Opinnäytetyö (AMK)

Liiketalous, Tietojenkäsittelyn ko.

Yrityksen tietoliikenne ja tietoturva

2015

Mira Lahtinen

TIETOTURVA JA TIETOTURVALLINEN TOIMINTA

– koulutusmateriaali julkishallinnon organisaation henkilöstölle

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalous, tietojenkäsittelyn koulutusohjelma | Yrityksen tietoliikenne ja tietoturva

2015 | 34 sivua

Matti Kuikka

Mira Lahtinen

TIETOTURVA JA TIETOTURVALLINEN TOIMINTA – KOULUTUSMATERIAALI JULKISHALLINNON ORGANISAATION HENKILÖSTÖLLE

Tämän opinnäytetyön keskeisiä tavoitteita ovat tietoturvaan liittyvän teorian kartoittaminen sekä tietoturvakoulutusmateriaalin valmistelu toimeksiantajalle julkishallinnon organisaation perushenkilöstölle tarjottavan koulutuskokonaisuuden tueksi. Opinnäytetyö toteutettiin toimeksiantona Turun yliopiston kehittämis- ja koulutuspalveluja tarjoavalle Brahea-keskukselle.

Opinnäytetyön teoriaosuudessa tutustutaan tietoturvaan, sen uhkatekijöihin sekä organisaation tietoturvalliseen toimintaan. Teoriapohjan kartoituksen jälkeen selvitetään mahdollisen kohdeorganisaation tietoturvan nykytilaa haastattelun avulla. Haastattelun tuloksiin ja teoriaan perustuen kirjoitetaan koulutusmateriaali, jolla organisaation työntekijöiden toimintaa pyritään ohjaamaan tietoturvallisempaan suuntaan. Varsinaisen koulutustilaisuuden seuranta ja arviointiosuus rajataan työn ulkopuolelle.

Teoreettisen tietopohjan sekä mahdolliseen kohdeorganisaatioon tehdyn haastattelun avulla opinnäytetyön tuloksena valmistui tietoturvaa ja tietoturvallista toimintaa organisaatiossa käsittelevä koulutusmateriaali.

Tietoturvaa uhkaavat muun muassa laitteistoon, tietoliikenteeseen, ohjelmistoihin, ympäristöön sekä ihmisiin liittyvät tekijät. Tietoturvan ylläpito vaatii lukuisia toimia, joista kouluttaminen on vain yksi osa. Oikein kohdennetulla koulutuksella voidaan kuitenkin vähentää esimerkiksi henkilöstön osaamattomuudesta tai tietämättömyydestä aiheutuvia tietoturvauhkia.

ASIASANAT:

Tietoturva, koulutus, koulutusmateriaali, henkilöstö

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of Business Administration, Information Technology | Telecommunications and Information Security

2015 | 34 pages

Matti Kuikka

Mira Lahtinen

INFORMATION SECURITY AND SAFE INFORMATION HANDLING – TRAINING MATERIAL

This thesis was commissioned by Brahea Centre which is a service and collaboration unit of the University of Turku. The purpose of this thesis was to provide security training material as part of a basic training package provided to the staff of a public administration organization.

This thesis examines information security, threats, and an organization's safe information handling. The needs of the possible target organization's education are examined through interview survey and on the basis of theory. The survey provides educational material which aims to lead employee's daily procedures towards safe information handling.

The theoretical base combined with the interview survey allowed for the completion of the required information security training material.

Information security threats can be caused by either intentional or accidental actions concerning environmental and human factors, telecommunication or information systems. Security management requires a number of actions of which training is only one part. However, properly targeted training can significantly reduce security threats caused by, for example, employees' lack of knowledge.

KEYWORDS:

Information security, data security, education, staff

SISÄLTÖ

LIITTEET

KUVAT

KUVIOT

TAULUKOT

SANASTO JA KÄYTETYT LYHENTEET

Asiakirja	Dokumentti, josta tietosisällön lisäksi on saatavilla asiakirjan luomiseen liittyvä konteksti (Arkistolaitos 2015).
Biometrinen tunnistus	Henkilön tunnistamista ihmisen ainutlaatuisia piirteitä hyväksikäyttäen. Tunnistus voi perustua esimerkiksi kasvoihin, ääneen tai sormenjälkiin. (Tietosuojavaltuutetun toimisto 2010.)
Kaistanleveys	Tiedonsiirtokanavan tiedonsiirtonopeus (Kotimikro 2009).
LAN	Rajoitetulla alueella toimiva tietoliikenneverkko. (engl. Local Area Network)
Palomuuri	Ohjelma tai laite, joka hallinnoi tietoliikennettä estämällä tai sallimalla tiedon pääsyn tietokoneeseen (Microsoft 2015a).
Palvelin	Tietokone, joka tarjoaa palvelinohjelmistojen avulla palveluja muille ohjelmille (Linux.fi 2015).
Palvelunestohyökkäys	Verkkohyökkäys, jonka tarkoituksena on estää tietyn kohdejärjestelmän tai palvelun käyttö ylikuormittamalla (Digitoday 2007).
Reititin, reititys	Reitittimiä, keskittimiä, kytkimiä ja tukiasemia käytetään verkossa yhdistämään tietokoneita toisiinsa. Reititin mahdollistaa tiedon siirron kahden verkon välillä sekä verkon liikenteen ohjauksen (reititys). (Microsoft 2015b.)
Tietojärjestelmä	Järjestelmä jonkin tietojenkäsittelykokonaisuuden suorittamiseen. Koostuu tiedosta, tiedon käsittelysäännöistä, käsittelyn henkilö- ja laiteresursseista sekä tiedonsiirtolaitteista ja toimintaohjeista. (Sanastokeskus TSK:n termipankki 2015a.)
Tieto(liikenne)verkko	Tietokoneiden ja tiedonsiirtoyhteyksien muodostama palvelujen yhdistelmä. (Sanastokeskus TSK:n termipankki 2015b.)
Tietoturva-aukko	Heikkous, joka mahdollistaa vahingon toteutumisen, tai jota voidaan käyttää vahingon toteuttamisessa. Voidaan kutsua myös haavoittuvuudeksi. (Sanastokeskus TSK 2004.)
VLAN	Virtuaalilähiverkko (engl. Virtual LAN). Virtuaalinen lähiverkko mahdollistaa itsenäisten virtuaaliverkkojen luonnin fyysisen verkon sisään. (Apple Inc. 2015.)
VPN	Yksityinen virtuaaliverkko (engl. Virtual Private Network) mahdollistaa suojatun yhteyden muodostamisen tietokoneiden välille (Symantec 2008).
WAN	Laajaverkko (engl. Wide Area Network) kattaa laajoja maantieteellisiä alueita.

ISO/IEC 27000	Standardisarja, joka sisältää suosituksia esimerkiksi tietoturvan hallintaan ja kontrollointiin (Suomen standardisoimisliitto 2015).
BS 7799	Alun perin vuonna 1999 julkaistu tietoturvastandardi, joka on myöhemmin liitetty osaksi ISO-standardiperhettä (BS7799 Audit & Compliance 2002).
COBIT	Viitekehys IT-palvelujohtamiseen (engl. Control Objectives of Information and related Technology) (ITSMF Finland 2015a).
ITIL	Kokoelma käytäntöjä IT-palveluiden suunnitteluun, toimitukseen, hallintaan ja johtamiseen. (ITSMF FINLANS 2015b.)

1 JOHDANTO

Tietojärjestelmien ja tietoverkkojen kautta tapahtuva tiedon siirto ja käsittely on nykypäivänä yhä useamman organisaation toiminnan perusedellytys. Valtakunnallisten tietojärjestelmien ja tietoverkkojen toimivuus vaikuttaa luonnollisesti myös yksityishenkilöiden tiedon siirtoon ja käsittelyyn. Tietoturvallisella toiminnalla pyritään varmistamaan tärkeän tiedon suojaus sekä tiedonkäsittelyyn ja siirtoon liittyvien toimintojen sujuvuus.

Tietoturvallisuudelle uhkia aiheuttavat paitsi tietojärjestelmien ja tietoliikenneverkkojen tekniseen toteutukseen liittyvät seikat, myös ympäristö sekä tiedonkäsittelijä itse. Organisaatiossa kokonaisvaltaisen tietoturvan ylläpito vaatii organisaatiolta perehtyneisyyttä tietoturvan eri osa-alueisiin sekä niistä aiheutuvien uhkien minimointiin.

Tämän opinnäytetyön tavoitteena on selvittää mitä tietoturvalla tarkoitetaan, mitä asioita tietoturvaan liittyy ja minkälaiset asiat aiheuttavat tietoturvalle uhkia. Tietoturvan perusteiden läpikäynnin jälkeen perehdytään tarkemmin tietoturvallisiin toimiin organisaatiossa. Lopuksi valmistellaan julkishallinnon organisaation tietojenkäsittelijöille suunnattu peruskoulutusmateriaali toimeksiantajan, Turun yliopiston Brahea-keskuksen käyttöön. Koulutusmateriaalin avulla pyritään vähentämään kohdeorganisaation henkilöstön tietämättömyydestä ja osaamattomuudesta aiheutuvia tietoturvauhkia sekä vahvistamaan tietoturvallisia toimintatapoja osana jokapäiväisiä työskentelyrutiineja.

2 TUTKIMUSONGELMAT JA TUTKIMUSMENETELMÄT

Opinnäytetyön keskeisiä tutkimusongelmia ovat tietoturvan, sen osa-alueiden sekä siihen kohdistuvien uhkien kartoitus. Lisäksi työssä taustoitetaan tarkemmin tietoturvan ylläpitoon ja kehittämiseen liittyviä toimia organisaatiossa.

Opinnäytetyön empiirisessä osuudessa sovelletaan toimintatutkimuksen vaiheita. Toimintatutkimuksella tarkoitetaan jatkuvaa prosessia, jolla etsitään ratkaisuja käytännön ongelmiin vaikuttamiseksi teorian sekä toiminnan keinoin. Toimintatutkimukselle olennaista on tutkittavien osallistuminen tutkimuksen kulkuun. (Saaranen-Kauppinen & Puusniekka 2006.) Toimintatutkimus perustuu jatkuvaan sykliin, joka alkaa tarpeen havainnoinnista ja määrittelystä, ja kulkee kartoitusten ja toimintasuunnitelmien laadinnan kautta suunnitelmien toteutuksiin ja arviointiin. Toimintasuunnitelmia ja arviointeja jatketaan, kunnes ongelmaan on saatu ratkaisu. (Kajaanin ammattikorkeakoulu 2015.)

Opinnäytetyössä tarkoituksena on teoriapohjan ja muiden vastaavien koulutusmateriaalien sisältövertailun lisäksi tutustua koulutuksen mahdollisen kohdeorganisaation tietoturvan nykytilaan sekä käytännön toimintaan henkilöstöä haastattelemalla. Selvitettyä tilaa pyritään jatkossa muuttamaan perushenkilöstölle tarjottavan koulutusmateriaalin keinoin. Varsinaisen koulutustilaisuuden seuranta ja arviointi joudutaan rajaamaan työn ulkopuolelle koulutustilaisuuden toteutuessa vasta opinnäytetyön valmistumisen jälkeen.

3 TIETOTURVAN PERUSTEET

3.1 Määritelmä

Tietoturvalla tarkoitetaan tiedon ja tietojärjestelmien suojausta valtuuttamattomalta pääsyltä, käytöltä, muutoksilta sekä häiriöiltä ja tiedon häviämiseltä. Tietoturvan päätavoitteina pidetään perinteisesti kolmea kriteeriä; tiedon luottamuksellisuutta, eheyttä sekä saatavuutta (confidentiality, integrity, availability). (Legal Information Institute 2015.) Luottamuksellisuuden, eheyden ja saatavuuden tavoitteiden varmistamisella taataan, että tieto on vain valtuutettujen saatavilla, eikä muutu tai tuhoudu esimerkiksi toiminnan, haittaohjelmien, laitteistoon tai ohjelmistoihin liittyvien vikojen tai muiden häiriötilanteiden seurauksena. Lisäksi tiedon on oltava luotettavaa, oikeaa ja ajantasaista, sekä tarvittaessa vaivattomasti saatavilla. (Pietikäinen 2013.)

Saatavuuden, eheyden ja luottamuksellisuuden lisäksi tietoturvan tavoitteita voidaan täydentää kiistämättömyyden (non-repudiation), pääsynvalvonnan (access control) ja todentamisen (authentication) käsitteillä. Kiistämättömyydellä tarkoitetaan tietojärjestelmän kykyä tunnistaa ja tallettaa järjestelmän käyttäjän tiedot. Pääsynvalvonnalla tarkoitetaan menetelmiä, joilla tietojenkäsittelyympäristön käyttöä rajoitetaan. Todentamisella (tai autenttisuudella) tarkoitetaan esimerkiksi käyttäjän luotettavaa tunnistamista. (Hakala ym. 2006, 5-6.)

Yksinkertaistettuna voidaan ajatella, että tietoturva koostuu tiedosta, sekä tietoa käsittelevien tekijöiden turvallisuudesta huolehtimisesta. Tietoturvan tavoitteiden avulla määritellään pohja niille keinoille, joilla tiedon turvaaminen on mahdollista saavuttaa.

Organisaatiossa tietoturva käsittää teknisiä ja hallinnollisia keinoja, sekä niiden suunnittelua, toteutusta ja seurantaa organisaatioissa laadittujen tavoitteiden mukaisesti (Laaksonen ym. 2006, 17).

3.2 Osa-alueet

Tietoturvallisuuden kokonaisuus voidaan jakaa osa-alueisiin eri tavoin. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI jakaa tietoturvan hallinnolliseen ja fyysiseen turvallisuuteen sekä henkilö-, tietoaineisto-, ohjelmisto-, laitteisto-, käyttö- ja tietoliikenneturvallisuuteen. (Kuvio 1.) (Valtiovarainministeriö 2015a.) Seuraavissa kappaleissa käsitellään näiden osa-alueiden tarkempia sisältöjä.

Kuvio 1. Tietoturvallisuuden osa-alueet Valtionhallinnon tietoturvallisuuden johtoryhmän mukaan.

Hallinnollisella tietoturvalla tarkoitetaan tietoturvan kehittämiseen ja johtamiseen liittyviä toimia, joita ovat esimerkiksi yhteydenpito muihin turvallisuudesta vastaaviin tahoihin sekä lainsäädännön vaikutusten arviointi organisaatioon ja sen toimintaan (Hakala ym. 2006, 10). Hallinnollinen tietoturva organisaatiossa käsittää muun muassa tiedottamista, seurantaa, ohjausta ja koulutusta (Tirronen 2003).

Fyysiseen turvallisuuteen kuuluvat organisaation tuotanto- sekä toimitilojen suojaamiseen liittyvät asiat, joilla estetään esimerkiksi tärkeän informaation tuhou-

tuminen, vahingoittuminen ja vääriin käsiin joutuminen (Vedenoja 2007). Fyysisen turvallisuuden suunnittelussa huomioitavia asioita ovat esimerkiksi kulunvalvonta, murtosuojaukset, palvelintilojen lukitseminen, paloturvallisuus ja hälytysjärjestelmät. Lisäksi on huomioitava muun muassa tärinän, energia- ja jännitevaihteluiden, säteilyn ja pölyn aiheuttamat vahingot. (Tirronen 2003.)

Henkilöturvallisuudella tarkoitetaan toimia henkilöstöön liittyviin uhkiin varautumiseksi. Näitä ovat esimerkiksi organisaation tietojärjestelmän käyttäjien toimintakyvyn varmistaminen sekä tietojärjestelmiä koskevien vastuiden ja oikeuksien määrittely. (Hakala ym. 2006, 11.) Merkittävänä osana organisaation henkilöturvallisuuden ylläpitoa voidaan mainita henkilöstön koulutus, jolla minimoidaan huolimattomuudesta, tietämättömyydestä tai osaamattomuudesta aiheutuvia riskejä. (Tirronen 2003.)

Tietoaineistoturvallisuus on asiakirjojen, tiedostojen ja muiden tietoaineistojen luokitteluun, tietoturvallisuuden hallintaan, käsittelyyn, säilytykseen ja hävittämiseen liittyviä toimia (Valtiovarainministeriö 2009). Tietoaineistoturvallisuuden päätavoite on säilyttää tietojen ja tietoaineistojen luottamuksellisuus, sekä estää tietojen tuhoutuminen tai valtuuttamaton muuttuminen (Tirronen 2003).

Ohjelmisto- ja laitteistoturvallisuudella tarkoitetaan käyttöjärjestelmiin ja muihin organisaation ohjelmistoihin liittyviä toimia, kuten asennusta ja ylläpitoa. Ohjelmisto- ja laitteistoturvallisuuteen luetaan kuuluvaksi myös tietojärjestelmissä käytettävien laitteiden omistajien sekä ohjelmistojen hallinta ja valvonta sekä esimerkiksi tietojen palautuksista huolehtiminen poikkeamatilanteissa. (Laakso 2015a, Valtiovarainministeriö 2015b.)

Tietoliikenneturvallisuus on tiedonsiirtoratkaisujen ja viestintäjärjestelmien turvallisuudesta huolehtimista. (Hakala ym. 2006, 12.) Tietoverkkojen oikeaoppinen rakentaminen sekä suunnittelu ovat ylläpidon ja seurannan lisäksi oleellinen osa tietoliikenneturvallisuuden toteuttamista.

Käyttöturvallisuudella tarkoitetaan jokapäiväisten tietojenkäsittelytoimintojen turvaamista. Käyttöturvallisuus voi sisältää esimerkiksi tietojenkäsittelyn valvontaa ja salasanojen hallintaa. (Miettinen 2002, 158-159.)

Tämä edellisissä kappaleissa käsitelty ryhmittely ei ole ainoa tapa määrittää tietoturvan osa-alueita; jaottelutavat poikkeavat lähteistä riippuen hieman toisistaan. Esimerkiksi kansallinen tietoturva-auditointikriteeristö KATAKRI jakaa tietoturvan vain kolmeen osaan; turvallisuusjohtamiseen sekä fyysiseen ja tekniseen turvallisuuteen (Puolustusministeriö 2015). Tarkempi tutustuminen osioihin kuitenkin osoittaa kriteeristön tuovan esille pitkälti samankaltaisia jo käsiteltyjä asiakokonaisuuksia.

3.3 Kansallinen lainsäädäntö ja asetukset

Suomessa tietoturvallisuuteen liittyviä määräyksiä löytyy useista eri laeista. Organisaation on toimintansa kannalta tärkeää hahmottaa ne säädökset, velvoitteet ja oikeudet, jotka liittyvät organisaation tietoturvan suunnitteluun, ylläpitoon ja kehitykseen (Laaksonen ym. 2006, 18).

Tietoturvaa sivuavia lakeja ovat laki viranomaisten toiminnan julkisuudesta, laki kansainvälisistä tietoturvallisuusvelvoitteista sekä laki sähköisen viestinnän tietosuojasta. Lisäksi tietoturvalle rajoja luovat laki yksityisyyden suojasta työelämässä, laki tietoyhteiskunnan palvelujen tarjoamisesta, laki sähköisestä asioinnista viranomaistoiminnassa, laki sähköisestä tunnistamisesta ja allekirjoituksesta sekä viestintämarkkinalaki, henkilötietolaki, perustuslaki, ja rikoslaki. (Laaksonen ym. 2006, 23.) Viestintämarkkinalaki sekä laki tietoyhteiskunnan palvelujen tarjoamisesta on kumottu ja korvattu tietoyhteiskuntakaarella vuonna 2014 (917/2014).

Mainittuja lakeja tarkennetaan asetuksilla viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999) sekä tietoturvallisuudesta valtionhallinnossa (681/2010). Euroopan Unionin valmisteleman uuden tietosuoja-asetuksen tavoitteita ovat muun muassa ”yksilön oikeuksien vahvistaminen”, ”tietosuojan globaalin ulottuvuuden huomioiminen” sekä ”tietosuojasääntöjen täytäntöönpanon valvonnan tehostaminen”. Arvioiden mukaan asetuksen valmistelu saadaan päätökseen vuoden 2015 loppuun mennessä ja asetusta aletaan soveltaa vuoden 2018 alusta lähtien. (Opi tietosuojaa 2015.)

4 TIETOTURVAUHKIA

4.1 Inhimilliset tekijät

Yhtenä suurimmista tietoturvaa uhkaavista tekijöistä voidaan pitää tietokoneen käyttäjää itseään. Suuri osa tietoturvaa uhkaavista inhimillisistä tekijöistä on tahattomia; syitä tietoturvan vaarantumiselle ovat esimerkiksi kiire, osaamattomuus ja huolimattomuus (Järvinen 2012, 19, Pietikäinen 2013).

Tietoturvauhkia aiheuttavia käyttäjästä itsestään johtuvia toimia voivat olla esimerkiksi harkitsematon verkkokäyttäytyminen ja henkilökohtaisten tietojen jako sosiaalisen median kanavissa. Myös lataukset epäluotettavilta verkkopalveluilta, palomuurien ja virustorjuntaohjelmien käytön laiminlyönti sekä tietokoneen luvaton tai ohjeistusten vastainen käyttö aiheuttavat pienellä vaivalla ehkäistävissä olevia tarpeettomia uhkia tietoturvallisuuden ylläpidolle.

Ympäristöstä aiheutuvia inhimillisistä tekijöistä johtuvia tietoturvauhkia aiheuttavat muun muassa identiteettivarkaudet (Järvinen 2012, 256) sekä verkkorikolliset, haktivistit ja krakkerit, jotka murtautuvat tietojärjestelmään tai verkkosivulle luvattomasti tarkoituksenaan tehdä tahallisesti haittaa järjestelmän tai sivun haltijalle (Haakana 2002).

4.2 Hallinnolliset tekijät

Organisaation tietoturvauhkien torjunnassa vastuu on pitkälti ylimmällä johdolla. Johdolta edellytetään tietoturvaan liittyvien tavoitteiden, liiketoimintaprosessien, tietoisuuden ja koulutuksen, sekä toiminnan kehittämiseen ja tarkasteluun liittyviin toimiin sitoutumista ja toimien tukemista. (Hakala ym. 2006, 114.) Sitoutumisella, koulutuksella ja toiminnan kehittämisellä pyritään minimoimaan organisaation henkilöstöstä johtuvat inhimilliset uhat.

Hallinnolliseen tietoturvan ylläpitoon voidaan lukea myös esimerkiksi työntekijöiden taustoihin tai työtehtävien ulkoistukseen liittyvät uhat. Uusien työntekijöiden palkkauksessa taustatarkastuksilla voidaan selvittää henkilön sopivuutta työhön, ja näin minimoida tulevaisuuden uhkia (Laaksonen ym. 2006, 139). Vastaavasti vanhojen työntekijöiden lähtiessä on varmistuttava siitä, ettei tärkeää tietoa päädy muualle työntekijän mukana. Ulkoistetun työn tietoturvasta tulee varmistua samalla tavalla kuin organisaation sisäisestä toiminnasta (Laaksonen ym. 2006, 239).

4.3 Ohjelmisto- ja laitteistotekijät

Käyttöjärjestelmien ja sovellusten säännöllinen päivittäminen on tietoturvan edellytys. Päivityksiä käytetään ohjelmointivirheiden, ilmestyneiden yhteensopivuusongelmien sekä tietoturva-aukkojen korjaamiseen. (Järvinen 2006, 15-17.)

Haittaohjelmaksi voidaan lukea kaikki ne ohjelmat, jotka asentuvat koneelle luvatta ja tuovat käyttäjälle haittaa. Haittaohjelmien avulla voidaan toteuttaa esimerkiksi vakoilua ja näppäimistökaappausta, palvelunestohyökkäyksiä, huijausviestien tai roskapostin lähetystä, selaustietojen ja sähköpostiosoitteiden keräämistä sekä uusien haittaohjelmien levittämistä. Haittaohjelmat voivat päästä koneelle esimerkiksi sähköpostin liitetiedostona tai käyttöjärjestelmän tai selaimen tietoturva-aukon kautta. (Järvinen 2006, 77-81.)

Kannettavat tietokoneet ja muut liikkuvat päätelaitteet aiheuttavat haasteita tietoturvalle. Tiedon käsittelyyn kannettavalla laitteella tulee kiinnittää erityistä huomiota tietojen vääriin käsiin päätymisen estämiseksi. Mikäli laite on pidemmän aikaa poissa organisaation verkosta, on myös mahdollista, että liitettäessä organisaation verkkoon ulkoverkosta tullut virus pääsee leviämään organisaation tietojärjestelmään. (Hakala ym. 2006, 137.)

Tietoturvauhkia voi joissain tapauksissa luoda myös niin kutsuttu metadata eli ohjelmien muistiin jäävä piilotieto. Piilotietoa ovat usein esimerkiksi tekijöiden nimet, luokittelutiedot, avainsanat ja muokkausajat. Piilotietoa on pidetty esi-

merkiksi Microsoftin toimisto-ohjelmien ongelmana, mutta ilmiö liittyy myös muihin sovelluksiin. (Järvinen 2006, 303-304.)

4.4 Ympäristötekijät

Tiedon kalastelu (phishing) tarkoittaa taloudelliseen hyötyyn tähtäävää tietojen urkintaa. Kalastelu perustuu käyttäjän huijaamiseen teknisten suojausten kierron sijasta (social engineering -hyökkäys). Tietojen kalastelua voidaan tehdä paitsi sähköpostitse tai aidontuntuisilla väärennetyillä verkkosivuilla myös esimerkiksi puhelimitse tai kahdenkeskisissä tapaamisissa. (Järvinen 2006, 273-274.)

Sähköpostihuijauksesta hyvänä esimerkkinä voidaan käyttää ns. Nigerialaiskirjettä. Nigerialaiskirjeellä tarkoitetaan huijausta, jossa lähettäjällä on tyypillisesti hallussaan miljoonia dollareita ja vastaanottajalle luvataan osa summasta tiettyjä toimenpiteitä vastaan. (Järvinen 2012, 162.) Muita yleisiä sähköpostihuijauksia ovat esimerkiksi ilmoitukset arpajaisvoitoista, rahapyynnöt sekä muut valheelliset mainokset ja verkkopalvelut. (Järvinen 2012, 164-173.)

Fyysisiä uhkia tietoturvalle aiheuttavat sähköisten dokumenttien säilytykseen sekä laitteistoon liittyvät asiat. Näitä ovat esimerkiksi kolhut, mekaaninen rasitus, valo, kosteus, kuumuus, sähköhäiriöt varmuuskopiointien puute, laite- ja ohjelmistoviat sekä esimerkiksi laitevarkaudet ja ilkivalta. (Tirronen 2003.) Fyysisiin uhkiin voidaan laskea myös tulipalot ja muut katastrofit, jotka toteutuessaan voivat tuhota heikosti varmuuskopioidun informaation (Laakso 2015b).

5 TIETOTURVALLINEN TOIMINTA ORGANISAATIOSSA

5.1 Johtaminen ja hallinnointi

Organisaation tietoturvallisen toiminnan perustana voidaan pitää organisaation tarpeita vastaavaksi mitoitettua johtamista. Yksinkertaisimmillaan tietoturvallisuuden johtaminen voi tarkoittaa lain vähimmäisvaatimusten täyttymisen seurantaa (Laaksonen ym. 2006, 115). Lisäksi johtaminen voi sisältää tietoturvapolitiikan ja toimintaohjeiden laatimista, tavoitteiden asettamista sekä valvontaa ja toiminnan kehittämistä organisaation toiminnan laajuudesta riippuen.

Tietoturvapolitiikka on dokumentti, jossa määritellään organisaation tietoturvallisuuden kohteet ja vaatimukset, sekä menetelmät tiedon ja teknologian suojaamiseksi. Tietoturvan toteutumisen kannalta olennaista on henkilöstön hyväksyntä sekä sitoutumus noudattaa määriteltyä politiikkaa. Hyödyksi tietoturvan toteuttamisessa on myös henkilöstön ymmärrys toimintansa vaikutuksista tietoturvan tasoon. (Fraser 1997.)

Tietoturvaohjelmalla tarkoitetaan tietoturvaohjeiden, toimintamallien sekä teknisten suojauskeinojen kehittämistä tietoturvan parantamiseksi. Tavoitteena on turvata organisaation tärkeä tieto. (Laaksonen ym. 2006, 120.) Tietoturvaohjelma perustuu organisaation nykytilan kartoituksiin ja toiminnan arviointiin. Tietoturvaohjelma sisällytetään osaksi organisaation johtamismenetelmää. (Laaksonen ym. 2006, 120-121.)

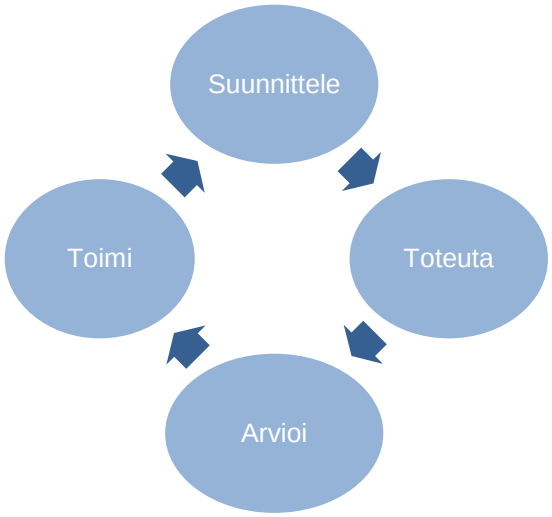
Tietoturvan hallinnoinnin suunnittelun tueksi on olemassa useita erilaisia standardeja, viitekehyksiä ja toimintamalleja. Keskeisiä tietoturvastandardeja ovat kansainvälisesti käytetyt ISO- standardiperhe sekä BS 7799. Tunnettuja toimintamalleja tarjoavat esimerkiksi COBIT ja ITIL. (Laaksonen ym. 2006, 83-100.)

Hyvän tietoturvan toteutumisen kannalta on tärkeää, että tietoturvaan liittyvät asiat huomioidaan kaikissa organisaatioin yksiköissä. Tietoturvallinen ajattelutapa on saatettava osaksi jokaisen työntekijän päivittäisiä toimia. (Laaksonen

ym. 2006, 116.) Tietoturvan ja tietoturvallisten toimintatapojen sisällyttämisellä päivittäisiin toimiin helpotetaan paitsi henkilöstön, myös hallinnon toimintaa. Kun ohjeistusten mukaiset työskentelytavat ovat henkilöstölle ennalta selkeitä, tarve esimerkiksi toistuvalle perusasioita käsittelevälle koulutukselle vähenee.

5.2 Kehittäminen ja riskienhallinta

Toiminnan kehittämisen tueksi on olemassa lukuisia erilaisia toimintamalleja. Näitä malleja voidaan soveltaa myös tietoturvan johtamis- ja hallintajärjestelmän kehittämisessä. Yksi tunnetuimmista toiminnan kehittämismalleista on PDCA -malli (Kuvio 2.) Mallin nimi muodostuu englannin kielen sanoista plan, do, check ja act, jotka suomeksi tarkoittavat suunnittelua, toteutusta, arviointia ja toimintaa. Mallin suunnitteluvaiheessa tunnistetaan ja määritellään suojattavat kohteet ja uhat sekä määritellään suojauksen tavoitteet. Toteutusvaihe sisältää varsinaisen järjestelmän tekoprosessin. Arviointivaiheessa tarkastellaan järjestelmän toimivuutta ja toimintavaiheessa arvioinnissa ilmenneet korjausehdotukset toteutetaan. (MindTools 2015.)



Kuvio 2. PDCA -malli.

Tietoturvariskienhallinnan keinot voidaan jakaa kolmeen osaan. Näitä keinoja ovat tekniset toimenpiteet (esim. laite- ja työtilaratkaisut) organisaation toimin-

taan vaikuttavat toimenpiteet (esim. toimintaohjeistusten laatiminen, arviointi ja valvonta) sekä yksilöiden toimintamahdollisuuksiin vaikuttavat toimenpiteet (esim. työvälineet, koulutus, perehdytys). (Karsisto 2007.) Riskienhallinnan tulee perustua organisaation toiminnan jatkuvaan arviointiin ja valvontaan.

Organisaatiota uhkaavien riskien hallinnan mahdollistamiseksi muodostetaan kokonaisvaltainen kuva toimintaympäristöstä riskikartoituksen avulla. Riskikartoituksessa huomioidaan paitsi nykytilanteen, myös tulevaisuuden uhkia. Kartoituksen jälkeen alkaa arviointivaihe, jossa pohditaan riskien vaikutuksia sekä niiden toteutumisen todennäköisyyttä. (Hakala ym. 2006, 80-81.)

Riskienhallinnan tueksi voidaan laatia riskikartoitusten perusteella luotuja jatkuvuus- ja toipumissuunnitelmia. Jatkuvuussuunnitelman avulla turvataan liiketoiminnan jatkuminen häiriötilanteissa ja niiden jälkeen. Toipumissuunnitelman avulla pyritään mahdollistamaan liiketoimintaprosessien tehokas toipuminen toteutuneista häiriötekijöistä. Toipumissuunnitelmassa voidaan määritellä esimerkiksi varajärjestelmävaatimuksia sekä vastuita ja toimintaohjeita katastrofitilanteiden varalle. (Laaksonen ym. 2006, 227.)

5.3 Tietojenkäsittely-ympäristön suojaus

Tietojenkäsittely-ympäristön suojaukseen kuuluu olennaisesti tietojärjestelmien käyttöoikeuksien hallinta, sekä sen edellyttämä käyttäjien henkilökohtainen tunnistus. Käyttäjätunnukset ja salasanat ovat laajasti käytetty keino käyttäjien tunnistamiseen ja todentamiseen. Käyttäjätunnusten ja salasanojen lisäksi tunnistusta voidaan tehdä esimerkiksi älykorttien tai biometrisen tunnistuksen avulla. Biometrinen tunnistus voi perustua esimerkiksi käyttäjän sormenjälkiin. (Hakala ym. 2006, 124.)

Tietojärjestelmien käyttöoikeudet voidaan jakaa kahteen ryhmään, joita ovat järjestelmän käyttöön sekä järjestelmän ylläpitoon tarkoitetut tunnukset. Järjestelmän käyttöön tehtyjen tunnusten hallinnointiin voidaan lukea käyttöoikeuksien ja työtehtävien vastaavuuden varmistus, turhien käyttäjätunnusten tuhoaminen sekä salasanojen vahvuuden seuranta. Ylläpitoa varten tehtyjen tunnusten hal-

linnassa ja valvonnassa organisaation on oltava lisäksi erityisen tarkkana laajojen käyttöoikeuksien vuoksi; muun muassa henkilötietolaki asettaa rajoituksia esimerkiksi palkkatietojen tai muiden arkaluontoisten henkilötietojen katselulle ja käytölle. (Laaksonen ym. 2006, 176.)

Organisaation työntekijät tuottavat tärkeää tietoa työasemilleen. Näistä tiedoista huolehtiminen on tärkeä osa tietojenkäsittely-ympäristön suojaamista. Työntekijät tulee ohjeistaa tallentamaan tiettyyn paikkaan esimerkiksi palvelimelle, jolloin tiedot voidaan varmistaa organisaation tarpeiden mukaisesti. (Hakala ym. 2006, 135.) Mikäli työasemalla käsitellään salaista tietoa, käsittely edellyttää salausmenetelmien käyttöä. Salausmenetelmien avulla tieto muutetaan ei-ymmärrettävään muotoon, joka saadaan ymmärrettäväksi vain oikean tiedon, eli salausavaimen avulla. Salausta voidaan tehdä esimerkiksi ulkoisille muisteille, kiintolevyille tai vain tietyille verkkopalveluille tai sähköpostille. (Aho 2010a.)

ISO/IEC 17799 -standardi jakaa tietojenkäsittelytiloihin liittyvät tekniset kontrollit kuuteen osaan. Kontrolleista ensimmäinen edellyttää tietoja sisältävien laitteiden ja tilojen suojausta rakennusmateriaalien ja lukitusmenetelmien avulla. Lisäksi kulunvalvonnasta sekä palo- ja rikosilmoituksen teosta on huolehdittava. Toisen kontrollin mukaan tulee varmistua siitä, että vain auktorisoiduilla henkilöillä on pääsy turvattuihin tiloihin. Kolmannessa ja neljännessä kontrollissa edellytetään tilojen suojauksen suunnittelua ja toteutusta. Viides osa korostaa fyysinen suojauksen toteutusta sekä turvatuissa tiloissa työskentelyn periaatteiden noudattamista. Viimeinen kontrolli edellyttää yleisö- ja asiakastilojen sekä lastauslaiturien valvontaa ja eristystä muista tietojenkäsittelytiloista. (Hakala ym. 2006, 304, ISO/IEC 17799.)

5.4 Tietoliikenneverkon turvallisuus

Myös tietoliikenneyhteydet on rakennettava niin, että niiden kautta turvallinen työskentely on mahdollista. Hakala, Vainio ja Vuorinen (2006, 182) mainitsevat tietoliikenneverkon turvallisuudesta huolehtimisessa käytetyiksi kontrolleiksi palomuurit, virtuaaliset lähiverkot, verkon fyysisen suojauksen, reitityksen, verkon

käytön seurannan ja analysoinnin, kaistanleveyden hallinnan sekä etätoimipisteiden ja kotityön vaatimien yhteyksien rakentamisen. Mainittujen kontrollien avulla pyritään parantamaan tietoliikenteeseen liittyviä tietoturvallisuuden kriteerejä, kuten luottamuksellisuutta ja saatavuutta.

Palomuurin avulla verkon palveluiden ja verkon käyttöä voidaan rajoittaa organisaation tarpeiden mukaisesti. Myös palvelunestohyökkäyksiin voidaan varautua palomuuriasetusten huolellisella suunnittelulla. Lähiverkon (LAN) sisäistä liikennettä ja järjestelmiin pääsyä voidaan rajoittaa kytkentäisillä aktiivilaitteilla, joihin määritellään virtuaaliset lähiverkot (VLAN). (Hakala ym. 2006, 182.)

Verkon fyysisellä suojauksella tarkoitetaan esimerkiksi kaapeleiden ja liittimien suojausta asiattomalta käytöltä. Reitityksessä suositaan kuormituksen tasausta rinnakkaisten reitittimien käytöllä mahdollisuuksien mukaan. Myös virheellisten reittitietojen lähettäminen voidaan estää. (Hakala ym. 2006, 182.)

Verkon kuormitustilanteen, vikojen ja mahdollisten hyökkäysten havainnoimiseksi verkon liikennettä tulee seurata ja analysoida säännöllisesti. Analysoinnin perusteella laitteille laaditaan asetukset, joissa riittävä tiedonsiirtokapasiteetti taataan kaikissa tilanteissa. Ulkoisille ja sisäisille laajaverkkoyhteyksille (WAN) voidaan luoda varayhteydet hyökkäysten tai operaattorivikojen varalta. Etätoimipisteiden ja kotityön mahdollistamiseksi luodaan yhteyksiä, joiden toiminta perustuu usein VPN -tunneleihin. (Hakala ym, 2006, 182-183.)

5.5 Laitteistojen ja ohjelmistojen kunnossapito

Laitteistojen suojaus alkaa niiden sijoituksesta. Laitteistot on sijoitettava ja suojattava niin, että ne ovat suojassa ympäristöstä aiheutuvilta uhilta sekä luvattomalta käytöltä. Laitteiston toiminnan takaamiseksi myös sähkön ja vedensaanti on turvattava. Kaapelointi ja muut tiedonsiirtoon liittyvät järjestelmät on suojattava salakuuntelulta ja vahingoittamiselta. (Hakala ym. 2006, 308, ISO/IEC 17799.)

Laitteiston säännöllistä huoltoa ja ylläpitoa voidaan pitää tärkeänä laitteistoturvallisuuden osana. Laitteiston ylläpitoon kuuluu muun muassa käyttöjärjestelmien ja ohjelmistojen tietoturva- ja korjauspäivityksistä huolehtiminen. Ennen päivityksen käyttöönottoa päivitykset on mahdollisten virhetilanteiden vuoksi testattava huolellisesti (Hakala ym. 2006, 135).

Hyvin suunnitellut ja organisaation tarpeeseen mitoitetut, toimivat tietojärjestelmät vähentävät tietoturvaan liittyvien ongelmien syntyä (Hakala ym. 2006, 315). Järjestelmien, ohjelmistojen ja sovellusten toimintaan ja niiden hyödynnettävyyteen vaikuttaa merkittävästi myös laitteen käyttäjä. Käyttäjien koulutuksella voidaankin ehkäistä osaa käyttötilanteissa ilmenevistä ongelmista.

Nykypäivänä organisaatiossa on tärkeää huolehtia myös muualla, kuin toimistolla tapahtuvan tietojenkäsittelyn riskien huomioimisesta, sekä näiden riskien edellyttämien turvatoimien käyttöönotosta. Laitteistoja ja ohjelmistoja hävitettäessä luottamuksellinen data on poistettava. Laitteiden, ohjelmistojen ja tiedon vientiä organisaation ulkopuolelle on myös kontrolloitava. (Hakala ym. 2006, 308, ISO/IEC 17799.)

Virustorjunnasta tulee huolehtia paitsi työasemissa, myös esimerkiksi etä- ja kotikäyttöön tarkoitetuissa laitteissa, selainliikenteessä sekä palvelimissa ja muissa tuotannollisissa järjestelmissä. (Laaksonen ym. 2006, 205.)

5.6 Tietoaineistojen luokittaminen ja hallinnointi

Tietoaineistojen tietoturvallisuuden takaamiseksi tiedon hallintaa helpotetaan luokittelemalla se eri luokkiin tiedolle asetettujen vaatimusten perusteella (Aho 2010b). Suomessa esimerkiksi julkisuuslaki (621/1999) asettaa vaatimuksia tiedon hallinnalle ja käsittelylle. Lisäksi henkilötietolaki (523/1999) ohjaa henkilötietojen käsittelyä.

Tiettyjen salassa pidettävien tietoaineistojen käsittelyä ohjataan muun muassa Tietoturvallisuusasetuksen 9 & 12 momenteissa määriteltyjen suojaustasojen ja turvallisuusluokittelunimikkeiden perusteella. Suojaustasot voidaan jakaa nel-

jään luokkaan, joista suojaustaso I on korkein ja IV matalin. (Taulukko 1.) (Aho 2010b.)

Taulukko 1. Suojaustasot ja turvallisuusluokittelunimikkeiden vastaavuus. (Aho 2010b.)

SUOJAUSTASO	TURVALLISUUSLUOKITTELUN NIMIKE	LYHENNE
Suojaustaso I	ERITTÄIN SALAINEN	ERSAL (E)
Suojaustaso II	SALAINEN	SAL (S)
Suojaustaso III	LUOTTAMUKSELLINEN	LUOT (L)
Suojaustaso IV	KÄYTTÖ RAJOITETTU	RAJ (R)

Tietoaineisto sijoitetaan tiedon paljastumisen seurauksen merkitysten mukaan tasoon, jossa tulee huomioida asiakirjan tai tiedon tuleva käsittelytarve. Kunkin asiakirjan luokitustarve arvioidaan erikseen. Eri suojaustasoihin liittyvä tieto tulisi sijoittaa eri asiakirjoihin asiakirjan käytettävyyden mahdollistamiseksi. (Aho 2010b.)

Asiakirja on pidettävä salassa, mikäli se on laissa määrätty salattavaksi, tai muuten sisältää tietoa, josta laissa on määrätty vaitiolovelvollisuus. Salassapitomerkintä on tehtävä asiakirjaan, joka annetaan asianosaiselle, toiselle viranomaiselle, tai muulle tietoja käsittelevälle taholle sekä on salassa pidettävä toisen tai yleisen edun vuoksi. (621/1999, 25 §) Merkinnästä tulee selvitä mitkä osat asiakirjasta ovat salattuja ja mihin salassapito perustuu. Tiedon salassa pitäminen loppuu kun asiakirjan antamisesta ei aiheudu salassapitoa edellyttäviä vaikutuksia tai kun julkisuuslaissa määritelty salassapitoaika on mennyt umpeen. (Aho 2010b.)

5.7 Henkilöstön koulutus

Oppimiseen ja tiedon omaksumiseen vaikuttavina tekijöinä voidaan pitää esimerkiksi oppijan aikaisempia tietoja, uusien asioiden esittämistapaa, sekä oppimiseen liittyvää vuorovaikutusta ja asioiden käsittelyä. (Jyväskylän yliopisto 2015.) Oppimiseen tai opetustilanteen kulkuun ei kuitenkaan ole olemassa yksi-

selitteistä ratkaisua, jolla tehokas oppiminen voitaisiin kaikkien koulutukseen osallistuvien kohdalla taata. Eri ihmiset myös omaksuvat tietoa eri tavoin.

Henkilöstön tietoturvakäyttäytymiseen vaikuttavat tekijät voidaan jakaa karkeasti organisaatiotekijöihin sekä henkilöstä itsestään riippuviin tekijöihin. Organisaatiosta riippuvia tekijöitä ovat tiedon lähteet (arvot, tietoturvapolitiikka, toimintaohjeet, koulutus), sekä kollegojen esimerkki. Työntekijästä riippuvia tietoturvakäyttäytymiseen vaikuttavia tekijöitä ovat henkilökohtaiset arvot ja asenteet, työkokemus, työntekijän suhtautuminen työnantajaan sekä ohjeiden noudattamisen edellyttämä työmäärä. (Laaksonen ym. 2006, 249.)

Tietoturvakoulutuksen sisällön tulisi olla linjassa organisaation tietoturvapolitiikkaan ja sen pohjalta tehtyihin toimintaohjeisiin. Koulutuksen tarkoituksena on saada henkilöstö toimimaan organisaation haluamalla tavalla tärkeän tiedon suojaamiseksi. Tietoturvakoulutuksen tavoitteet saavutetaan, kun työntekijät ymmärtävät omaan työhönsä liittyvät riskit, sekä ovat tietoisia niiden minimoinnin keinoista. (Laaksonen ym. 2006, 254.)

Oppimista voidaan koulutustilanteessa tehostaa muun muassa esimerkkien sekä säännöllisyyden ja muiden kohderyhmälle suunnattujen opetusmenetelmien avulla. Myös koulutuksen ympäristö vaikuttaa oppimiseen. Koulutustilanteessa henkilöstöä on pyrittävä motivoimaan, jotta säännöllinen tietoturvakoulutus pysyy miellyttävänä kokemuksena henkilöstölle. (Laaksonen ym. 2006, 254-256.)

6 KOULUTUSMATERIAALIN TOTEUTUS

6.1 Toimeksiantajaorganisaatio ja työn taustaa

Brahea-keskus on Turun yliopiston alaisena toimiva erillislaitos, jonka toiminnan tavoitteita ovat muun muassa kehittämis- ja koulutuspalveluiden tuottaminen, sekä yliopiston asiantuntemuksen hyödyntämisen edistäminen yhteyksien luomisen muodossa. Keskuksen toimintaan liittyvät oleellisesti erilaiset kansalliset ja kansainväliset projektit. (Turun Yliopisto 2015)

Tietoturvaa käsittelevän koulutusmateriaalin tarve oli tullut ilmi Brahea-keskuksen aiemman asianhallintaan liittyvän koulutustilaisuuden yhteydessä. Tällöin koulutusmateriaalin tarpeesta mainitsivat asianhallinnan koulutustilaisuuden osallistujat. Tietoturvaan ja tietoturvalliseen toimintaan liittyvän koulutuskokonaisuuden suunnittelu sai alkunsa huhtikuussa 2015, jolloin sovittiin materiaalin valmistelusta syksyn 2015 aikana. Valmiin materiaalin oli tarkoitus toimia pohjana mahdollisesti keväällä 2016 toteutuvassa koulutustilaisuudessa.

6.2 Tavoitteet ja suunnittelu

Tavoitteena oli suunnitella ja toteuttaa yleisesti hyväksyttyihin standardeihin pohjautuva tietoturvaa käsittelevä materiaali ensisijaisesti julkishallinnon organisaation tietoa käsitteleville toimistotyöntekijöille. Koulutusmateriaalin sisällön tavoitteiksi asetettiin selkeys ja käytännöllisyys. Varsinaisen koulutuskokonaisuuden laajemmiksi tavoitteiksi kirjattiin tietoturvatietoisuuden lisääminen sekä henkilöstön toimista johtuvien tietoturvallisuusriskien ennaltaehkäisyn merkityksen korostaminen kohdeorganisaatiossa.

Koulutusmateriaalin suunnitteluvaiheessa tutustuttiin vastaavan kaltaista tietoturvamateriaalia tarjoavien organisaatioiden koulutusten sisältöihin sekä niiden hintaesimerkkeihin. Tiedoista koottiin keskuksen käyttöön tausta-aineistoksi suuntaa-antava taulukko, jota voitaisiin hyödyntää tulevaisuudessa esimerkiksi

koulutuksen markkinoinnissa. Suunnittelun toinen oleellinen osa käsitti tarkempaa tutustumista sekä kansallisiin, että kansainvälisiin tietoturvaan liittyviin standardeihin ja ohjeistuksiin. Kansainvälisistä standardeista tutustuttiin erityisesti ISO 27000- standardisarjaan sekä kansalliseen KATAKRI- tietoturvallisuuden auditointikriteeristöön. Lisäksi käytiin läpi valtionhallinnon tietoturvaan liittyvien VAHTI-ohjeistusten sisällöt.

Kohderyhmän tarpeiden huomioimiseksi sekä koulutusmateriaalin tavoitteiden toteuttamiseksi materiaalin pohjana päätettiin hyödyntää pääosin kansallisia Valtionhallinnon ohjeistuksia. Näitä ohjeistuksia olivat VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje sekä VAHTI 4/2013 Henkilöstön tietoturvaohje. Lisäksi apuna käytettiin VAHTI 2/2011 Johdon tietoturvaopasta sekä VAHTI 2/2014 Tietoturvallisuuden arviointiohjetta.

6.3 Kohderyhmä ja tarpeiden kartoitus

Haasteen koulutusmateriaalin teolle toi koulutuksen tulevan tarkan kohderyhmän epävarmuus. Kohderyhmäksi määriteltiin projektin alussa julkishallinnon organisaation tietoa käsittelevä henkilöstö. Tämän tarkemmin kohderyhmä ei koulutusmateriaalin valmistelun aikana selvinnyt. Aikataulun puitteissa työn oli edettävä, joten päätimme edetä haastattelemalla yhden mahdollisen kohdeorganisaation henkilöstöä tarkemmin. Haastattelun keinoin tarkoituksena oli tuoda esiin asioita, joiden merkitystä kannattaisi mahdollisesti korostaa koulutusmateriaalia kirjoitettaessa samankaltaista työtä tekevälle henkilöstölle.

Haastattelu toteutettiin koulutuskokonaisuuden yhteen mahdolliseen kohdeorganisaatioon, jonka nimeä ei opinnäytetyössä sopimussyistä tuoda esille. Haastateltu kohdeorganisaatio on alueellisesti toimiva valtakunnallisen organisaation osa, jonka 19 työntekijästä haastateltiin kaksi henkilöä. Haastateltavia henkilöitä olivat alueellisen organisaation ylitarkastaja sekä yksi tutkijoista.

Haastattelussa kävimme läpi käytännön tietoturvaan ja tietoturvalliseen toimintaan liittyviä asioita kyseisessä organisaatiossa. Haastattelu oli muodoltaan

teemahaastattelu, jonka aihepiirit laadittiin teoreettisen kehyksen pohjalta. Kehyksenä käytettiin perustasoa asetuksesta tietoturvallisuudesta valtionhallinnossa (Liite 3.). Kaikkia tässä asetuksessa mainittuja kohtia ei kuitenkaan ollut koulutusmateriaalin teon kannalta oleellista käydä tarkasti läpi, vaan keskustelu kohdistettiin etenkin tietoturvaan liittyvään koulutukseen sekä organisaation ohjeistuksiin. Kirjoitin haastattelun aikana muistiinpanot keskustelussa esiin tulleista huomionarvoisista asioista.

Haastattelussa esiin tulleet tietoturvakoulutusmateriaalin tekoon liittyvät huomiot olivat seuraavanlaisia: organisaation sisäisestä intranetistä löytyi tietoturvaan liittyvä laaja Valtionhallinnon ohjeistus, sekä muutama ajankohtainen tietoturvaan liittyvä uutinen tiedon kalasteluyrityksiin liittyen. Työhön liittyvien salaisten materiaalien käsittelyyn liittyvät ohjeet olivat saatavilla sekä paperiversioina että sähköisenä. Ohjeet etätyöhön sekä sosiaalisen median käyttöön olivat työntekijöiden saatavilla intranetissä. Tietoturvaan liittyvää koulutusta oli järjestetty viimeisen viiden vuoden aikana, koulutuksen osallistujia ei kuitenkaan tiettävästi ollut dokumentoitu. Organisaation varsinaisen tietoturvapolitiikan tarkka sisältö sekä sen saatavuus oli haastatelluille epäselvä. (Lahtinen 2015.)

Haastattelussa selvinneet asiat olivat jokseenkin odotettavissa. Työhön olennaisesti liittyvän salaisen materiaalin käsittelyä koskevia lainmukaisia ohjeistuksia on olemassa, ja ne ovat salaista tietoa käsittelevän henkilöstön tiedossa. Myös muuhun tietoturvaan liittyviä ohjeistuksia on työntekijöiden saatavilla. Näihin muihin intranetistä löytyviin laajoihin ohjeistuksiin perehtyminen vaatii kuitenkin jossain määrin työntekijän omaa aktiivisuutta. Oman organisaation tietoturvapolitiikan sisältö voi olla organisaation tietoturvaan liittyvien asioiden kanssa harvemmin tekemisissä olevalle työntekijälle epäselvä.

6.4 Toteutus ja sisältö

Valtionhallinnon ohjeistusten sekä tehdyn esityön pohjalta aloitettiin varsinaisen koulutusmateriaalin tarkemman sisällön hahmottelu. Koska täysin tarkka kohdeorganisaatio ei ollut tiedossa, koulutusmateriaali pyrittiin tekemään yleisesti hyväksyttyihin tietoturvakäytäntöihin pohjautuen, kuitenkin esimerkkiorganisaation haastattelussa esiin tulleet asiat huomioiden. Materiaalin tuli sisältää tietoturvan perusteet, sekä käytännön ohjeistusta päivittäisiin tietoturvaan ja tietoturvan ylläpitoon liittyviin toimiin. Myös tietoturvatason arviointiin liittyvä osuus päätettiin lisätä materiaalin loppuun.

Koulutusmateriaali pyrittiin suhteuttamaan julkishallinnon organisaation perushenkilöstön tarpeisiin sopivaksi niin sisällöltään kuin laajuudeltaankin. Sisältö pyrittiin pitämään mahdollisimman selkeänä, jotta materiaali on miellyttävää luettavaa myös tietoturvaan vähemmän perehtyneille koulutettaville.

Tietoturvakoulutuksen pohjana käytettävä teoriaosuus toteutettiin Word-dokumenttina myöhemmän julkaisutavan epävarmuudesta johtuen. Varmaa tässä vaiheessa oli, että materiaali tulisi pohjaksi keväällä 2016 mahdollisesti järjestettävälle koulutustilaisuudelle. Keskusteluissamme esille tuli kuitenkin myös mahdollisuus esimerkiksi verkossa jaettavalle julkaisulle.

Valmis tietoturvakoulutusmateriaalidokumentti (Liite 1. Salattu) koostui kolmesta osasta. Materiaalin ensimmäisessä osassa käsitellään tietoturvaa yleisesti, sekä selvitetään eri tietoturvakäsitteiden merkitystä. Ensimmäisen kappaleen alaluvut sisältävät tietoturvan määritelmän, kansallisen lainsäädännön ja asetusten esittelyn, tietoturvan osa-alueiden esittelyn, esimerkkejä tietoturvauhista, sekä katsauksen tietoturvan riskienhallintaan ja kehittämiseen. Teoriaosuus pohjautuu pitkälti opinnäytetyön teoriaosuuteen.

Toisessa osassa (Kuva 1.) perehdytään tarkemmin niihin käytännön toimiin, jotka vaikuttavat organisaation tietoturvan ylläpitoon.

Kuva 1. Kuvankaappaus koulutusmateriaalin toisen osan sisällöstä.

Alaluvuissa käsitellään asiakirjallisen tiedon vaatimuksia ja käsittelyä, tietoturvan toteuttamisen osatekijöitä, sekä organisaation perushenkilöstön toimia tietoturvan toteuttamisessa. Perushenkilöstön toimet on jaettu alaotsikoihin asiakirjan elinkaari ja luottamuksellisen materiaalin käsittely, tietokoneiden ja muiden päätelaitteiden käyttö, internetin ja sähköpostin käyttö, käyttöoikeudet ja salasanaturvallisuus, etä- ja matkatyö, välineistön ja toimitilojen turvallisuus sekä ongelmatilanteissa reagointi. Toisen osuuden pohjana on hyödynnetty pitkälti Valtionhallinnon henkilöstön tietoturvaohjetta (4/2003).

Koulutusmateriaalin kolmannessa ja viimeisessä osassa tutustutaan vielä tietoturvan arviointiin ja arvioinnin keinoihin, sekä organisaation sisällä että ulkoisesti. Oppimateriaali on laajuudeltaan 19 sivua ja sisältää kahden sivun mittaisen keskeisiä tietoturvaan liittyviä termejä selittävän sanaston. Word-dokumentin lisäksi laadittiin materiaalia tukeva esitysgrafiikka (Liite 2. Salattu).

6.5 Arviointi ja palaute

Koulutusmateriaali valmistui toimeksiantajan käyttöön sovitusti ja oli sisällöltään toiveiden mukainen. Kohderyhmä, jolle koulutusmateriaali valmisteltiin, ei materiaalin kirjoitusprosessin aikana täysin tarkentunut. Haastatellun organisaation

vastausten yleistettävyys pyrittiin kuitenkin huomioimaan koulutusmateriaalia kirjoitettaessa. Kohderyhmän tarkentuessa tietoturvan perusteita käsittelevän materiaalin täydennys käy vaivattomasti. Ennen varsinaisen koulutustilaisuuden järjestämistä olisi tärkeää huomioida vielä esimerkiksi koulutukseen osallistuvien taustatiedot, kohderyhmälle sopivat oppimismenetelmät sekä oppimisympäristön vaikutukset itse koulutustilanteeseen.

Koulutusmateriaalin sisällön tavoitteiksi asetettiin suunnitteluvaiheessa selkeys ja käytännöllisyys. Selkeyttä pyrittiin lisäämään myös opinnäytetyössä käytettyjen tekstiin lisättyjen kuvioiden avulla. Päivittäisiä toimia organisaatiossa tuotiin esiin käytännön esimerkein ja tietoturvaan olennaisesti liittyviä sanoja lisättiin materiaalin alun sanastoon sisällön ymmärtämisen helpottamiseksi. Myös koulutusmateriaalin tueksi tehty diaesitys voi osaltaan tehostaa tilaisuuteen osallistuvien oppimista.

Koulutusmateriaalin sisällön onnistumisen arvioimiseksi kevään koulutustilaisuuteen olisi hyvä yhdistää lyhyt palautekysely. Näin saataisiin selville kuinka hyvin materiaali on tavoittanut kohderyhmänsä ja mitä materiaaliin vielä mahdollisesti toivottaisiin. Mikäli koulutustilaisuudessa päätetään teettää osallistujilla oppimista syventäviä tehtäviä, myös näiden vastaukset voivat auttaa tässä kehitysprojektissa - oliko joukossa kysymyksiä, joihin osallistujat eivät varsinaisen koulutustilaisuuden jälkeen osanneet vastata? Mikäli näitä tulee ilmi, on syytä pohtia miksi näin on, ja miten opettamista ja kohderyhmän oppimista voisi vielä tehostaa toivotun tuloksen aikaansaamiseksi.

7 YHTEENVETO JA POHDINTA

Tietoturva on laaja kokonaisuus, jonka hallinta yksityishenkilönä ja erityisesti organisaation toiminnassa edellyttää toimia esimerkiksi tietoturvan suunnitteluun, ylläpitoon ja seurantaan liittyen. Kaikkia tietoturvaa uhkaavia tekijöitä ei voida mitätöidä, eikä organisaation toiminnan jatkumisen kannalta tämä ole edes oleellista. Riskikartoitukset ja toimien suunnittelu tuleekin järjestää niin, että toimet tiedon turvaamiseksi kohdennetaan todennäköisten uhkien toteutumisen ennaltaehkäisemiseen. Yhtenä suurimmista tietoturvaan vaikuttavista tekijöistä pidetään ihmistä, minkä vuoksi tietoisuuden jakamista ja erityisesti organisaatiossa koulutuksen merkitystä voidaan tuskin liikaa korostaa.

Opinnäytetyön keskeisiä tavoitteita olivat tietoturvan merkityksen sekä yleisten uhkatekijöiden kartoittaminen paitsi yleisesti, myös organisaation näkökulmasta. Mielestäni nämä tavoitteet toteutuivat suunnitellusti.

Tarkoituksena oli pitää työ selkeänä ja sisällöltään varsinaista tietoturvakoulutusmateriaalin tekoprosessia tukevana. Tietoturvan laajuuden takia aiheiden rajaus sekä selkeä jaottelu asetti haasteita työn alkuvaiheessa. Lopputuloksessa olen pyrkinyt käsittelemään tiiviisti eri osa-alueiden opinnäytetyön empiiriseen osuuteen merkittävästi liittyviä asioita. Laajojen aiheiden käsittely on työssäni kuitenkin melko pintapuolista.

Teoriaosuuden pohjana käytettiin pääasiallisesti kirjallisuutta sekä erilaisia verkkojulkaisuja. Verkkojulkaisuiden valinnoissa pyrin valitsemaan mahdollisuuksien mukaan tunnettuja julkaisijatahoja. Osa kirjallisista lähteistä on julkaistu jo 2000-luvun alkupuolella, mutta käsiteltyjen aiheiden muuttumattomuuden vuoksi lähteitä voidaan edelleen pitää käyttökelpoisena perusteita esittelevän opinnäytetyön pohjaksi.

Varsinaisen koulutustilaisuuden tarkempia yksityiskohtia voidaan selvittää vasta kohderyhmän tarkennuttua. Koulutustilaisuuden järjestämisessä, seurannassa ja arvioinnissa voisikin olla aihetta jatkotutkimukselle.

LÄHTEET

Aho, T. 2010a. Valtiovarainministeriö. Luokiteltujen tietoaineistojen käsittelyvaatimuksia. Viitattu 24.11.2015. https://www.vahtiohje.fi/web/guest/luokiteltujen-tietoaineistojen-kasittelyvaatimuksia.

Aho, T. 2010b. Valtiovarainministeriö, Tietoaineistojen luokittelu. Viitattu 24.11.2015. https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu

Apple Inc. 2015. OS X Mavericks: Virtuaalisen lähiverkon (VLAN) käyttäminen. Viitattu 10.12.2015. https://support.apple.com/kb/PH14163?viewlocale=fi_FI&locale=fi_FI.

Arkistolaitos. 2015. Keskeiset käsitteet. Viitattu 24.11.2015. http://www.arkisto.fi/fi/palvelut/julkaisuluettelo/d-verkko-oppaat/arkistot-yhteiskunnan-toimiva-muisti/keskeiset-kaesitteet

BS7799 Audit & Compliance. 2002. The BS7799 Security standard. Viitattu 10.12.2015. http://www.riskserver.co.uk/bs7799/

Fraser, B. 1997 Site Security Handbook. Viitattu 12.9.2015. ftp://ftp.funet.fi/pub/standards/RFC/rfc2196.txt.

Haakana, K. 2002. Krakkerit ja haktivistit vaanivat. Tietoviikko. Viitattu 28.10.2015. http://www.tivi.fi/Arkisto/2002-02-14/Krakkerit-ja-haktivistit-vaanivat-3092740.html

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

ITSMF Finland. 2015a. Cobit 5. Viitattu 10.12.2015. http://vanha.itsmf.fi/cobit.

ITSMF Finland. 2015b. ITIL ja parhaat käytännöt. Viitattu 10.12.2015. http://itsmf.fi/itil-parhaat-kaytannot/.

ISO/IEC 17799

Järvinen, P. 2012. Arjen tietoturva – vinkit ja ratkaisut. Jyväskylä: Docendo.

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo.

Jyväskylän yliopisto. 2015. Oppimiseen vaikuttavat tekijät ja opetukselliset tavoitteet. Viitattu 10.12.2015. https://koppa.jyu.fi/avoimet/mit/Verkkokurssin%20tuotantoprosessi/johdanto-verkkokurssien-maailmaan/yleistae-opetuksen-suunnittelusta-1/oppimiseen-vaikuttavat-tekijaet-ja-opetukselliset-tavoitteet.

Kajaanin ammattikorkeakoulu. 2015. Toimitatutkimus. Viitattu 7.12.2015. https://www.kamk.fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Toimintatutkimus.

Karsisto, T. 2007. Tietoturvariskianalyysin tehostaminen työkalun avulla. Diplomityö. Espoo: Teknillinen korkeakoulu. Viitattu 25.11.2015 http://lib.tkk.fi/Dipl/2007/urn007703.pdf.

Kotimikro. 2009. Kaistanleveys. Viitattu 25.11.2015. http://kotimikro.fi/ordbog-nasto/kaistanleveys.

Laakso, M. 2015a. Ohjelmistoturvallisuus. Viitattu 30.9.2015. http://www.tietojesiturvaksi.fi/tietoturvasuunnitelma/ohjelmistoturvallisuus.

Laakso, M. 2015b. Fyysinen tietoturva. Viitattu 30.9.2015. http://www.tietojesiturvaksi.fi/tietoturvasuunnitelma/fyysinen-tietoturva.

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

Lahtinen, M. 2015. Kohdeorganisaation henkilöstön edustajien haastattelu. 10.9.2015.

Legal Information Institute. 2015. Definitions. Viitattu 2.10.2015 https://www.law.cornell.edu/uscode/text/44/3542.

Linux.fi. 2015. Palvelin. Viitattu 25.11.2015. https://www.linux.fi/wiki/Palvelin.

Microsoft. 2015a. Palomuuri: Usein kysytyt kysymykset. Viitattu 19.11.2015 http://windows.microsoft.com/fi-fi/windows/firewall-faq#1TC=windows-7.

Microsoft. 2015b. Mitä eroa on keskittimellä, kytkimellä, reitittimellä ja tukiasemalla?. Viitattu 25.11.2015 http://windows.microsoft.com/fi-fi/windows/hubs-switches-routers-access-points-differ#1TC=windows-7.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media Oy.

MindTools. 2015. Plan-Do-Check-Act (PDCA). Viitattu 23.11.2015 https://www.mindtools.com/pages/article/newPPM_89.htm.

Opi tietosuojaa. 2015. EU:n tietosuoja-asetuksen velvoitteet johdolle. Viitattu. 28.10.2015 https://opitietosuojaa.fi/index.php/fi/56-lainsaeaedaentoe/lait/eun-tietosuoja-asetus.

Palvelunestohyökkäykseltä voi suojautua 2007. Digitoday. Viitattu 24.11.2015. http://www.digitoday.fi/tietoturva/2007/06/15/palvelunestohyokkaykselta-voi-suojautua/200714925/66.

Pietikäinen, S. 2013. Valtiovarainministeriö, Tietoturvallisuus – mitä se on?. Viitattu 29.9.2015 https://www.vahtiohje.fi/web/guest/691.

Puolustusministeriö. 2015. Katakri 2015 – tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 7.12.2015. http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille.

Saaranen-Kauppinen, A . & Puusniekka, A. 2006. KvaliMOTV - Toimintatutkimus. Viitattu 26.11.2015. http://www.fsd.uta.fi/menetelmaopetus/kvali/L5_4.html.

Sanastokeskus TSK. 2004. Tiivis tietoturvasanasto. Viitattu 26.11.2015 http://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf-

Sanastokeskus TSK:n termipankki. 2015a. Tietojärjestelmä. Viitattu 25.11.2015 http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&height=165&qfind=tietoj%C3%A4rjestelm%C3%A4.

Sanastokeskus TSK:n termipankki. 2015b. Tietoverkko. Viitattu 25.11.2015 http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&height=158&qfind=tietoverkko.

Suomen standardisoimisliitto. 2015. ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä. Viitattu 8.12.2015. http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta.

Symantec. 2008. VPN-opas. Viitattu 25.11.2015 http://www.symantec.com/region/fi/resources/vpn.html.

Tietosuojavaltuutetun toimisto. 2010. Biometrinen tunnistus – mikä se on?. Viitattu 25.11.2015 http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqPiEON/Biometrinen_tunnistus_mika_se_on.pdf.

Tirronen, H. 2003. Tietoturvan osa-alueet. Viitattu. 4.11.2015 http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html.

Turun yliopisto. 2015. Turun yliopiston Brahea–keskus. Viitattu 24.11.2015 http://www.utu.fi/fi/yksikot/braheakeskus/Sivut/home.aspx.

Valtiovarainministeriö. 2015a. Ohjeiden ryhmittely, tietoturvallisuuden osa-alueet. Viitattu 24.11.2015 https://www.vahtiohje.fi/web/guest/vahti-ohjeet-by-caterogy.

Valtiovarainministeriö. 2015b. Laitteistoturvallisuus. Viitattu 4.11.2015 https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus.

Valtiovarainministeriö. 2009. Tietoaineistoturvallisuus. Viitattu 27.10.2015 https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus.

Vedenoja, J. 2007. Yrityksen fyysinen tietoturva. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Lahti: Lahden ammattikorkeakoulu. Viitattu 26.11.2015 https://www.theseus.fi/bitstream/handle/10024/11928/2007-12-03-18.pdf.

”Asetus tietoturvallisuudesta valtionhallinnossa - 1.7.2010/681 5 §

Tietoturvallisuuden perustason täyttäminen edellyttää asetuksen mukaisesti alla kuvattuja toimenpiteitä. Tietoturvatasojen tarkemmat toteuttamisohjeet ja vaatimukset löytyvät julkaisusta Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010).

Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:

1. viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan
2. viranomaisen käytössä on riittävä asiantuntemus tietoturvalllisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3. asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4. tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5. asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6. tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7. asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8. henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
9. henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10. annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.”