonaisuus, joka voi mahdollistaa uhan toteutumisen. Uhka-agentteja voivat olla luonto, jonka muo-

dostamana uhkana voidaan pitää esimerkiksi tulvaa. Myös ihmiskunta voi toimia uhka-agenttina, jonka mahdollistama uhka voi olla luottamuksellisten tietojen julkistaminen. (Landoll 2011, 27.)

Haavoittuvuudella tarkoitetaan tilannetta, jossa tieto-omaisuutta ei ole suojattu ollenkaan tai omaisuuden suojaustaso on heikko, mikä mahdollistaa pääsyn tieto-omaisuuteen (Krutz & Vines 2003, 17). Yleisimpänä esimerkkinä haavoittuvuudesta voidaan pitää käyttöjärjestelmää, jota ei päivitetä.

6 TIETOTURVALLISUUDEN OSA-ALUEET

Hakala, Vainio ja Vuorinen jakavat kirjassaan (2006, 10) tietoturvallisuuden seitsemään eri osa-alueeseen. Tämä osa-alueisiin jakaminen selkeyttää tietoturvadokumenttien rakennetta sekä auttaa hallitsemaan riskienhallinnan kokonaiskuvaa.

Hakala ja muut jaottelevat tietoturvallisuuden seuraaviin osa-alueisiin:

- hallinnollinen turvallisuus
- fyysinen turvallisuus
- henkilöstöturvallisuus
- tietoaineistoturvallisuus
- ohjelmistoturvallisuus
- laitteistoturvallisuus
- tietoliikenneturvallisuus (Hakala ym. 2006, 10).

Osa-alueiden jaottelu voi poiketa yllä esitetystä. Esimerkiksi Juha Miettinen luettelee kirjassaan kymmenen eri tietoturvallisuuden osa-aluetta. Edellä olevien lisäksi Miettinen listaa tietojenkäsittelyn turvallisuuden, käyttöturvallisuuden sekä yksityisyyden suojan erillisiksi osa-alueiksi. (Miettinen 2006, 15.)

Hallinnollinen turvallisuus

Hallinto vastaa yhdistyksen turvallisuudesta ja viimeisenä kantaa vastuun sen ylläpidosta tai laiminlyönnistä (Landoll 2011, 155). Hallinnon onkin määriteltävä, ketkä tietoturvallisuudesta sekä sen osa-alueista vastaavat (Laaksonen ym. 2006, 128). Hallinnollinen turvallisuus on yleensä tietohallinnon alainen toimialue (Hakala ym. 2006, 11).

Hallinnollisen turvallisuuden tehtävänä on koota eri turvallisuuden osa-alueet yhtenäiseksi, hallittavaksi kokonaisuudeksi (Miettinen 2006, 18). Edellä mainittujen tehtävien lisäksi hallinnolliseen turvallisuuteen kuuluu yhteydenpito erilaisiin turvallisuustoimijoihin joko yhdistyksen sisällä tai sen ulkopuolella sekä myös yhteydenpito erilaisiin turvallisuusviranomaisiin (Hakala ym. 2006, 10).

Fyysinen turvallisuus

Fyysisen turvallisuuden tavoitteena on taata yhdistykselle turvallinen ja häiriötön toimintaympäristö (Laaksonen ym. 2006, 125) siten, että toimitiloihin pääsee valvotusti ja turvallisesti (Miettinen 2006, 19).

Edellä mainittu turvallinen toimintaympäristö saavutetaan suojaamalla toimitilat erilaisilta fyysisiltä uhilta. Tällaisia ovat muun muassa ilkivalta, murrot, vesivahingot, tulipalot sekä sähkö- ja lämmitysjärjestelmän toimintahäiriöt. (Hakala ym. 2006, 11.)

On huomioitavaa, että kaikki yhdistyksen toimitilat eivät tarvitse samantasoista suojausta. Yhdistyksen on suojattava tehokkaammin sen omiin vahvuusalueisiin liittyviä tiloja kuten kalustohallia, perinnehuonetta, hallituksen huonetta, arkistoa, miehistötiloja ja toimistoa (Laaksonen ym. 2006, 125).

Yleensä fyysisen turvallisuuden alle lueteltujen asioiden ylläpito on ulkoistettu kolmannelle osapuolelle, esimerkiksi vartiointiyritykselle, joka asentaa toimitiloihin murto- ja palohälyttimet. Myös kiinteistöhuoltoyritykset huolehtivat fyysisestä turvallisuudesta vastaamalla lämmitysjärjestelmien toiminnasta sekä huolehtimalla muun muassa pihavalaistuksen toimivuudesta. (Hakala ym. 2006, 11.)

Henkilöstöturvallisuus

Henkilöstöturvallisuuden tavoitteena on henkilöstön toimista tapahtuvien tietoturvauhkien sekä järjestelmiä käyttävän henkilöstön turvallisuusuhkien hallintaa (Laaksonen ym. 2006, 138). Henkilöstöturvallisuus kattaa niin yhdistyksen jäse-

net, sen työntekijät kuin yhdistyksen sidosryhmien henkilötkin (Miettinen 2006, 18).

Tavallisimmat toimet henkilöstöturvallisuuden varmistamiseksi ovat henkilöstön taustaselvitys palkkaustilanteessa, rajattujen käyttöoikeuksien myöntäminen henkilöstölle sekä avainten palautus työsuhteen tai jäsenyyden päätyttyä (Landoll 2011, 146-154).

Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen kuuluvat tietojen säilyttämiseen, varmuuskopiointiin, palauttamiseen sekä tuhoamiseen liittyvät toimet. Myös sähköisistä järjestelmistä otetut tulosteet kuuluvat tietoaineistoturvallisuuden piiriin. (Hakala ym. 2006, 11.)

Yleisenä ohjeena tulosteiden käsittelystä voidaan pitää ”puhtaan pöydän sääntöä”, jossa organisaation työntekijät eivät pidä näkyvillä mitään arkaluonteista tietoa sisältävää aineistoa (Laaksonen ym. 2006, 169).

Ohjelmistoturvallisuus

Ohjelmistoturvallisuuden tarkoituksena on varmistaa ohjelmistojen tarkoituksenmukaisuus tarkoitettuun tehtävään, niiden keskinäinen yhteensopivuus sekä toiminnan virheettömyys (Hakala ym. 2006, 11).

Miettinen jakaa ohjelmistoturvallisuuden kirjassaan (2006, 21) kahteen eri alaosioon: sisäisten suojausominaisuuksien ohjelmistoihin ja erityisesti suojaamiseen tarkoitettuihin ohjelmistoihin. Sisäisiksi suojausominaisuuksiksi Miettinen listaa lokitietojen keruun, salasanojen vanhenemisen automaattisen valvonnan sekä ohjelmistojen pääsyoikeuksien hallinnan. Erityisesti suojaamiseen tarkoitetuista ohjelmistoista Miettinen nostaa esille virustorjunta-, varmuuskopiointi-, sekä salausohjelmistot. (Miettinen 2006, 21.)

Laitteistoturvallisuus

Laitteistoturvallisuus keskittyy organisaation käytössä olevien laitteiden turvallisuuteen siten, että organisaatiolle hankitaan vain toiminnaltaan varmoja laitteita, joiden tietoturvallisuuteen on keskitytty suunnitteluvaiheessa ja joiden komponenttien saatavuus on taattu tulevaisuudessa (Miettinen 2006, 21). Näiden lisäksi osa-alueeseen kuuluvat laitteiden huollot sekä organisaation varautuminen laitekannan vanhentumiseen (Hakala ym. 2011, 12).

Laitteistoturvallisuus linkittyy läheisesti hyvään IT-omaisuuden hallintaan. Tämän saavuttamiseksi laitteista, niiden hankinnoista, ylläpidosta, ohjelmista, ohjelmien lisensseistä sekä käyttäjäoikeuksista tulisi pitää kirjaa. (Laaksonen ym. 2006, 223.)

Tietoliikenneturvallisuus

Tietoliikenneturvallisuus keskittyy verkkoyhteyksien sekä muiden viestintäjärjestelmien turvallisuuteen (Hakala ym. 2006, 12). Sillä suojataan yrityksen käsittelemä tieto, kun se kulkee yrityksen sisäisessä verkossa tai internet-operaattorin verkossa. Tavoitteena on, että lähetetty tieto päätyy oikealle vastaanottajalle muuttumattomana. (Miettinen 2006, 20.)

7 TIETOTURVARISKIEN ANALYYSI

Tietoturvariskien analyysissä tutkitaan, kuinka hyvin analyysin kohteena oleva tieto-omaisuus, esimerkiksi verkko, ohjelmisto, dokumentit ja henkilöstö, on suojattu erilaisia uhkia vastaan (NIST 2008, 12). Riskianalyysi voidaan jakaa karkeasti kahteen osa-alueeseen: riskikartoitukseen sekä riskien arviointiin (Hakala ym. 2006, 80).

Riskikartoituksessa etsitään paitsi yleisluontoisia riskejä, jotka voisivat uhata organisaation tietoturvallisuutta, myös tietojärjestelmäkohtaisia riskejä (Hakala ym. 2006, 81). Riskien arvioinnin ihannetilanteessa jokainen tieto-omaisuuden muoto analysoidaan ja sen mahdolliset riskit arvioidaan. Arviointi voi olla määrällinen tai laadullinen. Tämä arviointi antaa organisaation johdolle mahdollisuuden asettaa riskit tärkeysjärjestykseen. (ISO/IEC 27005 2011, 26.)

Jos riski on liian suuri hallittavaksi, organisaation on toimittava siten, että riski saadaan pienennettyä hallittavalle tasolle (Stallings & Brown. 2008, 515).

Tietoturvariskianalyysi prosessina jakautuu seuraaviin osa-alueisiin:

- tieto-omaisuuden tunnistaminen
- uhkien, riskien ja haavoittuvuuksien analysointi
- toteutuneiden riskien vaikutukset organisaatiolle sekä
- riskien hallintamenetelmät (Stallings & Brown 2008, 521-528).

7.1 Riskianalyysityökalut

Riskianalyysejä varten on kehitetty erilaisia ilmaisia sekä maksullisia riskianalyysidokumenttipohjia, jotka toimivat tarkistuslista-periaatteella. Santa Fe -ryhmän omistuksessa oleva Shared Assesments -projekti on luonut taulukkolaskentaohjelmassa toimivan tarkistuslistan, jolla organisaatiot voivat tarkistaa tieto-omaisuutensa riskitekijät (Shared Assesments 2013).

Toinen yleisesti käytössä oleva tarkistuslista-tyyppinen riskianalyysityökalu on yhdysvaltalaisen Software Engineering Instituten CERT-ohjelman alaisuudessa julkaistu ja ylläpidettävä Octave-niminen (Operationally Critical Threat, Asset and Vulnerability Evaluation) analyysityökalu. Octave jakautuu kolmeen erilaiseen tarkastuslistaan:

- Alkuperäinen Octave-tarkastuslista
- Octave-S pienille organisaatioille
- Octave Allegro, joka on kevennetty versio alkuperäisestä Octavesta. (Software Engineering Institute 2013.)

7.2 Octave-S

Opinnäytetyön riskianalyysin suoritukseen Octave-S antaa parhaat lähtökohdat, sillä se on suunniteltu alle sadan hengen organisaatioille (Software Engineering Institute 2013). Octave-S ei ole puhdas työkalu, vaan prosessimuotoinen metodi, jolla yhdistys voi tunnistaa, priorisoida ja hallita tietoturvariskejään (ISACA 2009).

7.3 Tietoturvariskien hallinta

Kun tietoturvariskit on tunnistettu, voi yhdistyksen hallinto päättää hallita riskejä neljällä tavalla. Mahdolliset tavat ovat seuraavat:

- riskin vähentäminen, jolloin käytetään suositeltuja turvallisuustekijöitä kuten palomuurin asetusten muuttamista vähentämään olemassa olevan riskin suuruutta
- riskin ulkoistaminen, jolloin riskin hallinta annetaan kolmannelle osapuolelle esimerkiksi ostamalla vakuutus tieto-omaisuudelle, rakennukselle tai henkilöstölle

- riskin hyväksyminen, jolloin yhdistys elää riskin uhan ja sen toteutumisen kanssa
- riskin välttäminen, jolloin yhdistys eliminoi mahdollisen riskin kokonaan esimerkiksi sulkemalla tarpeettomat TCP-portit palvelimelta.

Se, mikä riski on yhdistykselle sopivin hallita olemassa olevilla resursseilla, riippuu täysin yhdistyksen tietoturvallisuuden tahtotasosta ja siitä, millaisten riskien kanssa yhdistys on tekemisissä. (Landoll 2011, 389.)

Tietoturvariskien hallintaprosessi

Tietoturvariskien hallinnan tulisi olla jatkuva prosessi, eikä kertaluontoinen tapahtuma. Tietoturvariskin hallintaprosessin tarkoituksena on antaa yhdistyksen vastaavalle hallinnolle kokonaisvaltainen kuva olemassa olevista suojausmenetelmistä, uhkista joita vastaan niillä suojaudutaan, riskeistä jotka muodostuvat olemassa olevista uhista sekä suojauksen kohteena olevasta tietoomaisuudesta. (ISO/IEC 27005 2011, 18.)

Tietoturvariskien hallintaprosessi koostuu arviointiympäristön määrittämisestä, riskien arvioinnista, riskien käsittelystä, riskien hyväksynnästä, riskeistä viestinnästä sekä riskien tarkkailusta ja katselmoinnista (ISO/IEC 27005 2011, 18).

Tietoturvariskin hallintajärjestelmäprosessi toteutuu niin kutsutun PDCA-syklin avulla, kuten taulukosta 2 nähdään. PDCA on lyhenne englannin kielen sanoista Plan (suunnittele), Do (toteuta), Check (tarkasta) sekä Act (toimi) (ISO/IEC 27005 2011, 24).

Taulukko 2. Tietoturvallisuuden hallintajärjestelmän ja tietoturvariskien hallintaprosessin liittyminen toisiinsa ISO/IEC 27005:2011 -standardin mukaan.

Tietoturvallisuuden hallintajärjestelmäprosessi	**Tietoturvariskien hallintaprosessi**
Suunnittele (Plan)	Määritetään tietoturvariskien arviointiympäristö, arvioidaan riskit, laaditaan riskien käsittelysuunnitelma sekä hyväksytään riskit
Toteuta (Do)	Toteutetaan edellä suunniteltu riskien käsittelysuunnitelma
Tarkasta (Check)	Tarkkaillaan ja katselmoidaan riskejä jatkuvasti
Toimi (Act)	Ylläpidetään ja parannetaan tietoturvariskien hallintaprosessia

8 YHDISTYS JA LAINSÄÄDÄNTÖ

Yhdistysten toimintaa Suomessa säätelee Yhdistyslaki. Yhdistyslaissa määritellään muun muassa yhdistyksen perustamista, hallintoa sekä tilintarkastusta koskevia asioita. Yhdistyslaki velvoittaa yhdistyksen pitämään jäsenluetteloa (Yhdistyslaki 30.12.1992/1614).

> Yhdistyksen jäsenistä on hallituksen pidettävä luetteloa. Luetteloon on merkittävä kunkin jäsenen täydellinen nimi ja kotipaikka. [..] Yhdistyksen jäsenelle on pyydettäessä varattava tilaisuus tutustua 1 momentissa tarkoitettuihin tietoihin. Jäsenluettelossa olevien tietojen luovuttamisesta muutoin säädetään henkilörekisterilaissa.

Kuten lainauksesta nähdään, yhdistyksen on pidettävä jäsenistään kirjaa. Laki määrittelee riittäväksi jäsenluetteloksi jäsenen nimen ja kotipaikkakunnan. Yhdistykselle nimi ja kotipaikkakunta ovat usein riittämättömät jäsentiedot, varsinkin jos yhdistys kerää jäsenmaksuja, joiden maksamista varten lähetetään lasku kirjepostina yhdistyksen jäsenille. Tällöin yhdistyksen on pidettävä osoitetietolistaa, josta selviävät yhdistyksen jäsenten kotiosoitteet.

8.1 Henkilötieto

Henkilötieto määritellään laissa hyvin laajasti. Innasen ja Saarimäen (2012, 86) mukaan henkilötiedolla tarkoitetaan

> ..kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.

Tästä johtuen voidaan todeta, että edellä mainittu jäsenluettelo itsessään on jo henkilötietoja sisältävä lista, johon sovelletaan henkilötietolakia. Samainen laki velvoittaa rekisterinpitäjän käsittelemään tietoja siten, ettei rekisterissä olevan yksityisyyden suojan turvaavia perusoikeuksia tulla rajoittamaan ilman laissa olevaa perustetta (Innanen & Saarimäki, 2012, 89). Lain määrittämiä perusteita on olemassa yhdeksän kappaletta (Innanen & Saarimäki 2012, 88), joista yhdistystoiminnan osalta tärkeimmät ovat yhteysvaatimus, asiakasyhteys sekä rekisterinpitäjän toimesta tapahtuva maksupalvelu.

Yhteysvaatimuksella tarkoitetaan tilannetta, jossa rekisteröidyllä on jäsenyyden tai muun vastaavan suhteen vuoksi asiallinen yhteys rekisterinpitäjään. Asiakasyhteys on asiakkuussuhteen vuoksi ylläpidettävä rekisteri yhdistyksen asiakkaista sekä heidän yhteystiedoistaan. Rekisterinpitäjän toimesta tapahtuva maksupalvelu linkittyy asiakasyhteyteen. (Innanen & Saarinen 2012, 88.)

8.2 Rekisteri-ilmoitus

Henkilötietolaki määrää rekisterinpitäjän ilmoittamaan tietosuojavaltuutetulle automaattisella tietojenkäsittelyllä ylläpidetystä henkilörekisteristä lähettämällä tälle rekisteriseloste. Lakiin on kuitenkin kirjattu poikkeustapauksia, joissa ilmoitusta ei vaadita. Tällaiset poikkeukset ovat edellisessä kappaleessa mainitut jäsenyys- sekä asiakkuussuhteet. (Henkilötietolaki 22.4.1999/523.)

8.3 Henkilötietojen tietoturva-vaatimukset

Henkilötietolaki ei suoraan määrittele teknisiä tai hallinnollisia vaatimuksia, joilla varmistettaisiin yhdistyksen keräämien henkilötietojen tietoturvallisuus. Henkilörekisterin tietoturvallisuuden tason laki määrittelee seuraavasti (22.4.1999):

> Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Lisäksi Henkilötietolaki määrää huolellisuusvelvoitteesta siten, että rekisterinpitäjän on huolehdittava henkilötietojen laillisesta käsittelystä, huolellisuuden noudattamisesta sekä hyvän tietojenkäsittelytavan noudattamisesta. Huolellisuusvelvoite määrää lisäksi rekisterinpitäjän huolehtimaan, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laillista perustetta. (Henkilötietolaki 22.4.1999/523.)

Hyvällä tietojenkäsittelytavalla tarkoitetaan tietojenkäsittelyssä suunnittelu-, tarpeellisuus-, huolellisuus- ja suojaamisvelvoitteita sekä rekisteröityjen henkilöiden oikeuksien huomioon ottamista (Tietosuojavaltuutettu 2013).

9 TURUN VPK:N TIETOTURVATARKASTUS (SALATTU)

10 JOHTOPÄÄTÖKSET, RISKIANALYYSIT SEKÄ TOIMINTASUOSITUKSET (SALATTU)

11 YHTEENVETO

Opinnäytetyön tarkoituksena oli suorittaa tietoturvallisuuden riskianalyysi Turun Vapaaehtoiselle Palokunnalle sekä antaa tietoturvallisuutta parantavia toimenpide-ehdotuksia. Sopimuspalokunnilla ei ole tietoturvaohjeistusta aluepelastuslaitoksien toimesta, eivätkä sopimuspalokuntayhdistyksen toimijat välttämättä tiedosta kaikkia tietoturvallisuuden riskejä, joita pelastus- ja yhdistystoiminnassa käsiteltävien dokumenttien ja tiedostojen osalta muodostuu.

Tietoturvallisuus sekä etenkin riskienhallinta käsitteenä kattaa hyvinkin laajasti yhdistystoiminnan eri osa-alueita. Koska aiheet ovat yhteneviä monelta osalta, oli opinnäytetyön vaarana työn laajuuden leviäminen hallitsemattomiin mittoihin. Riskienhallinnan analyysityö on yksityiskohtiin asti pureutuvaa selvitystyötä, jonka vuoksi riskianalyysissä keskityttiin enimmäkseen suurten linjojen analysoimiseen. Aikataulujen puitteissa ei yhdellä hengellä suoritettavassa riskianalyysissä voitu analysoida muun muassa tietokoneiden ajureiden mahdollisia haavoittuvuuksia. Jos yhdistyksen koko tai työn viitekehys olisi ollut suurempi, olisi riskianalyysityöhön vaadittu kahden henkilön työpanos.

Opinnäytetyön teoriamateriaalia oli runsaasti saatavilla ja se oli hyvin ajantasaista. Suurimmaksi ongelmaksi muodostui saatavilla olevien riskianalyysityökalujen, kuten Octave-S, sisältämät laajat aihe- ja toimenpideohjeistukset, jotka eivät sellaisenaan käyneet opinnäytetyöhön. Koska Octave-S on suunniteltu yrityksiä varten, joilla on käytössään pääomaa, tuottotavoitteita sekä palkattua henkilöstöä moninkertainen määrä verrattuna sopimuspalokuntayhdistykseen, eivät jotkut Octave-S:n kysymykset sovellu sellaisenaan ollenkaan käytettäväksi. Octaven tehtäväpaperit kuitenkin antoivat työhön selkeän tiekartan yhdessä Douglas Landollin kirjan kanssa.

Riskianalyysi onnistui tavoitteisiin, työmäärään ja saatuihin vastauksiin suhteutettuna erinomaisesti. Yhdistys oli alusta alkaen positiivisella ja myönteisellä kannalla opinnäytetyön aihetta ja sen toteutusta kohtaan.

Itselleni näen opinnäytetyöstä olleen pelkkää ammatillista hyötyä: opinnäytetyö syvensi ymmärrystäni riskienhallintaan sekä sen osa-alueisiin ja rohkaisi jatkamaan omatoimista opiskelua riskienhallinnan saralla.

Kehitettäviksi asioiksi voitaisiin mainita yhteydenpidon kohdeyhdistyksen jäsenten sekä toimeksiantajan välillä. Etenkin riskianalyysien ja uhkien arvottamisessa tulisi ehdottomasti toimia yhteistyössä riskejä ja niiden vaikutuksia arvioiden.

LÄHTEET

Abloy 2014. Abloy Protec Cliq -teknologia osana lukitus- ja avainjärjestelmää. Viitattu 24.2.2014. http://www.abloy.fi/fi/abloy/abloyfi/Tuotteet/?groupId=1768&productId=896.

Andress, J. 2011. The Basics of Information Security. Waltham: Elsevier publishing.

Brenton, C. & Hunt, C. 2003. Mastering Network Security. Alameda, Sybex.

European Network and Information Security Agency 2012. Threat Landscape. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape.

Henkilötietolaki 22.4.1999/523.

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

Innanen, A. & Saarimäki, J. 2012. Internetoikeus. Helsinki: Edita Publishing.

ISACA 2009. The OCTAVE Approach to Information Risk Assesment. http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Pages/The-OCTAVE-Approach-to-Information-Security-Risk-Assessment1.aspx.

ISO/IEC 27005. 2011. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta.

Jordan, E. & Silcock, L. 2006. Strateginen IT-riskien hallinta. Suom. Kaskas Design. Helsinki: Edita Prima.

Kirjapitolaki 30.12.1997/523.

Krutz, D. & Vines, R. 2003. Tietoturvasertifikaatti. Helsinki: Edita Prima.

Laaksonen, M.; Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Landoll, D. 2011. The Security Risk Assesment Handbook. Boca Raton: CRC Press.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen – Näin turvaat yrityksesi toiminnan. Helsinki: Kauppakaari.

NIST 1995. An Introduction to Computer Security. Viitattu 24.10.2013. http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter2.html.

NIST 2006. Information Security Handbook: A Guide for Managers. Viitattu 24.10.2013. http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

NIST 2008. Technical Guide to Information Security Testing and Assesment. Viitattu 25.10.2013. http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

NIST 2012. Guide for Conducting Risk Assesment, Revision 1. Viitattu 24.10.2013. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

Oikeuslaitos 2013. Konkurssi. Viitattu 17.9.2013 http://www.oikeus.fi/5903.htm.

Oikeusministeriö 2014. Rikostaustan tarkistaminen vapaaehtoistoiminnassa. Viitattu 9.3.2014. http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/rikosoikeus/rikostaustantarkistaminenvapaaehtoistoiminnassa.html

Shared Assesments 2013. About Shared Assesments. Viitattu 4.11.2013. http://sharedassessments.org/about/.

Software Engineering Institute 2013. OCTAVE. Viitattu 4.11.2013. https://www.cert.org/octave/.

Soiri-Snellman, H. 2012. Brankku – Turun VPK:n talo. Turku: Turun Vapaaehtoinen Palokunta ry / Turun Museokeskus.

Stallings, W. & Brown, L. 2008. Computer Security – Principles and Practice. Upper Saddle River: Pearson Education.

Suomen Sopimuspalokuntien Liitto 2013. Tietoa ja tunnuslukuja pelastustoimesta. Viitattu 20.5.2013. http://www.sspl.fi/?id=222.

Tietosuojavaltuutettu 2013. Sanastoa. Viitattu 4.11.2013 http://www.tietosuoja.fi/27247.htm#kohta2.

Turun VPK 2012. Toimintakertomus vuodelta 2012, viitattu 20.5.2013.

Yhdistyslaki 30.12.1992/1614.