TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ JYVSECTEC -HANKKEESEEN
CASE: Tietoturvan testausjärjestelmä

Mikko Nisonen

Opinnäytetyö
Joulukuu 2012

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

Tekijä
NISONEN, Mikko

Julkaisun laji
Opinnäytetyö

Päivämäärä
11.12.2012

Sivumäärä
75

Julkaisun kieli
Suomi

Verkkojulkaisulupa myönnetty
(X)

Työn nimi
TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ JYVSECTEC -HANKKEESEEN, CASE: Tietoturvan testausjärjestelmä

Koulutusohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
HAUTAMÄKI, Jari; HÄKKINEN, Antti

Toimeksiantaja(t)
Jyväskylä Security Technology
WECKSTRÖM, Petteri

Tiivistelmä

Opinnäytetyö toteutettiin Jyväskylän ammattikorkeakoulussa vuonna 2011 aloitettuun JYVSECTEC -hankkeeseen. JYVSECEC -hankkeessa toteutetaan tietoturvan testaus-, kehitys- ja koulutuspalveluita yhteistyöverkoston käyttöön.

Opinnäytetyön tavoitteena oli toteuttaa tietoturvallisuuden hallintajärjestelmä JYVSECTEC -hankkeeseen tietoturvan testausjärjestelmän osalta. Testausjärjestelmä sisältää teknisen testauksen ohjelmistoihin ja laitteisiin. Hankkeella ei ollut tietoturvan toteutusta. Opinnäytetyön tuloksena saatujen dokumenttien pohjalta hankkeeseen oli tarkoitus luoda tietoturvallisuuden hallintajärjestelmä.

Opinnäytetyön teoriaosuus pohjautuu suurelta osin ISO 27000 -sarjan tietoturvastandardiperheeseen. Teoriaosuudessa perehdyttiin teoreettiseen tietoturvan toteutukseen. Käytännön toteutuksessa hyödynnettiin VAHTI 2/2010 ja KATAKRI II asiakirjoja.

Työn tuloksena JYVSECTEC -hankkeelle suoritettiin suojattavien kohteiden kartoitus, jossa listattiin hankkeelle tärkeitä suojattavia kohteita. Suojattaville kohteille suoritettiin riskianalyysi. Riskianalyysissä havaittuihin uhkiin kehitettiin turvamekanismeja. Turvamekanismit sisällytettiin tietoturvantestausympäristöön. Opinnäytetyössä otettiin myös kantaa tietoturvan koulutukseen hankkeessa. Testausympäristöön suoritettiin KATAKRI II mukainen turvallisuusauditointi, jonka pohjalta havaittuja puutteita hankkeessa korjattiin.

Lopputuloksena opinnäytetyön pohjalta JYVSECTEC -hankkeen tietoturvan testausjärjestelmään integroitiin tietoturvallisuuden hallintajärjestelmä. Tietoturvan kehittäminen hankkeessa jatkuu tämän opinnäytetyön pohjalta.

Avainsanat (asiasanat)
Tietoturva, JYVSECTEC, Riskianalyysi, KATAKRI, Auditointi, Hallintajärjestelmä, ISO 27000

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author(s)	Type of publication	Date
NISONEN, Mikko	Bachelor´s Thesis	11122012
	Pages 75	Language Finnish
		Permission for web publication (X)

Title
INFORMATION SECURITY MANAGEMENT SYSTEM FOR JYVSECTEC -PROJECT, CASE: Information security testing system

Degree Programme
Information Technology

Tutor(s)
HAUTAMÄKI, Jari; HÄKKINEN, Antti

Assigned by
Jyväskylä Security Technology
WECKSTRÖM, Petteri

Abstract

The thesis was carried out for JYVSECTEC -project which started in September 2011 in JAMK University of Applied Sciences. The JYVSECTEC -project's objective is to produce information security testing, developing and educational services for the use of collaboration network.

The purpose of this thesis was to create information security management system for JYVSECTEC -project focusing on information security testing system. Testing system includes technical testing for programs and devices. At the beginning the project did not have information security implementation. The purpose of the documents which were made during this thesis was to create information security management system for the JYVSECTEC -project.

The theory part of this thesis is mostly based on ISO 27000 -series of information security standards. Theory part consists of theoretical information security implementation. VAHTI 2/2010 and KATAKRI II documents were used in practice section of the thesis.

As a result of the thesis for JYVSECTEC -project inventory of important assets was created and risk analysis was conducted for them. Security mechanisms were created for the threats which were discovered in the risk analysis. These mechanisms were integrated to information security testing environment. Information security education is also mentioned in the thesis. KATAKRI II based security audit were made for testing environment and discovered faults were corrected.

As a final result of this thesis information security management system were integrated to information security testing environment in JYVSECTEC -project. Information security development continues based on this thesis.

Keywords
Information security, JYVSECTEC, Risk analysis, KATAKRI, Audit, Management system, ISO 27000

Miscellaneous

SISÄLTÖ

KUVIOT

TERMIT JA MÄÄRITELMÄT

Eheys	”ominaisuus, että suojattavien kohteiden oikeellisuus ja täydellisyys turvataan”
Haavoittuvuus	”suojattavan kohteen tai kohteiden ryhmän heikkous, jota yksi tai useampi uhka voi käyttää hyväksi”
Jäännösriski	”riskien käsittelyn jälkeen jäljellä oleva riski”
Kolmas osapuoli	”henkilö tai elin, jonka on tunnistettu olevan riippumaton asiaan liittyvistä osapuolista kyseisessä asiassa”
Käytettävyys	”ominaisuus olla saatavilla ja käyttökelpoinen valtuutetun tahon niin vaatiessa”
Luottamuksellisuus	”ominaisuus, että tietoa ei anneta käytettäväksi tai paljasteta luvattomille henkilöille, tahoille tai prosesseille”
Ohje	”selkiyttävä kuvaus, mitä tulisi tehdä ja miten, jotta saavutetaan politiikassa asetetut tavoitteet”
Politiikka	”johdon julkituoma yleinen tarkoitus ja suunta”
Riski	”tapahtuman todennäköisyyden ja sen seurauksen yhdistelmä”
Riskien arviointi	”yleiskäsite, joka kattaa riskianalyysin ja riskien vaikutuksen arvioinnin”

Riskien hallinta	”koordinoidut toimenpiteet, joilla johdatetaan ja ohjataan organisaation riskien käsittelyä”
Riskien käsittely	”prosessi, jossa valitaan ja toteutetaan riskejä muuttavia toimenpiteitä”
Riskien välttäminen	”päätös pysytellä poissa riskitilanteesta tai toimenpide, jolla poistutaan riskitilanteesta”
Riskianalyysi	”systemaattinen tietojen käyttäminen riskien tunnistamiseen ja niiden vaikutuksen arviointiin”
Suojattava kohde	”mikä tahansa, mikä on arvokas organisaatiolle”
Tietoturvahäiriö	”yksi tai useampi epätoivottu tai odottamaton tietoturvatapahtuma, joka merkittävällä todennäköisyydellä vaarantaa liiketoiminnot ja uhkaa tietoturvallisuutta”
Tietoturvallisuus	”tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttäminen; lisäksi tähän voi sisältyä muita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus”
Tietoturvallisuuden hallintajärjestelmä	”se osa yleistä toimintajärjestelmää, joka liiketoiminta riskien arviointiin perustuen luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan ja ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus”
Tietoturvariski	”mahdollisuus, että jokin uhka hyödyntää suojattavan kohteen tai suojattavien kohteiden ryhmän haavoittuvuutta ja siten aiheuttaa organisaatiolle haittaa”

Tietoturvatapahtuma	”sellainen tunnistettu järjestelmän, palvelun tai verkon tila, joka viittaa mahdolliseen tietoturvapolitiikan murtamiseen tai turvatakuiden pettämiseen, tai aikaisemmin tuntematon tilanne, jolla saattaa olla merkitystä turvallisuudelle”
Turvamekanismi	”keino hallita riskejä, sisältäen periaatteet, menettelytavat, ohjeet, käytännöt tai organisaatiorakenteet, jotka voivat olla luonteeltaan hallinnollisia, teknisiä, juridisia tai johtamiseen liittyviä”
Uhka	”mahdollinen syy epätoivottuun tapahtumaan, josta voisi seurata haittaa järjestelmälle tai organisaatiolle”
Vaikuttavuus	”haitallinen muutos liiketoimintatavoitteiden saavuttamisen tasossa”

(SFS ISO/IEC 17799:fi 2006, 20-23; SFS ISO/IEC 27001:fi 2006, 10-13; SFS ISO/IEC 27005 2009, 10-11.)

1 OPINNÄYTETYÖN LÄHTÖKOHDAT

1.1 JYVSECTEC -hanke toimeksiantajana

Jyväskylän ammattikorkeakoulun teknologiayksikössä aloitettiin vuoden 2011 syyskuussa JYVSECTEC -hanke (Jyväskylä Security Technology). Hankkeen tarkoituksena on toteuttaa keskitetty johto- ja valvontakeskus laite- ja verkkoympäristöineen, jossa pystytään tarkkailemaan tietoturvan tilannekuvaa. Hankkeen avulla pystytään testaamaan järjestelmiin kohdistuvia tietoturvauhkia evaluoimalla hyökkäyksiä ja samalla kehittämään erilaisia suojamekanismeja hyökkäyksiä vastaan. Hankkeen tarkoituksena on myös toteuttaa tuotekehitystä samassa ympäristössä. Sen puitteissa voidaan myös kouluttaa tietoturvaa kolmansille osapuolille yksityisellä ja julkishallinnollisella sektorilla. (JYVSECTEC – Jyväskylä Security Technology. 2012.)

1.2 Tehtävä ja tavoitteet

Aihealueen tarkennus

Opinnäytetyön lähtökohtana oli toteuttaa toimeksiantajalle, JYVSECTEC -hankkeelle tietoturvallisuuden hallintajärjestelmä. Toimeksiantajan resurssien puutteen vuoksi jouduttiin kaventamaan opinnäytetyön aihealuetta koskemaan ainoastaan JYVSECTEC -hankkeen omissa tiloissa tapahtuvan teknisen testauksen tietoturvallisuuden hallintajärjestelmää. Tämä testaus käsittää kolmannen osapuolen laitteisiin ja ohjelmistoon tapahtuvan testauksen. Aihealueen tarkennuksella saavutettiin myös tarkempi perehtyminen yhden osa-alueen tietoturvallisuuden hallintajärjestelmään.

Opinnäytetyön tuloksena toimeksiantajalle oli toteuttaa tietoturvatestauksen riskienhallinta ja tietoturvan jatkuvan kehittämisen suunnitelma. Nämä ovat erillisiä dokumentteja, joiden pohjalta tietoturvaa hankkeessa toteutetaan.

Edellä mainittuihin tuloksiin sisältyvät uhkakartoitukset, riskienhallinta ja turvamekanismien määrittelyt testauksen osalta.

Opinnäytetyön tavoitteena oli luoda työkalu, jolla tietoturvallisuuden hallintajärjestelmää kehitetään. Hallintajärjestelmän pohjalta hankkeeseen tullaan luomaan selkeät ohjeet tietoturvallisuuden ylläpitämiseen. Näitä ohjeita noudattamalla pyritään luomaan tietoturvallinen ympäristö, jossa tietoverkkoturvallisuutta voidaan kehittää. Tärkein tavoite tässä opinnäytetyössä oli luoda yleinen toimintamalli ja menetelmät tietoturvallisuuden hallinnalle ja tietoturvan jatkuvuuden toteutukselle. Tavoitteena oli myös suorittaa turvallisuusauditointi KATAKRI II asettaman suojaustaso 4 mukaisesti. Lisäksi opinnäytetyön tarkoituksena oli laatia toimenpiteet, joiden avulla suojaustaso 4 hankkeessa saavutetaan.

JYVSECTEC -hanke on keskittynyt tietoverkkoturvallisuuteen ja sen kehittämiseen, joten tietoturvallisuuden tulee itse hankkeessa olla hyvällä tasolla. Hyvällä tietoturvallisuuden tasolla tarkoitetaan muun muassa jatkuvaa tietoturvan kehittämistä ja tietoturvan huomioon ottamista päivittäisessä käytössä. Toteutuksessa tulee myös ottaa huomioon mahdolliset kolmansien osapuolien asettamat haasteet tietoturvan ylläpitämiseksi. (JYVSECTEC – Jyväskylä Security Technology. 2012.)

Tietoturvasta ei voida koskaan sanoa, että se on täysin valmis, vaan sitä täytyy kehittää koko ajan. Ympäri maailmaa havaitaan jatkuvasti uusia tietoturvauhkia, jotka aiheuttavat toimenpiteitä kuluttajille, ohjelmistokehittäjille ja laitevalmistajille. Tavoitteena opinnäytetyössä oli luoda toimiva pohja hankkeen tietoturvalle, josta sitä voidaan kehittää erilaisten menetelmien avulla jatkossa.

1.3 Opinnäytetyön lähdemateriaali

Tietoturva on hyvin laaja käsite ja tässä opinnäytetyössä toteutettiin tietoturvallisuuden hallintajärjestelmä JYVSECTEC -hankkeelle, keskittyen vain hankkeelle oleellisiin kohteisiin. Teoriapohjana opinnäytetyössä käytettiin pääasiallisesti kolmea kansainvälistä tietoturvastandardia:

- SFS ISO/IEC 17799
- SFS ISO/IEC 27001
- SFS ISO/IEC 27005.

SFS ISO/IEC 17799 standardista on olemassa myös uudempi SFS ISO/IEC 27002, joka on saman sisältöinen standardi pienillä päivityksillä. Opinnäytetyön toteutuksessa oli saatavilla vanhempi versio, eli SFS ISO/IEC 17799. Standardit ovat yleispäteviä ohjeistuksia tietoturvallisuuden toteutukseen organisaatioissa. Standardeja ei ole pakko noudattaa, mutta ne antavat oikean suunnan organisaation tietoturvallisuuden kehitykselle. Organisaation kannalta näiden standardien mukainen tietoturvallisuuden toteutus on hyvä, sillä ne ovat tunnettuja maailmalla ja organisaatio voi markkinoida omaa tietoturvallisuuden tasoaan mainitsemalla standardeihin pohjautuvan tietoturvan. On otettava kuitenkin huomioon, että organisaatiossa täytyy suorittaa standardin mukainen auditointi, mikäli organisaatiota halutaan mainostaa standardien mukaisena. Opinnäytetyön käytännön toteutuksen pohjana toimivat:

- Kansallinen turvallisuusauditointikriteeristö (KATAKRI II)
- Valtionhallinnon tietoturvallisuuden johtoryhmän laatima asiakirja: ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta” (VAHTI 2/2010).

Edellä mainituissa asiakirjoissa otetaan kantaa tietoturvan toteutukseen käytännössä. Asiakirjat valittiin, koska ne ovat valtakunnallisesti tunnettuja ja käy-

tettyjä. Lisäksi niissä on määriteltynä käytännön suojausmenetelmiä eri suojaustason vaativille asiakirjoille. (Kansallinen turvallisuusauditointikriteeristö versio II. 2010.)

2 TIETOTURVALLISUUS

2.1 Määritelmä

Tieto eli informaatio on organisaation liiketoiminnalle tärkeä suojattava kohde. Nykyisin tietoa on monessa muodossa muun muassa sähköisesti tallennetussa dokumentissa ja paperille tulostettuna. Tieto tulisi aina suojata riippumatta siitä, missä muodossa se esiintyy. Nykyaikainen yhteiskunta asettaa haasteita tietoturvallisuudelle verkottumisen muodossa. Tiedon levittäminen eteenpäin on tehty helpoksi esimerkiksi perinteisen postin muodossa konkreettisena dokumenttina ja sähköpostin välityksellä sähköisessä muodossa. (SFS ISO/IEC 17799:fi 2006, 14-15.)

Tietoturvan toteuttamiseen tarvitaan turvamekanismeja. Turvamekanismeja ovat erilaiset ohjelmistotoiminnot ja laitteiden toiminnot, organisaatiorakenteet, prosessit ja toimintaperiaatteet. Turvamekanismien käyttöönotto ei yksin riitä, vaan niitä tulee katselmoida riittävän usein ja havaittuihin puutteisiin tulee reagoida. Tällöin tietoturvantoteutusta parannetaan jotta saavutetaan organisaation määrittämät tavoitteet tietoturvalle. (SFS ISO/IEC 17799:fi 2006, 14-15.)

2.2 Tarve

Tietoturvan tarve on kasvanut ja on suuressa osassa nyky-yhteiskunnassa. Erilaiset hyökkäykset palvelunestojen, hakkeroinnin ja haittaohjelmien muodossa ovat yleistyneet huomattavasti. Esimerkiksi CERT-FI sivustolle päivitetään viikoittain uusia maailmalla löydettyjä haavoittuvuuksia. Erilaisilla hyök-

käysmenetelmillä voidaan yrittää varastaa informaatiota yrityksen toiminnan kannalta tärkeistä kohteista tai vaikuttaa yrityksen maineeseen. Tietoturvaa uhkaavat myös fyysiset uhat, jotka eivät liity välttämättä tietoliikenteeseen, kuten vesivahingot, tulipalot ja ilkivalta. (SFS ISO/IEC 17799:fi 2006, 14-15.)

Tietoturvallisuus on oleellinen osa yritystä. Tietoturvallisuuden avulla pyritään varmistamaan yrityksen asema markkinoilla kilpailijoihin verrattuna. Hyvin toteutettu tietoturva takaa yrityssalaisuuksien säilymisen, työntekijöiden turvallisuuden sekä järjestelmien tehokkaan hyödyntämisen. (SFS ISO/IEC 17799:fi 2006, 14-15.)

Tietoturvan tarve korostuu entisestään tilanteissa, joissa kahden osapuolen tulee jakaa tietoja keskenään. Näissä tapauksissa hyvin suunniteltu ja toteutettu tietoturva takaa yhteistyön onnistumisen, ilman että tietoturvan tasosta poiketaan. Tietoturvaa suunniteltaessa otetaan huomioon kolmansien osapuolten kanssa toteutettava tietoturva, jota voidaan soveltaa erilaisissa yhteistyötilanteissa.

2.3 Vaatimusten luominen

Turvallisuusvaatimuksien tunnistaminen on organisaation kannalta tärkeää. Tällöin saavutetaan paras mahdollinen tietoturvan taso juuri kyseessä olevan organisaation tarpeisiin. Yleisesti turvallisuusvaatimuksiin on kolme pääasiallista lähdettä. Lähteet käsitellään seuraavaksi. (SFS ISO/IEC 17799:fi 2006, 14-15.)

Organisaatiossa suoritetaan riskianalyysi. Tämän avulla määritetään liiketoiminnalle ja tavoitteille kohdistuvat uhat. Suojattaville kohteille arvioidaan niiden altistuminen vahingoille, vahinkojen todennäköisyys sekä vahingoista mahdollisesti aiheutuvat vaikutukset organisaation toiminnalle. (SFS ISO/IEC 17799:fi 2006, 14-15.)

Sopimukset, säännökset, asetukset ja lainsäädäntö muodostavat omat vaatimukset, joita organisaation, kauppakumppanien, sopimusosapuolten sekä palveluntarjoajien on noudatettava. Esimerkiksi asiakirjoille voidaan määritellä eritasoisia luokituksia, joiden mukaan niitä suojataan. Yleisesti tunnettuja luokituksia ovat

- Erittäin salainen (Suojaustaso I)
- Salainen (Suojaustaso II)
- Luottamuksellinen (Suojaustaso III)
- Käyttö rajoitettu (Suojaustaso IV).

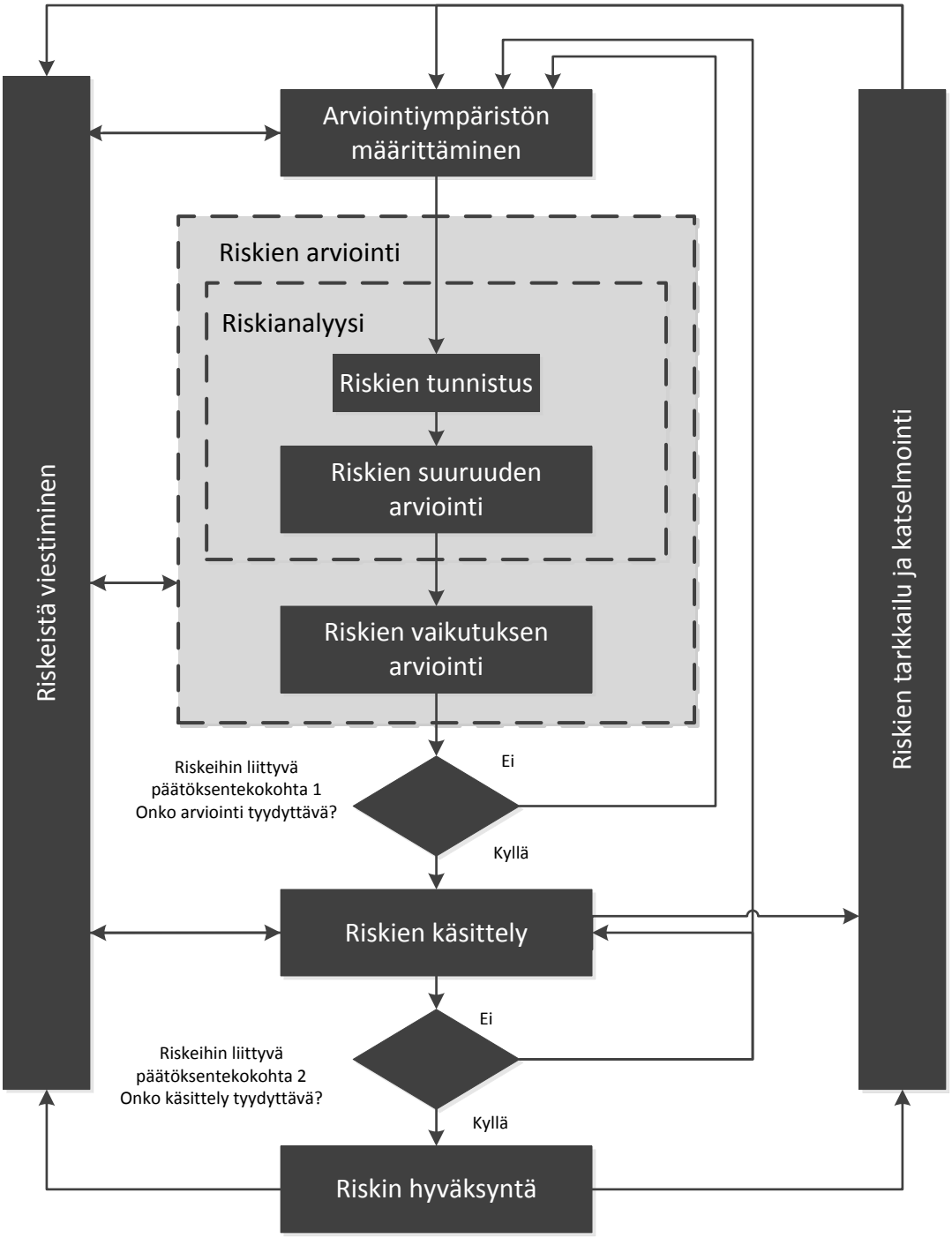
(A 1.7.2010/681; Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, 2/2010. 2010, 35; SFS ISO/IEC 17799:fi 2006, 16-17.)

Tässä opinnäytetyössä toimeksiantajaa auditoitaessa käytettiin arviointikriteerinä käyttörajoitettu (suojaustaso IV). Suojaustaso valittiin toimeksiantajan määräyksestä. Opinnäytetyöntekijällä ei ollut mahdollisuutta vaikuttaa valintaan.

Edellä mainittujen vaatimusten lisäksi tietojenkäsittelyyn liittyvät liiketoiminnan vaatimukset, tavoitteet ja periaatteet luovat vaatimuksen tietoturvalle. (SFS ISO/IEC 17799:fi 2006, 16-17.)

2.4 Riskien arviointi

Organisaatiossa on valittava toimintamalli, jolla tietoturvariskejä arvioidaan. Näin saavutetaan yhtenäinen prosessi tietoturvariskien arviointiin. Kuviossa 1 on esitetty vuokaavio, jota voidaan hyödyntää riskien hallintaan organisaatiossa.



KUVIO 1. Tietoturvariskien hallintaprosessi

(SFS ISO/IEC 27005 2009, 16-17)

Arviointiympäristöllä tarkoitetaan riskien hallintaan liittyvää organisaatiota sekä tietoturvallisuuden hallintajärjestelmän kattavuuden ja rajojen määrittämistä.

Riskien vaikutuksen arviointikriteereissä tulee ottaa huomioon muun muassa lakien ja viranomaisten asettamat vaatimukset ja sopimusvelvoitteet. Lisäksi tulee huomioida suojattavien kohteiden kriittisyys ja liiketoimintaprosessin strateginen arvo. (SFS ISO/IEC 27005 2009, 20-21.)

Vaikuttavuuskriteereillä tarkoitetaan tietoturvatapahtuman organisaatiolle aiheuttamaa vahinkoa tai kustannusta. Vaikuttavuuskriteereissä tulee ottaa huomioon muun muassa suojattavan kohteen luokitustaso, vahingoittuneet toiminnot ja rahalliset menetykset organisaatiolle. (SFS ISO/IEC 27005 2009, 22-23.)

Riskeille voidaan organisaatiossa määritellä erilaisia hyväksyntäkriteerejä perustuen muun muassa tietyissä tilanteissa sallittaviin riskeihin, arvioidun riskin ja mahdollisesti saavutettavan voiton suhteeseen ja riskin keston arviointiin. Mikäli riski on voimassa vain hetken aikaa, voidaan se tilapäisesti sallia. (SFS ISO/IEC 27005 2009, 22-23.)

Järjestelmällisellä turvallisuusriskien arvioinnilla voidaan määritellä turvallisuusvaatimukset yksittäisille osa-alueille. Turvamekanismien aiheuttamat kustannukset tulee arvioida suhteessa niiden epäonnistumisesta aiheutuvaan menetykseen organisaation kannalta. Organisaation johdon tehtävä on riskien arvioinnin pohjalta määritellä tarvittavat tietoturvan hallintatoimenpiteet, niiden tärkeysjärjestys sekä tarvittavien valvontamekanismien käyttöönotto. (SFS ISO/IEC 17799:fi 2006, 14-15.)

Lisää turvallisuuteen vaikuttavista riskeistä ja niiden hallinnasta kerrotaan luvussa 3.

2.5 Turvamekanismit

Turvallisuusvaatimusten, riskien tunnistamisen ja riskien käsittelypäätösten jälkeen valitaan ja toteutetaan turvamekanismit. Turvamekanismien avulla riskit pyritään alentamaan tasolle, jotka ovat hyväksyttäviä organisaation kannalta. Organisaatio voi siis itse päättää, mikä on hyväksyttävä taso erilaisille riskeille, jotka uhkaavat organisaatiota. (SFS ISO/IEC 17799:fi 2006, 16-17.)

Turvamekanismien valintaan ei ole yksiselitteistä käytäntöä, vaan ne voidaan valita standardiin perustuen, toisista turvamekanismijärjestelmistä tai organisaatiossa voidaan kehittää uusia erityisiin tarpeisiin pohjautuvia turvamekanismeja. Valintoihin tulisi kuitenkin soveltaa kaikkia asiaankuuluvia kansallisia ja kansainvälisiä lakeja ja asetuksia. (SFS ISO/IEC 17799:fi 2006, 16-17.)

3 TURVALLISUUSRISKIEN ARVIOINTI JA KÄSITTELY

Turvallisuusriskien arvioinnissa on tarkoitus eritellä organisaatiota koskevat riskit ja määritellä niiden suuruus. Riskien arvioinnissa luodaan järjestys, jonka pohjalta riskejä ryhdytään alentamaan, jotta päädytään organisaation kannalta hyväksyttyyn ratkaisuun. Turvallisuusriskien arvioinnista saatuja tuloksia organisaation johto pystyy käyttämään tietoturvallisuuden hallintatoimenpiteiden määrittämiseen. Lisäksi pystytään luomaan hallintatoimenpiteiden tärkeysjärjestys ja määrittämään turvamekanismien käyttöönotto. (SFS ISO/IEC 17799:fi 2006, 26-27.)

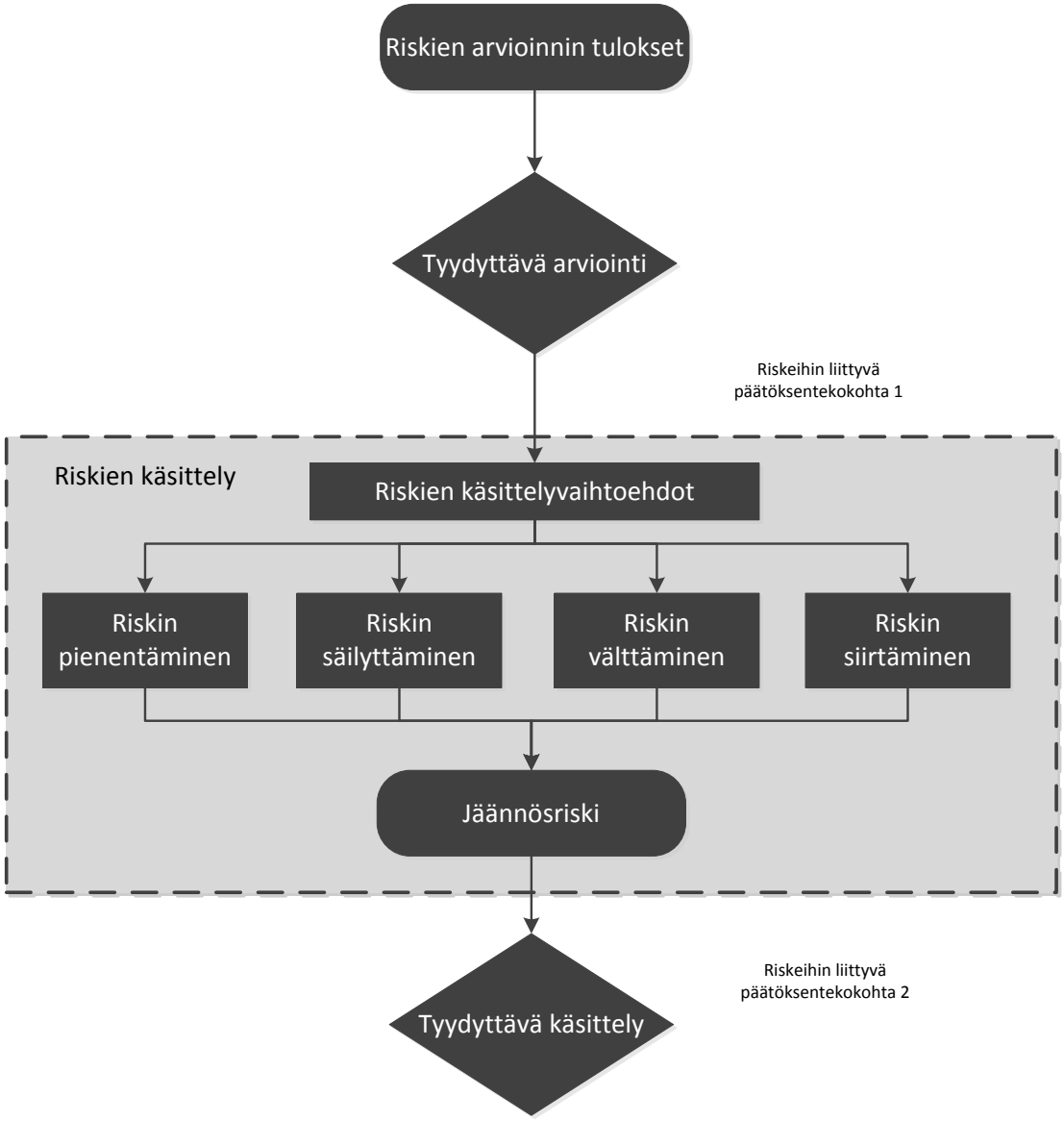
Turvallisuusriskejä arvioidessa tulee suorittaa riskianalyysi ja riskien vaikutuksen arviointi. Riskianalyysissä käydään läpi järjestelmällisesti organisaatiota uhkaavien riskien suuruusluokka. Riskien vaikutuksen arviointi on prosessi, jossa arvioituja riskejä verrataan riskikriteereihin, minkä jälkeen määritellään riskien merkittävyys. (SFS ISO/IEC 17799:fi 2006, 26-27.)

Turvallisuusriskejä tulee arvioida säännöllisin väliajoin ja yhdenmukaisin menetelmin, jotta arviot ovat luotettavia ja vertailukelpoisia keskenään. Arviointeja tulee suorittaa myös silloin, kun organisaatiossa tapahtuu huomattavia muutoksia uhkien tai suojattavien kohteiden osalta. Huomattava muutos voi olla esimerkiksi uuden järjestelmän käyttöönotto. Arviointeja tulee suorittaa, kun havaitaan riskitilanteita esimerkiksi uusia haavoittuvuuksia järjestelmissä. Arvioinneilla tulee myös olla selkeästi määritelty laajuus. (SFS ISO/IEC 17799:fi 2006, 26-27.)

Turvallisuusriskien arviointi voidaan suorittaa koko organisaatiolle, tietylle osalle organisaatiota, palvelulle tai yksittäiselle järjestelmälle organisaatiossa riippuen siitä, mikä on organisaation kannalta järkevää ja hyödyllistä. Tässä opinnäytetyössä arvioitiin JYVSECTEC -hankkeessa testaukseen liittyviä turvallisuusriskejä. (SFS ISO/IEC 17799:fi 2006, 26-27.)

Ennen turvallisuusriskien käsittelyä organisaatiossa on päätettävä kriteerit, joilla riskit joko hyväksytään tai mikäli ne aiheuttavat jatkotoimenpiteitä. Mikäli riski hyväksytään, tulee tämäkin tieto kirjata ylös. Näin varmistutaan, että organisaatiossa on otettu huomioon kaikki esille tulleet riskit. Riski voidaan hyväksyä, mikäli havaitaan sen olevan yritykselle vähäinen tai sen käsittelystä aiheutuvat kustannukset eivät ole organisaation kannalta järkeviä. (SFS ISO/IEC 17799:fi 2006, 26-27.)

Jatkotoimenpiteitä tarvitseville riskeille tehdään päätös aina riskikohtaisesti. Erilaisia käsittelyvaihtoehtoja on käsitelty kuviossa 2.



KUVIO 2. Riskien käsittelytoiminta

(SFS ISO/IEC 27005 2009, 42-43.)

Riskejä voidaan pienentää turvamekanismeilla. Riskin säilyttämisellä tarkoitetaan riskin hyväksymistä, mikäli se täyttää organisaation politiikan ja riskien hyväksymiskriteerit. Riskien välttämisellä tarkoitetaan esimerkiksi sellaisen toiminnon kieltämistä, josta riski aiheutuu. Riskin siirtämisellä tarkoitetaan sen välittämistä kolmannelle osapuolelle esimerkiksi vakuutusyhtiölle tai toimittajille. (SFS ISO/IEC 17799:fi 2006, 26-27.)

Kun turvallisuusriskin alentamisessa hyväksytylle tasolle tarvitaan asianmukaisia turvamekanismeja. Tällöin organisaation tulee ottaa huomioon seuraavat seikat:

- ”Kansallisen ja kansainvälisen lainsäädännön vaatimukset ja rajoitukset”
- ”Organisaation tavoitteet”
- ”Toiminnalliset vaatimukset ja rajoitukset”
- Aiheutuvat kustannukset, verrattuna riskin pienenemiseen
- Turvallisuusmekanismista aiheutuvien investointien tasapainotus riskin aiheuttamiin haittoihin nähden.

(SFS ISO/IEC 17799:fi 2006, 26-27.)

Turvallisuusriskejä käsitellessä tulee pitää mielessä, ettei millään turvamekanismien yhdistämisellä päästä täydelliseen tietoturvallisuuteen. Sillä täydellistä tietoturvaa ei ole olemassa. (SFS ISO/IEC 17799:fi 2006, 28-29.)

4 TIETOTURVAPOLITIIKKA

Tietoturvapolitiikasta tulee käydä ilmi organisaation johdon tuki ja aloitteellisuus tietoturvan toteuttamiselle. Tietoturvapolitiikka pohjautuu organisaation tavoitteisiin ja yleisiin kansallisiin ja kansainvälisiin lakeihin ja säädöksiin. Tietoturvapolitiikalla tulee olla organisaation johdon tuki ja sitoumus sen noudattamisesta. Lisäksi sen luominen ja ylläpito ovat organisaation johdon vastuulla. (SFS ISO/IEC 17799:fi 2006, 28-29.)

Organisaation johdon vastuulla on tiedottaa tietoturvallisuuspolitiikan olemassaolosta työntekijöille ja kolmansille osapuolille. Tietoturvapolitiikkaa tulee tuoda kaikkien organisaation jäsenten tietoisuuteen siten, että se on hyvin käytettävässä, ymmärrettävässä ja asianmukaisessa muodossa. Tietoturvapo-

litiikan määrittelyasiakirjasta tulee käydä selväksi johdon sitoutuminen tietoturvallisuuteen sekä organisaation näkemys tietoturvallisuuden hallinnasta. Organisaation tietoturvapolitiikasta julkaistavan määrittelyasiakirjan tulee sisältää julkilausumat seuraavista kohdista:

- Yrityksen johdon sitoutuminen tietoturvan ylläpitämiseen
- Yrityksen toimenpiteet tietoturvatapahtumien kirjaamiseen
- Tietoturvallisuuden merkitys yrityksen toiminnalle
- Tietoturvallisuuden toteutukseen liittyvän koulutuksen vaatimukset
- Maininta tietoturvapolitiikkaa tukevien asiakirjoista, joita tulee noudattaa
- Riskien arviointi ja riskienhallinnan rakenne
- Selvitys organisaatiolle tärkeiden menettelytapojen, periaatteiden, standardien ja vaatimusten noudattamisesta.

(SFS ISO/IEC 17799:fi 2006, 28-31.)

Tietoturvapolitiikkaa täytyy katselmoida tietyin väliajoin, jotta pystytään varmistumaan siitä, että se vastaa organisaation tarpeita. (SFS ISO/IEC 17799:fi 2006, 30-31.)

5 TIETOTURVAN TOTEUTUS

5.1 Yleistä tietoturvasta

Tietoturva on laaja käsite ja sen toteuttamiseen tarvitaan koko organisaation tuki. Organisaation johdolta täytyy tulla aloite tietoturvan toteuttamiseen, jotta muut työntekijät näkevät suunnan johon kyseisen organisaation tietoturva painottuu. Vaikka johdolla on suuri merkitys, on jokainen työntekijä tärkeä osa organisaation tietoturvaa tuomalla oman panoksensa ja edesauttamalla omalta osaltaan tietoturvan toteuttamista. Tietoturvakoulutukset organisaatiossa

auttavat työntekijöitä sisäistämään tietoturvan merkityksen ja luovat samalla hyvän pohjan organisaation tietoturvalle. (SFS ISO/IEC 17799:fi 2006, 32-33.)

5.2 Tietoturvallisuuden organisointi

Organisaation johdon tulee ottaa vastuu tietoturvallisuuden organisoimisesta. Organisointia varten tulee luoda hallintarakenne, jonka avulla tietoturvallisuuden toteuttaminen ja valvonta helpottuvat. Johdon tehtävänä on hyväksyä organisaatiossa laadittu tietoturvapolitiikka ja määrittää siihen liittyvät tehtävät henkilöille organisaation sisällä. (SFS ISO/IEC 17799:fi 2006, 32-33.)

Organisaation sisällä voidaan itse päättää, halutaanko käyttää ulkopuolisia tietoturvallisuuden asiantuntijoita. Ulkopuolisten asiantuntijoiden käyttö on suositeltavaa, sillä tämän avulla pysytään perillä tietoturvan kehityksessä, standardeissa sekä arviointimenetelmissä. (SFS ISO/IEC 17799:fi 2006, 32-33.)

Johdon vastuulla on, että tietoturvan taso vastaa hyväksyttyä tasoa ja samalla varmistaa, että tietoturvallisuudelle on annettu riittävät resurssit. Tietoturvapolitiikan luominen, katselmointi, hyväksyminen ja tietoturvasta tiedottaminen kuuluvat organisaation johdolle. Johdon tehtävänä on myös varmistaa, että koko organisaatiossa käytetään hyväksyttyjä tietoturvamekanismeja. (SFS ISO/IEC 17799:fi 2006, 32-33.)

Vastuu organisaation tietoturvan toteuttamisesta voi olla esimerkiksi erillisellä työryhmällä, hallituksella tai johtoryhmällä, riippuen organisaation koosta. Vastuu eri osa-alueiden tietoturvasta voidaan jakaa organisaatiossa kuitenkin pienempiin kokonaisuuksiin. Näille jokaiselle osa-alueille tulee nimittää oma vastuuhenkilö, joka vastaa kyseessä olevan osa-alueen tietoturvan toteutumisesta. Vastuut täytyy kuitenkin määritellä selkeästi ja tietoturvapolitiikan mukaisesti. (SFS ISO/IEC 17799:fi 2006, 32-35.)

Organisaatiossa on määriteltävä käytännöt, joita noudatetaan otettaessa yhteyttä viranomaisiin. Näistä käyvät ilmi milloin yhteydenottoa tarvitaan ja kenen toimesta yhteydenotto suoritetaan. Viranomaisina tässä tapauksessa tarkoitetaan esimerkiksi poliisia ja palolaitosta. (SFS ISO/IEC 17799:fi 2006, 32-35.)

5.3 Suojattavien kohteiden hallinta

Suojattavat kohteet voidaan jakaa ensisijaisiin suojattaviin kohteisiin ja ensisijaisia suojattavia kohteita tukeviin kohteisiin. Ensisijaisia suojattavia kohteita ovat

- Liiketoimintaprosessit ja liiketoiminnot
- Tieto.

Suojattavat liiketoimintaprosessit ja liiketoiminnot sisältävät prosesseja, joita organisaatio tarvitsee viranomaisvaatimusten, lakien ja sopimusten täyttämiseen. Lisäksi prosesseja, joihin liittyy tekijänoikeudella suojattua teknologiaa tai salaisia prosesseja. Sekä prosesseja, joiden muuttuminen vaikuttaa merkittävästi toiminta-ajatuksen muuttumiseen organisaatiossa. Sama koskee myös prosesseja, joiden vajaa toiminta tai menetys voisi johtaa organisaation toimimattomuuteen. (SFS ISO/IEC 27005 2009, 66-67.)

Suojattava tieto koostuu sellaisista henkilötiedoista, jotka määritellään yksityisyyttä suojaavien lakien perusteella. Lisäksi se koostuu välttämättömistä organisaation toiminta-ajatukseen ja liiketoiminnan toteutukseen liittyvistä tiedoista. Suojattava tieto koostuu myös strategisista tiedoista, jotka on määritetty strategisessa suunnittelussa tavoitteiden saavuttamiseksi. Lisäksi suojattavia tietoja ovat organisaatiolle kalliit tiedot, jotka määritellään hankintakustannuksien sekä tiedon siirtämiseen, käsittelyyn, säilytykseen ja keräämiseen kulutetun ajan perusteella. (SFS ISO/IEC 27005 2009, 66-67.)

Ensisijaisien suojattavien kohteiden lisäksi organisaatiossa tulee luetteloida ja tunnistaa ensisijaisia suojattavia kohteita tukevat suojattavat kohteet. Näihin suojattaviin kohteisiin liittyy haavoittuvuuksia joiden avulla voidaan pyrkiä vahingoittamaan ensisijaisia suojattavia kohteita. Ensisijaisia suojattavia kohteita tukevia suojattavia kohteita ovat

- Laitteistot
- Ohjelmistot
- Verkot
- Henkilöstö
- Toimipaikat
- Organisaatiorakenne.

(SFS ISO/IEC 27005 2009, 66-67.)

Laitteistot voidaan jakaa muun muassa siirrettäviin ja kiinteisiin laitteistoihin, tietojenkäsittelyn oheislaitteisiin ja erilaisiin tietovälineisiin esimerkiksi kannettava tietokone, palvelin, tulostin, muistitikku, asiakirja. (SFS ISO/IEC 27005 2009, 68-69.)

Ohjelmistot voidaan jakaa muun muassa käyttöjärjestelmiin, palvelu-, ylläpito-ohjelmistoihin, pakettiohjelmistoihin, liiketoimintasovelluksiin esimerkkinä tietokantahallintaohjelmisto ja kirjanpito-sovellus (SFS ISO/IEC 27005 2009, 70-71.)

Verkot koostuvat tietoliikennelaitteista, joiden avulla kytketään muun muassa toisiinsa tietojärjestelmän osia tai fyysisesti eri paikoissa sijaitsevia tietokoneita esimerkiksi ADSL -tekniikka, WLAN -tekniikka, reitittimet, keskittimet kuuluvat tähän ryhmään. (SFS ISO/IEC 27005 2009, 70-73.)

Suojattava henkilöstö koostuu tietojärjestelmän kanssa tekemisissä olevista ihmisryhmistä muun muassa päätöksentekijät, käyttäjät, ylläpito, kehittäjät

esimerkiksi projektipäällikkö, talousjohto, turvallisuuspäällikkö. (SFS ISO/IEC 27005 2009, 72-73.)

Organisaation sijaintiin liittyy monia alakohtia, joita täytyy ottaa huomioon. Toimipaikalla tarkoitetaan niitä paikkoja, joihin tietoturvallisuuden hallintajärjestelmä ulottuu sekä niitä fyysisiä välineitä, joita tarvitaan sen ylläpitämiseen. Organisaation sijainnissa ulkoisella ympäristöllä tarkoitetaan sellaisia paikkoja, joihin organisaatiossa määriteltyjä turvallisuusmenettelyjä ei voida soveltaa esimerkiksi työntekijöiden kodit. Toimitiloilla tarkoitetaan organisaation tiloja, jotka rajoittuvat organisaation ulkorajoihin ja ovat suoraan kosketuksissa ulkomaailman kanssa esimerkiksi rakennus, jossa organisaatio toimii. Vyöhykkeellä tarkoitetaan fyysisesti suojattuja rajoja, joilla organisaation toimitilat jaetaan osiin esimerkiksi toimistoihin. Peruspalveluihin kuuluvat esimerkiksi sähkönjakelu ja jäähdytys. (SFS ISO/IEC 27005 2009, 74-75.)

Organisaatioon kuuluvat kaikki tehtäviin nimetyt henkilöstöryhmät organisaatiossa, heillä on erilaisia tarkoituksia organisaatiossa. Valtuuttaja rajoittaa organisaation toimintaa määräysten, päätösten ja toimien avulla. Valtuuttaja voi olla juridinen osa organisaatiota tai ulkopuolinen taho esimerkiksi organisaation pääkonttori. Organisaation rakenne muodostuu eri haaroista ja niiden yhteisistä toiminnoista organisaation sisällä, jotka toimivat organisaation johdon ohjauksessa, esimerkiksi tietohallinto. Projekti- tai järjestelmäorganisaatio on tiettyä projektia tai palvelua varten perustettu osa organisaatiota, esimerkiksi tietojärjestelmän siirtymäprojekti. Lisäksi organisaatiossa voi olla alihankkijoita, toimittajia ja valmistajia, joiden tehtävä on tarjota palveluita ja resursseja erillisen sopimuksen mukaan organisaatiolle, esimerkiksi konsulttiyritys. (SFS ISO/IEC 27005 2009, 74-77.)

Suojattavista kohteista tulee tehdä luettelo, josta käy helposti ilmi kaikki tarvittava tieto kohteesta, esimerkiksi omistaja ja sijainti. Omistajan tehtävänä on huolehtia suojattavaan kohteeseen liittyvistä rajoituksista ja luokituksista. (SFS ISO/IEC 17799:fi 2006, 52-52.)

5.4 Henkilöstöturvallisuus

Henkilöstöturvallisuudella on merkittävä osuus organisaation tietoturvallisuudessa. Henkilöstöturvallisuudella pyritään varmistamaan henkilön sopivuus tehtäväänsä, velvollisuuksien ymmärtäminen ja kaikenlaisten väärinkäytösten, kuten varkauksien tai laittomuuksien vähentäminen. Erilaisilla turvallisuusselvityksillä voidaan kartoittaa henkilön taustoja, mikäli työtehtävät ovat arkaluontoisia. (SFS ISO/IEC 17799:fi 2006 56-59.)

Henkilöstöturvallisuutta harjoitetaan ja noudatetaan koko työsuhteen ajan organisaatiossa. Työntekijän valintavaiheessa on syytä kiinnittää huomiota hakijan sopivuuteen työtehtävässä. Yleisesti työsopimuksen yhteydessä käydään läpi yrityksen turvallisuuteen liittyvät seikat ja lisäksi käytetään sopimuksia, jonka allekirjoittamalla työntekijät hyväksyvät yrityksen vaatiman turvallisuustason. Sopimuksen rikkomisesta aiheutuvat seuraukset ovat aina tapauskohtaisia. (SFS ISO/IEC 17799:fi 2006, 58-59.)

Työsuhteen aikana on hyvä käydä säännöllisin väliajoin läpi osapuolten velvollisuuksia tietoturvan suhteen. Tämä sisältää muun muassa tietoturvaan kohdistuvia uhkien läpikäyntiä ja vahinkovastuuta mahdollisissa vahinkotapauksissa. Säännölliset koulutukset ja perehdytykset ovat hyvä tapa muistuttaa tietoturvan tärkeydestä organisaation sisällä. (SFS ISO/IEC 17799:fi 2006, 62-63.)

Työsuhteen päättymiseen on hyvä luoda myös omat tietoturvamäärittelyt, näin varmistetaan, että organisaatiosta lähtevä taho jättää organisaation suunnitellulla ja järjestelmällisellä tavalla. Tämä koskee käyttöoikeuksien poistamista ja laitteistojen palauttamista organisaatiolle takaisin. Samanlaista organisoitua tapaa on hyvä käyttää myös työsuhteen muuttuessa. (SFS ISO/IEC 17799:fi 2006, 64-65.)

5.5 Fyysinen turvallisuus

Fyysisellä turvallisuudella pyritään estämään organisaation toimitiloihin ja tietoaineistoon kohdistuva luvaton pääsy. Näin varmistetaan toiminnan jatkuminen organisaatiossa häiriöittä sekä toimitilojen turvaaminen vahingoilta. (SFS ISO/IEC 17799:fi 2006, 68-69.)

Fyysistä turvallisuutta voidaan toteuttaa kulunvalvonnalla esimerkiksi kulkukorteilla, joiden avulla voidaan liikkua organisaation tiloissa ovista ja hisseistä. Kulkukorttien avulla pyritään luomaan turva-alueita, joiden sisällä olevaan tietoon pääsyä pyritään valvomaan. Turva-alueen tulee olla selkeästi rajattu ja sinne pääsyyn liittyvät kriteerit tulee luoda suojattavan kohteen pohjalta. Vain valtuutetuilla henkilöillä, joilla on perusteltu tarve liikkua turva-alueella, tulee olla pääsyoikeus alueelle. Mahdollisille vierailijoille, jotka tarvitsevat pääsyn turva-alueen sisälle luodaan vierailijakäytäntö, johon voi kuulua esimerkiksi vierailijakortit, jotka on pidettävä esillä koko vierailun ajan. (SFS ISO/IEC 17799:fi 2006, 68-71.)

Luvaton käyttö ei ole ainoa fyysinen tietoturvauhka, joka organisaatiota uhkaa. Toisenlaisen uhan muodostavat muun muassa tulipalot, räjähdykset ja terrorismi. Nämä huomioidaan suunniteltaessa ulkoisilta uhilta suojautumista organisaatiossa. Erilaisia turvamekanismeja ovat muun muassa palokuorman vähentäminen organisaation tiloista, jolloin esimerkiksi ylimääräiset pahvilaatikot tulisi poistaa tiloista. Organisaation varalaitteet ja varmuuskopiot tulee sijoittaa toisaalle tarpeeksi kauas organisaation virallisesta käytössä olevasta toimipisteestä. Mahdollisen vahingon sattuessa varalaitteet ja varmuuskopiot eivät vahingoitu samalla ja organisaatio voi jatkaa toimintaansa pienen keskeytyksen jälkeen toisaalla. (SFS ISO/IEC 17799:fi 2006, 70-71.)

5.6 Laitteiden turvallisuus

Laitteiden tietoturvallisuuden tarkoituksena on estää niiden vahingoittuminen, varastaminen tai häviäminen, jonka seurauksena organisaation kannalta tärkeät toiminnot keskeytyisivät. (SFS ISO/IEC 17799:fi 2006, 74-75.)

Laitteiden tietoturvallisuutta suunniteltaessa on syytä ottaa huomioon niiden sijoittaminen ja suojaaminen organisaation tiloissa. Esimerkiksi erilliseen huoneeseen sijoitettavat palvelimet, reitittimet ja kytkimet ovat järkevämpi ratkaisu, kuin niiden hajanainen sijoittaminen ympäri toimitiloja. Näin pyritään minimoimaan luvaton fyysinen pääsy laitteisiin. (SFS ISO/IEC 17799:fi 2006, 74-75.)

Laitteita ulkoa uhkaavia toimia ovat myös esimerkiksi syöminen ja juominen laitteiden läheisyydessä. Tästä on hyvä tehdä oma linjaus organisaation sisällä. Näin pyritään minimoimaan laitteille mahdollisesti aiheutuvia vahinkoja. (SFS ISO/IEC 17799:fi 2006, 74-75.)

Laitteisiin tehtävät kytkennät on syytä dokumentoida organisaatiossa, jolloin minimoidaan kytkentämuutoksista aiheutuvia haittoja organisaation sisällä. Kytkentäkaapelit tulee merkitä selkeästi, jotta mahdollisilta väärinkäsityksiltä vältytään kytkentöjä ja muutoksia tehdessä. Lisäksi laitteistojen sähkönsyöttöön tulee kiinnittää huomiota. Varotoimina voidaan pitää ukkossuojattuja ja akkuvarmistettuja pistorasioita, joilla pyritään minimoimaan vaihtelut sähkönsyötössä esimerkiksi ukkosten ja sähkökatkojen aikana organisaatiolle kriittisten laitteiden kanssa. (SFS ISO/IEC 17799:fi 2006, 76-77.)

Organisaation laitteiden turvallisuus on otettava myös huomioon tilanteissa, joissa laitteet viedään organisaation tilojen ulkopuolelle. Laitteiden vieminen organisaation tilojen ulkopuolelle tulee olla luvanvaraista ja laitteiden liikkuminen toimitiloista sisään ja ulos tulee kirjata ylös. Laitteita ei tule jättää julkisille

paikoille vartioimatta. Tämä koskee myös dokumentteja, jotka sisältävät organisaation kannalta arkaluonteista informaatiota. (SFS ISO/IEC 17799:fi 2006, 78-81.)
Uusien laitteiden käyttöönottoon tulee luoda organisaation sisällä omat käytännöt esimerkiksi kuinka varmistetaan, että laite täyttää organisaation tietoturvavaatimukset. Lisäksi täytyy varmistaa, että organisaatiolla on käytettävissä asiantuntijoita laitteita varten, jotta mahdollisista ongelmatapauksista selvitään.

Myös vanhojen laitteiden käytöstä poistamiseen tulee luoda omat käytännöt. On varmistuttava, että organisaatiota koskevaa materiaalia ei joudu ulkopuolisten tahojen haltuun esimerkiksi tietokoneita ja matkapuhelimia poistettaessa organisaation käytöstä. Tallennusvälineet voidaan tuhota fyysisesti, mikäli tämä koetaan tarpeelliseksi organisaation etujen kannalta. (SFS ISO/IEC 17799:fi 2006, 78-79.)

5.7 Tietojärjestelmät

Tänä päivänä suuria määriä tietoa tuotetaan tietokoneilla ja sen tallennus tapahtuu esimerkiksi tietokoneen omalle kovalevylle, käytössä oleville servereille tai muistitikuille. Tiedon käsittelyä varten on syytä luoda omat ohjeistukset, jonka avulla tietoturvaa pystytään parantamaan esimerkiksi varmuuskopioinnin ohjeistamisen ja olemassa olevien dokumenttien muokkaamisen osalta. (SFS ISO/IEC 17799:fi 2006, 80-81.)

Työntekijöillä tulee olla henkilökohtaiset tunnukset järjestelmiin, jolloin käytönvalvontaa voidaan suorittaa tarkemmin, yksilöidysti. Näin voidaan havaita mahdolliset väärinkäytökset tietojärjestelmissä helposti ja rajata yksittäiset uhkatekijät pois järjestelmistä. Työntekijöillä tulee organisaation sisällä olla oikeudet vain sellaisiin järjestelmiin, joihin heillä on perusteltua päästä sisään. Näin pyritään ennalta ehkäisemään tietojärjestelmien väärinkäytöksiä esimer-

kiksi tahallisen tai tahattoman muokkaamisen muodossa. (SFS ISO/IEC 17799:fi 2006, 82-83.)

Käyttöoikeuksien hallinta on tärkeää koko käyttäjätunnusten voimassaoloajan, aina tunnusten luontivaiheesta palveluun tai järjestelmään ja siitä tunnusten poistoon asti. Mikäli käyttäjä siirtyy toisiin tehtäviin tai ei muuten enää tarvitse oikeuksia järjestelmään, tunnukset tulee poistaa. Näin pyritään minimoimaan palveluiden ja järjestelmien väärinkäyttötilanteet. Hyvä käytäntö tunnusten hallinnassa on tunnusten vanheneminen määräajoin, jolloin käyttäjän on uusittava tunnuksensa, jolloin voidaan tarkistaa, mikäli kyseessä oleva käyttäjä tarvitsee vielä oikeudet kyseessä olevaan palveluun tai järjestelmään. (SFS ISO/IEC 17799:fi 2006, 124-125.)

Käyttäjien salasanakäytännöt tulee määrittää organisaation sisällä. Käyttäjälle luotaessa tunnukset palveluun, oletussalasana tulee vaihtaa käyttäjän toimesta ensimmäisenä. Lisäksi salasanalle tulee tehdä vaatimusmäärittely, joka sisältää esimerkiksi:

- Salasanan pituuden
- Erikoismerkkien käytön
- Isojen ja pienten kirjainten käytön
- Kirjainten ja numeroiden käytön.

(SFS ISO/IEC 17799:fi 2006 126-127, 130-131.)

Käyttäjäoikeudet järjestelmiin tulee olla käyttäjäkohtaisia eikä omaa salasanaa tule luovuttaa missään tilanteissa muille käyttäjille. On olemassa erityisiä tilanteita, jossa voidaan käyttää niin sanottuja yhteiskäyttötunnuksia. Näillä tunnuksilla tietty ryhmä voi käyttää yhteistä tunnusta ja salasanaa kirjautuessaan järjestelmään tai palveluun. Salasanojen tallentamisesta tulee luoda omat käytänteet organisaation sisällä. (SFS ISO/IEC 17799:fi 2006, 130-131.)

6 TAPAHTUMIEN VALVONTA

6.1 Yleistä

Järjestelmän ylläpitäjillä tulee olla tieto organisaation verkon tilasta. Verkossa tapahtuvat tietoturvatapahtumat tulee kirjata ylös ja käynnistää vaaditut toimenpiteet mahdollisten rikkomuksien sattuessa. Valvonnassa tulee kuitenkin noudattaa voimassa olevia kansallisia ja kansainvälisiä lakeja. Henkilöstöllä voi olla erilaisia oikeuksia eri järjestelmiin, nämä oikeudet määrittyvät työtehtävien mukaa. Esimerkiksi tilanteessa jossa käyttäjä pääsee käsiksi sellaiseen tietoon, johon hänellä ei olisi oikeutta, tästä syntyy tietoturvatapahtuma. (SFS ISO/IEC 17799:fi 2006, 114-115.)

Tapahtumien valvontana voidaan pitää myös kulkuoikeuksien käytön tarkkailua. Kun ovista kuljetaan organisaation tiloissa, tulee tästä jäädä merkintä tietokantaan. Näin voidaan valvoa henkilöstön liikkeitä ja mahdollisten tietoturvatapahtumien sattuessa nähdään kuka tilassa on käynyt.

6.2 Lokit

Jotta organisaation tietoverkossa tapahtuvia tapahtumia pystytään valvomaan järjestelmällisesti, täytyy organisaatiossa ylläpitää tapahtumalokeja. Lokien käytettävyys paranee, mikäli ne sisältävät ainakin:

- Käyttäjätunnuksen
- Päivämäärän ja kellonajan
- Työaseman tunnuksen
- Havaitun tapahtuman.

(SFS ISO/IEC 17799:fi 2006, 114-115.)

Lokeista tulee ilmetä tapahtuma, jonka käyttäjä on suorittanut esimerkiksi:

- Kirjautumisyritys
- Järjestelmämuutos
- Järjestelmän suojauksien muuttaminen (esimerkiksi virustorjunta).

(SFS ISO/IEC 17799:fi 2006, 114-117.)

Lokeja ylläpidettäessä täytyy varmistua, että lokeja ei päästä muokkaamaan tai tuhoamaan minkään osapuolen toimesta. Riittävän tallennuskapasiteetin varmistaminen on tärkeää, etteivät tapahtumat jää merkitsemättä tai katoa järjestelmästä. (SFS ISO/IEC 17799:fi 2006, 116-119.)

Tapahtumalokit ovat järjestelmän ylläpitämisen kannalta tärkeitä, koska niihin tallentuvat myös verkossa tapahtuvat muutokset. Lokitiedoista pystytään havaitsemaan, mikäli jonkin muutoksen jälkeen verkon toimintakyky on laskenut merkittävästi. Esimerkiksi jos jokin palvelu on muutoksen jälkeen saavuttamattomissa. Järjestelmän ylläpitäjät voivat lokitietojen perusteella aloittaa vianrajauksen palvelun saattamiseksi takaisin toimintaan. Toimenpide on huomattavasti helpompi, kun voidaan määrittää vian alkuajan ja muutoksen ajankohta yhteneväiseksi ja näin rajata vikaa.

6.3 Synkronointi

Lokitiedoista on pystyttävä määrittelemään tapahtuma ajankohdat, joten synkronointi on tärkeä tehdä järjestelmälle. Synkronointi tulee suorittaa samasta lähteestä kaikille verkon laitteille. Ongelmatilanteiden ratkaisua helpottaa, mikäli kaikki laitteet ovat yhtenäisesti synkronoitu ja käyvät samassa ajassa. Kellojen synkronoinnissa tulee ottaa huomioon paikalliset aikaan liittyvät tekijät, aikavyöhykkeet ja kesä- ja talviaika. Synkronoinnin avulla voidaan varmistua aikatietojen paikkaansa pitävyydestä.
(SFS ISO/IEC 17799:fi 2006, 120-121.)

6.4 Toiminnan rajoittaminen

Verkossa tapahtuvaa liikennettä voidaan rajoittaa erilaisilla suodattimilla, joita asennetaan käytöstä riippuen joko suoraan käyttäjän omalle tietokoneelle tai organisaation verkon laitteisiin. Liikenteen rajoitus voi olla ohjelmallisesti tai erillisellä fyysisellä laitteella toteutettu. Tällaisella liikenteen rajoituksella pyritään suojaamaan organisaation kannalta tärkeiden palvelujen toimiminen. Verkon jakaminen loogisesti auttaa rajoituksien asettamisessa. Verkko voidaan jakaa loogisesti sisä- ja ulkoverkkoon, jolloin erotetaan organisaation sisällä olevia verkkoja ulkopuolisista verkoista. Rajoituksen kohteena voi olla esimerkiksi:

- Sähköpostiliikenne
- Tiedonsiirto
- Sovellus.

(SFS ISO/IEC 17799:fi 2006, 138-139.)

Verkossa tapahtuvaa tiedonsiirtoa voidaan myös rajoittaa eri viikonpäivinä ja kellonaikoina. Rajoitussääntöjen rikkomukset tulee kirjata lokiin, josta ne ovat järjestelmän ylläpidon nähtävillä. (SFS ISO/IEC 17799:fi 2006, 138-139.)

Rajoitteita laadittaessa on otettava huomioon, että liian tiukat rajoitteet voivat estää organisaation toiminnan kannalta tärkeän liikenteen. Halutut rajoitteet tulee testata huolellisesti testiympäristössä, jossa voidaan simuloida tilanteita, joissa tietty liikenne halutaan estää tai sallia.
(SFS ISO/IEC 17799:fi 2006, 138-139.)

Myös kulunvalvontaan voidaan soveltaa toiminnan rajoittamista. Mikäli työntekijällä ei ole tarvetta liikkua tilassa, ei hänelle myönnetä kulkuoikeutta tilaan. Näin pyritään minimoimaan organisaatiossa tapahtuvia väärinkäytöksiä.

7 JATKUVUUDEN HALLINTA

Odottamattomia, organisaation liiketoiminnan jatkuvuuteen vaikuttavia muutoksia voi tapahtua kaikista suunnitelmista huolimatta. Tämänlaisia tapahtumia voivat olla esimerkiksi:

- Tulipalo
- Vesivahinko
- Räjähdys
- Luonnonkatastrofi
- Laitevika.

(SFS ISO/IEC 17799:fi 2006, 184-185.)

Näistä tapahtumista toipumista varten organisaation sisällä täytyy luoda jatkuvuuden hallintasuunnitelma myös tietoturvan kannalta. Suunnitelmassa käydään läpi mahdollisia liiketoiminnan jatkuvuuteen vaikuttavia tekijöitä sekä turvamekanismeja, joilla pyritään pienentämään liiketoiminnalle aiheutunut haitta. Organisaation sisäisesti listataan tunnistetut uhat. Uhkien avulla määritellään niistä aiheutuvan liiketoiminnan keskeytyksen todennäköisyys ja vaikutus organisaatiossa liittyen katkoksen kestoon, tuhon laajuuteen ja palautumisaikaan. (SFS ISO/IEC 17799:fi 2006, 184-187.)

Jatkuvuuden hallintasuunnitelmaa tulee ylläpitää, testata ja kehittää jatkuvasti, kun saadaan uutta tietoa organisaatiota uhkaavista tekijöistä. (SFS ISO/IEC 17799:fi 2006, 186-187, 190-191.)

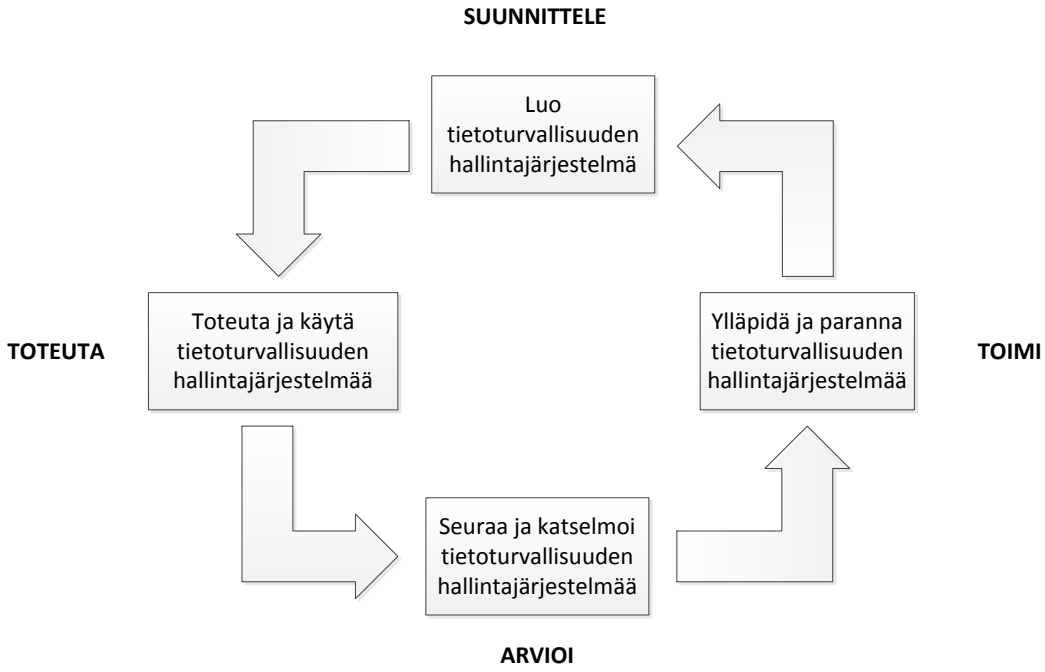
Tässä opinnäytetyössä jatkuvuuden hallintaa sovellettiin tietoturvan kehittämissuunnitelmaan. Suojattavat kohteet listattiin. Suojattaville kohteille kartoitettiin uhkia. Mikäli uhista muodostuvat riskit muodostuivat liian suuriksi, kehitettiin niille turvamekanismit. Jatkossa riskejä arvioidaan määräajoin ja mikäli

niissä havaitaan muutoksia, suoritetaan tarvittavat toimenpiteet riskikohtaisesti.

8 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

”Organisaation tulee luoda, toteuttaa, käyttää, valvoa, katselmoida, ylläpitää ja jatkuvasti kehittää dokumentoitua tietoturvallisuuden hallintajärjestelmää, joka tukee organisaation liiketoimintoja ja organisaatioon kohdistuvia riskejä.” (SFS ISO/IEC 27001:fi 2006, 14-15.)

Kuviossa 3 on havainnollistettu tietoturvallisuuden hallintajärjestelmän jatkuvan kehittämisen prosessi. Mallia kutsutaan myös PDCA-malliksi, joka tulee englannin kielen sanoista plan, do, check, act.



KUVIO 3. PDCA-malli

(SFS ISO/IEC 27001:fi 2006, 8.)

8.1 Luominen

Tietoturvallisuuden hallintajärjestelmää ja hallintapolitiikkaa luotaessa on määriteltävä niiden kattavuus ja rajat. Tähän vaikuttavia tekijöitä ovat esimerkiksi:

- Organisaation sijainti
- Liiketoiminta
- Suojattavat kohteet.

(SFS ISO/IEC 27001:fi 2006, 14-15.)

Tietoturvallisuuden hallintapolitiikan avulla luodaan suunta ja periaatteet tietoturvatoimenpiteille. Hallintapolitiikassa otetaan myös huomioon liiketoiminnan, lakien ja hallinnon asettamat vaatimukset sekä sopimuksien tuomat tietoturvavelvoitteet. Hallintapolitiikalla luodaan kriteerit, joiden avulla riskit arvioidaan. Lisäksi organisaation johdon täytyy hyväksyä tietoturvallisuuden hallintapolitiikka. (SFS ISO/IEC 27001:fi 2006, 14-15.)

Organisaation tulee määritellä itselleen sopiva riskien arviointitapa. Tätä arviointitapaa käyttäen organisaatio määrittää hyväksyttävät riskitasot ja riskien hyväksymiskriteerit. Valitun riskien arviointitavan avulla täytyy pystyä luomaan vertailukelpoisia ja toistettavia tuloksia. (SFS ISO/IEC 27001:fi 2006, 14-17.)

Tietoturvallisuuden hallintajärjestelmää luotaessa organisaatiossa tulee suorittaa seuraavat toimenpiteet:

- Riskien tunnistus
- Riskien vaikutusten analysointi ja arviointi
- Riskien käsittelyn vaihtoehtojen tunnistus ja arviointi
- Valvontatavoitteiden ja turvamekanismien valinta riskien käsittelyyn
- ”Hankkia johdon hyväksyntä jäännösriskeille”
- ”Hankkia johdon valtuutus tietoturvallisuuden hallintajärjestelmän käyttöönotolle ja käytölle”

- Valmistella soveltamissuunnitelma.

(SFS ISO/IEC 27001:fi 2006, 16-19.)

8.2 Toteutus

Organisaatiossa tulee määritellä ja ottaa käyttöön riskien käsittelysuunnitelma, jonka avulla tunnistetaan vastuut, toimenpiteet, resurssit, prioriteetit, kustannukset ja osoitetaan roolit tietoturvariskien hallinnassa. Tietoturvallisuuden hallintajärjestelmään liittyvät tärkeänä osana tietoturvamekanismit. Käytössä olevia turvamekanismeja on pystyttävä valvomaan ja mittaamaan tehokkaasti. Valvontaa varten on luotava mittarit, joiden avulla tutkitaan tietoturvaan liittyviä muutoksia. Lisäksi havaitut puutteet on raportoitava ja dokumentoitava välittömästi niiden havainnointi hetkellä ja niihin tulee puuttua mahdollisimman nopeasti. (SFS ISO/IEC 27001:fi 2006, 18-19.)

Jotta tietoturvallisuus toimisi organisaatiossa sen haluamalla tavalla, tulee organisaation sisällä suorittaa koulutus- ja tiedotusohjelmia, joiden avulla työntekijät saavat tarvittavia tietoja organisaation tietoturvasta. Tämä kuuluu osaksi tietoturvallisuuden hallintajärjestelmää. (SFS ISO/IEC 27001:fi 2006, 18-19.)

8.3 Johtaminen

Tietoturvallisuuden hallintajärjestelmää on valvottava ja katselmoitava asianmukaisesti. Valvonnan ja katselmoinnin avulla havaitaan tietoturvarikkomukset ja niiden yritykset organisaatiossa. Lisäksi pystytään myös tiedottamaan johdolle siitä, kuinka hyvin eri henkilöt suoriutuvat heille annetuista tehtävistä tietoturvan kannalta ja kuinka teknisesti toteutetut turvamenetelmät toimivat. Valvonnan ja katselmoinnin avulla voidaan myös määritellä kuinka tehokkaita turvallisuusrikkomusten käsittelytoimenpiteet ovat. (SFS ISO/IEC 27001:fi 2006, 18-19.)

Tietoturvallisuuden hallintajärjestelmän tehokkuutta täytyy säännöllisesti katselmoida. Katselmoinnissa on käytävä läpi tietoturvapolitiikka sen asettamien tavoitteiden noudattaminen sekä turvamekanismit. Tietoturvan hallintajärjestelmän katselmoinnissa käydään läpi tietoturva-auditointien tulokset, tietoturvahäiriöt, sidosryhmien ehdotukset ja palautteet sekä tehokkuusmittausten tulokset. (SFS ISO/IEC 27001:fi 2006, 18-19.)

Organisaatiossa tulee katselmoida riskien arviointi säännöllisin väliajoin myös jäännösriskien ja hyväksyttävien riskien tasot tulee katselmoida huomioiden muutokset:

- ”Organisaatiossa
- Teknologiassa
- Liiketoiminnan tavoitteissa ja liiketoimintaprosesseissa
- Tunnistetuissa uhkissa
- Käytössä olevien turvamekanismien tehokkuudessa
- Ulkopuolisissa tapahtumissa kuten muutokset lainsäädännössä tai hallinnollisessa ympäristössä, sopimusvelvoitteissa taikka yhteiskunnallisissa asenteissa”.

(SFS ISO/IEC 27001:fi 2006, 20-21.)

Tietoturvallisuuden hallintajärjestelmälle tulee suorittaa säännöllisesti sisäisiä auditointeja. Nämä auditoinnit organisaatio voi tehdä itse tai teettää ulkopuolisella taholla omaan sisäiseen käyttöönsä. Säännöllisen tietoturvallisuuden hallintajärjestelmän johdon katselmuksella pyritään varmistamaan järjestelmän riittävä kattavuus. Sekä varmistetaan jatkuvan parantamisen kohteiden tunnistaminen tietoturvaprosessissa. Turvallisuussuunnitelmaa tulee päivittää jatkuvasti huomioiden tarkkailu- ja katselmustoiminnoissa tehdyt havainnot. Lisäksi tulee kirjata ylös toimenpiteet ja tapahtumat, joilla voi mahdollisesti olla vaikutusta tietoturvan hallintajärjestelmän suorituskykyyn tai vaikuttavuuteen. (SFS ISO/IEC 27001:fi 2006, 20-21.)

Organisaation tietoturvallisuuden hallintajärjestelmän ylläpitoa ja parantamista varten täytyy seuraavia toimenpiteitä suorittaa

- Suorittaa tunnistetut parannustoimenpiteet
- Soveltaa ehkäiseviä ja korjaavia toimenpiteitä
- Soveltaa omia sekä muiden organisaatioiden oppimia tietoturvakokemuksia
- Tiedottaa sidosryhmille toimenpiteistä ja parannuksista
- Varmistaa parannusten johtaneen haluttuihin tavoitteisiin.

(SFS ISO/IEC 27001:fi 2006, 20-21.)

8.4 Dokumentointi

Dokumentoinnin avulla voidaan jäljittää organisaatiossa tehdyt päätökset tietoturvallisuuden hallintajärjestelmästä. Sen avulla voidaan osoittaa valittujen turvamekanismien perustuvan riskien arviointi- ja käsittelyprosessin tuloksiin ja tietoturvallisuuden hallintapolitiikkaan ja sen tavoitteisiin. Dokumentaation tulee sisältää

- ”Tietoturvapolitiikka ja valvontakohteet kirjallisena dokumenttina
- Tietoturvallisuuden hallintajärjestelmän kattavuus
- Tietoturvallisuuden hallintajärjestelmää tukevat menettelytavat ja turvamekanismit
- Riskien arvioinnin menettelytavan kuvaus
- Raportti riskien arvioinnista
- Riskien hallintaa koskeva suunnitelma
- Dokumentoidut menettelyt, joita organisaatio tarvitsee varmistamaan tietoturvaprosessiensa suunnittelu, käytön ja valvonnan ja kuvaamaan turvamekanismien tehokkuuden mittaustapa
- Soveltamissuunnitelma”

- Tallenteet, esimerkiksi vieraskirja tai tarkastuspöytäkirja tai käyttöoikeuksien myöntämislomake.

(SFS ISO/IEC 27001:fi 2006, 20-23.)

Tietoturvallisuuden hallintajärjestelmässä käytettäviä asiakirjoja täytyy suojella ja ohjata. Näitä toimenpiteitä varten täytyy laatia menettelyohje, jossa otetaan kantaa esimerkiksi:

- Asiakirjojen jakeluun
- Asiakirjojen päivitykseen
- Asiakirjojen käytettävyyteen
- Asiakirjojen alkuperän tunnistukseen.

(SFS ISO/IEC 27001:fi 2006, 22-23.)

8.5 Johdon vastuu

Organisaation johdon merkitys tietoturvallisuuden noudattamiseen organisaation sisällä on suuri. Tietoturvallisuuden hallintajärjestelmää tukevat toimenpiteet saavat alkunsa organisaation johdolta. Organisaation johdon tulee sitoutua tietoturvallisuuden hallintajärjestelmään sen koko elinkaaren ajan. Tietoturvallisuuden hallintajärjestelmää luotaessa johdon tulee määrittää tietoturvapolitiikka sekä varmistaa, että tietoturvatavoitteet asetetaan ja suunnitelmat laaditaan asiaan kuuluvasti. Käyttöönotossa johdon tulee määritellä roolit ja vastuut tietoturvallisuuteen liittyen. Johdon tulee viestiä tietoturvatavoitteiden ja tietoturvapolitiikan noudattamisesta organisaation sisällä. Johdon tulee varata tarvittavat resurssit, jotta tietoturvallisuuden hallintajärjestelmää pystytään kehittämään, toteuttamaan, käyttämään ja ylläpitämään. Johdon vastuulla on päättää riskien hyväksymiskriteerit sekä hyväksyttävät riskitasot. Organisaation johdon tulee myös varmistaa, että tietoturvallisuuden hallintajärjestelmään suoritetaan sisäiset auditoinnit ja johdon katselmukset. (SFS ISO/IEC 27001:fi 2006, 24-25; SFS ISO/IEC 27003, 62-63)

Organisaation johdon tulee määritellä ja varata tarvittavat resurssit tietoturvallisuuden hallintajärjestelmälle. Lisäksi tulee varmistua siitä, että tietoturvaprosessit tukevat organisaation liiketoimintaa. Johdon tulee ottaa huomioon lakien ja hallinnollisten vaatimuksien ja sopimusten tuomat turvallisuusvelvoitteet. Soveltamalla käytössä olevia turvamekanismeja varmistaa riittävä turvallisuustaso. Johdon tulee suorittaa katselmuksia ja toimittava niistä saatujen tuloksien mukaisesti. Parantaa tietoturvallisuuden hallintajärjestelmän vaikuttavuutta, mikäli tarvetta esiintyy. (SFS ISO/IEC 27001:fi 2006, 24-25.)

Organisaation johdon tulee varmistaa, että tietoturvallisuuden hallintajärjestelmässä vastuuta saaneilla henkilöillä on riittävä pätevyys tehtävien suorittamiseen. Organisaation tulee tarjota asianmukaista koulutusta henkilöille ja tarvittaessa palkata pätevää henkilöstöä täyttämään tietoturvallisuuden hallintajärjestelmän asettamat tavoitteet. Lisäksi vastuussa olevien henkilöiden täytyy tiedostaa tietoturvatehtäviensä merkitys ja tärkeys tietoturvallisuuden hallintajärjestelmän tavoitteiden savuttamisessa. Organisaatiossa täytyy ylläpitää dokumenttia, jossa on tiedot henkilöiden pätevyyksistä, kokemuksista, koulutuksista ja taidoista. (SFS ISO/IEC 27001:fi 2006, 24-25.)

8.6 Auditointi

Organisaatiossa tulee suorittaa sisäisiä auditointeja tietoturvallisuuden hallintajärjestelmään säännöllisin väliajoin, jotta voidaan varmistua hallintajärjestelmän valvontatavoitteiden, turvamekanismien, prosessien ja menettelytapojen olevan

- Standardin ISO/IEC 27001:fi ja lainsäädännön asettamien vaatimuksien mukaiset
- ”Tunnistettujen tietoturvavaatimusten mukaiset
- Vaikuttavasti toteutettuja ja ylläpidettyjä
- Toiminnassa odotusten mukaisesti”.

(SFS ISO/IEC 27001:fi 2006, 26-27.)

Auditointiohjelman suunnittelussa tulee ottaa huomioon aikaisempien auditointien tulokset, auditoitavien prosessien ja alueiden tila ja tärkeys. Auditoinneille tulee määrittää kriteerit, laajuus, suoritustaajuus sekä menettelyt. Auditoijat tulee valita siten, että omia töitä ei auditoida, jotta varmistutaan auditointiprosessin tasapuolisuudesta. (Kansallinen turvallisuusauditointikriteeristö versio II. 2010; SFS ISO/IEC 27001:fi 2006, 26-27.)

Auditointia varten tulee luoda oma dokumentoitu menettelyohje, jossa määritellään vastuut ja vaatimukset auditointien suunnitteluun, suoritukseen, tulosten raportointiin ja tallenteiden ylläpitoon. Mikäli auditoitaessa havaitaan puutteita, on auditoidun alueen johdon vastuulla suorittaa toimenpiteet puutteiden korjaamiseksi ilman aiheetonta viivettä. Kaikki suoritetut toimenpiteet tulee raportoida. (SFS ISO/IEC 27001:fi 2006, 26-27.)

8.7 Johdon katselmointi

Organisaation tietoturvallisuuden hallintajärjestelmää tulee katselmoida johdon toimesta säännöllisin väliajoin, kuitenkin vähintään kerran vuodessa. Katselmoinnilla varmistetaan hallintajärjestelmän jatkuva soveltuvuus, asianmukaisuus ja vaikuttavuus organisaatiossa. Katselmuksen tulee kattaa tietoturvallisuuden hallintajärjestelmän arviointi sisältäen tietoturvapolitiikan ja tietoturvatavoitteet, muutostarpeet ja parannusmahdollisuudet. Katselmuksesta saadut tulokset tulee dokumentoida sekä tallenteet ylläpitää. (SFS ISO/IEC 27001:fi 2006, 26-27.)

Johdon katselmuksessa käytettäviä lähtötietoja ovat esimerkiksi:

- Aiempien auditointien ja katselmusten tulokset
- Sidosryhmien palautteet

- Listat korjaavista ja ehkäisevistä toimenpiteistä
- Muutokset, jotka saattavat vaikuttaa tietoturvallisuuden hallintajärjestelmään.

(SFS ISO/IEC 27001:fi 2006, 26-27.)

Johdon katselmuksen tuloksiin sisältyvät päätökset ja toimenpiteet esimerkiksi:

- Hallintajärjestelmän vaikuttavuuden parantamiseen
- Resurssitarpeet
- Sisäisten tai ulkoisten tarpeiden aiheuttamat muutokset hallintajärjestelmään, esimerkiksi lakien tai sopimusten muutokset.

(SFS ISO/IEC 27001:fi 2006, 28-29.)

8.8 Hallintajärjestelmän parantaminen

Tietoturvallisuuden hallintajärjestelmän vaikuttavuutta tulee parantaa jatkuvasti. Parannuksia tulee tehdä käyttäen hyväksi:

- Tietoturvapolitiikkaa
- Tietoturvatavoitteita
- Auditoinneista saatuja tuloksia
- Valvottujen tapahtumien analysointia
- Korvaavia ja ehkäiseviä toimenpiteitä
- Johdon katselmuksia.

(SFS ISO/IEC 27001:fi 2006, 28-29.)

Mikäli organisaatiossa havaitaan poikkeamia tietoturvallisuuden hallintajärjestelmän asettamista vaatimuksista, tulee organisaatiossa suorittaa korjaavia toimenpiteitä. Korjaavia toimenpiteitä varten tulee luoda dokumentoitu menettelyohje, jossa määritellään vaatimukset:

- Poikkeamien tunnistamiseen
- Poikkeamien syiden selvitykseen
- Toimenpiteisiin, jotta poikkeama ei enää toistuisi
- ”Korjaavien toimenpiteiden määrittäminen ja toteuttaminen”
- Toimenpiteiden tulosten tallentamiseen
- Korjaavien toimenpiteiden katselmointiin.

(SFS ISO/IEC 27001:fi 2006, 28-29.)

Organisaatiossa tulee suorittaa myös ehkäiseviä toimenpiteitä, joilla mahdollisia tietoturvallisuuden hallintajärjestelmän poikkeamia pyritään estämään. Riskien arvioinnin tulosten perusteella määritellään ehkäisevien toimenpiteiden tärkeysjärjestys. Ehkäiseviä toimenpiteitä varten tulee myös luoda dokumentoitu menettelyohje, jossa määritellään vaatimukset:

- Mahdollisten poikkeamien ja niiden syiden tunnistamiseen
- Arvio toimenpiteiden tarpeista, joilla poikkeaman esiintyminen estetään
- Tarvittavien ehkäisevien toimenpiteiden määrittämiseen ja toteuttamiseen
- Suoritettujen toimenpiteiden tulosten tallettamiseen
- Suoritettujen ehkäisevien toimenpiteiden katselmoinnista.

(SFS ISO/IEC 27001:fi 2006, 30-31.)

9 KÄYTÄNNÖN TOTEUTUS

Standardien läpi käymisen jälkeen oli vuorossa varsinainen käytännön tietoturvan toteutus JYVSECTEC -hankkeelle. Alkuperäisen opinnäytetyön aiheen laajuudesta ja hankkeen resurssien puutteesta johtuen jouduttiin aihetta rajaamaan. Lopullinen opinnäytetyö rajattiin koskemaan vain JYVSECTEC -hankkeen tiloissa tapahtuvan laitteiston ja ohjelmiston teknisen testauksen tietoturvallisuuden hallintajärjestelmää. Hankkeella ei ollut aikaisemmin luotua

tietoturvallisuuden hallintajärjestelmää, joten tämän opinnäytetyön pohjalta alettiin rakentaa tietoturvaa hankkeeseen testauksen osalta. Jatkossa tietoturvan kehitys hankkeessa tapahtuu tämän opinnäytetyön tuloksina saatujen asiakirjojen ja dokumenttien pohjalta.

Käytännön toteutus aloitettiin kartoittamalla hankkeelle tärkeitä, suojattavia kohteita. Suojattavien kohteiden kartoituksessa käytettiin apuvälineenä SFS ISO/IEC 27005 standardia. Suojattavien kohteiden kartoituksen jälkeen vuorossa oli riskianalyysin tekeminen valituille suojattaville kohteille.

Jotta tietoturvaa pystyttäisiin ylläpitämään JYVSECTEC -hankkeessa, täytyi hankkeelle luoda tietoturvan kouluttamissuunnitelma. Opinnäytetyön puitteissa pystyttiin määrittämään aihealueet tarvittavalle tietoturvakoulutukselle. Sisältö koulutukselle jätettiin hankkeen johdon päätettäväksi.

JYVSECTEC -hankkeen tietoturvaa lähdettiin rakentamaan niin, että testausta pystytään tekemään myös viranomaisten turvallisuusluokitellulle materiaalille. Tästä johtuen hankkeen sisällä tehtiin Kansallisen turvallisuusauditointikriteeristön versio II (KATAKRI II) pohjautuen auditointi. Auditoinnin avulla määritettiin kuinka hankkeen eri osa-alueilla arvioitavat kohteet täyttävät turvallisuusluokituksen asettamat vaatimukset ja määriteltiin parannusta vaativat kohteet.

Kun tietoturvan sen hetkinen taso hankkeessa saatiin kartoitettua, oli vuorossa tietoturvan kehittämissuunnitelman laatiminen. Kehittämissuunnitelmassa käytiin läpi kohteet, jotka eivät täyttäneet KATAKRI II suojaustason 4 asettamia kriteereitä ja vaativat näin ollen parannusta. Lisäksi kehittämissuunnitelmassa käytiin läpi muut jatkossa huomioon otettavat tietoturva-asiat esimerkiksi riskianalyysistä saadut tulokset.

Käytännön toteutuksen kuvioissa sekä liitteissä esiintyvät taulukot ovat pohjia, joita käytettiin tiedon keräämiseen. Taulukot eivät sisällä toimeksiantajalta kerättyä tietoa, koska tieto on tarkoitettu vain toimeksiantajan eli JYVSECTEC -

hankkeen sisäistä käyttöä varten. Kerätyn tiedon julkaiseminen aiheuttaisi vahinkoa JYVSECTEC -hankkeen liiketoiminnalle.

10 SUOJATTAVIEN KOHTEIDEN KARTOITUS

Suojattavien kohteiden kartoituksessa käytettiin pohjana SFS ISO/IEC 27005 standardin liitteessä B esitettyä mallia, jossa on eriteltynä ensisijaisia suojattavia kohteita tietoa, liiketoimintoja ja liiketoimintaprosesseja tukevia osa-alueita. Nämä osa-alueet ovat yleisesti tunnetut tietoturvan kahdeksan osa-aluetta:

- Hallinnollinen ja organisatorinen tietoturvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus

(Tietoturvalliseen yhteiskuntaan. 2012.)

Jako kahdeksaan osa-alueeseen ja tätä kautta kartoitetut yksittäiset kohteet muodostivat mahdollisimman kattavan ja aukottoman listan suojattavista kohteista.

10.1 Suojattavien kohteiden valinta

Suojattavia kohteita kartoitettiin yhdessä hankkeen henkilöstön kanssa. Aluksi luotiin kattava lista suojattavista kohteista Microsoft Office Excel- ja XMind -työkaluja käyttäen.

Tietoturvan toteutuksen ollessa vasta alkutekijöissään hankkeessa, pienennettiin suojattavien kohteiden listaa yhdistelemällä yksittäisiä suojattavia kohteita suuremmiksi kokonaisuuksiksi. Yksittäisten suojattavien kohteiden käytöllä olisi saavutettu tarkempi riskianalyysi, mutta työmäärä olisi samalla kasvanut huomattavasti. Kattava lista suojattavista kohteista jäi hankkeen sisäiseen käyttöön, joten sitä pystytään hyödyntämään tulevaisuudessa, kun tietoturvaa hankkeessa kehitetään. Kattava lista suojattavista kohteista sisälsi reilusti yli sata kohdetta, kun taas yleistetty lista sisälsi alle kaksikymmentä kohdetta. Yli sadalle kohteelle luotava riskianalyysi olisi ollut mahdotonta toteuttaa tämän opinnäytetyön resurssien puitteissa. Suurempia suojattavia kokonaisuuksia hyödyntäen pystyttiin luomaan yleispätevä riskianalyysi halutuille kohteille lyhyemmässä ajassa.

Suojattavat kohteet jaettiin ensin kahteen ryhmään:

- JYVSECTEC -hankkeen omistamat
- Asiakkaan omistamat.

Näitä kahta pääkohderyhmää pilkottiin pienemmiksi yleisellä tasolla siten, että JYVSECTEC -hankkeen alle sijoitettiin suojattaviksi kohteiksi:

- Laitteet
- Ohjelmistot
- Asiakirjat ja dokumentit
- Henkilöstö
- Käyttäjätasot
- Toimitilat
- Verkko.

Asiakkaiden alle sijoitettiin suojattaviksi kohteiksi:

- Laitteet
- Ohjelmistot
- Asiakirjat ja dokumentit
- Henkilöstö.

10.2 Suojattavien kohteiden hyödyntäminen

Suojattavien kohteiden listaaminen on jo itsessään arvokasta tietoa, jota hankkeessa voidaan hyödyntää jatkossa. Suojattavien kohteiden listaamisessa käydään läpi organisaatioon liittyviä asioita, joita kohtaan voi muodostua tietoturvauhkia ja jopa liiketoimintaa haittaavia tietoturvatapahtumia.

Valituille suojattaville kohteille suoritettiin riskianalyysi, josta lisää luvussa 11. Vaikka JYVSECTEC -hanke ja asiakas pääkohderyhmät sisälsivät samoja suojattavia kohteita, päätettiin ne pitää erillään toisistaan, koska JYVSECTEC -hankkeen omistamien ja asiakkaan omistamien kohteiden muodostamat riskit ja niiden käsittelytavat olivat erilaisia.

11 RISKIANALYYSIN TEKEMINEN

11.1 Riskien tunnistus

Suojattavien kohteiden kartoituksen jälkeen oli vuorossa riskianalyysin teko. Valitut suojattavat kohteet listattiin, jonka jälkeen opinnäytetyön tekijä ja JYVSECTEC -hankkeen henkilöstö etsivät mahdollisia haavoittuvuuksia suojattaville kohderyhmille. Haavoittuvuuksista mahdollisesti aiheutuvat uhat listattiin myös taulukkoon, jonka pohja on kuviossa 4. SFS ISO/IEC 27005 standardin liitteestä D löytyy esimerkkejä haavoittuvuuksista ja niistä mahdollisesti aiheutuvista uhkista.

Suojattava kohderyhmä	Esimerkki haavoittuvuudesta	Esimerkki uhasta	Todennäköisyys (0-3)	Kriittisyys (1-3)	Vastuuhenkilö	Toimenpide	Prioriteetti (1-9)
Laitteisto							
Ohjelmisto							
Asiakirjat ja dokumentit							
Henkilöstö							
Käyttäjätasot							
Toimitilat							
Verkko							

KUVIO 4. Riskianalyysi

11.2 Riskien suuruuden arviointi

Suojattaville kohteille määriteltiin haavoittuvuudet ja niistä mahdollisesti aiheutuvat uhat. Tämän jälkeen arvioitiin niiden liiketoimintaan kohdistuvaa vaikutusta kolmiportaisella asteikolla ja häiriöskenaarion todennäköisyyttä neliportaisella asteikolla. Tämä taulukko on esitetty kuviossa 5. Tällaiseen arviointitaulukkoon päädyttiin, koska toimeksiantajalla ei ollut tarvetta tässä vaiheessa tarkemmalle riskien suuruuden arvioinnille. Arviointiin lisättiin todennäköisyyden kohdalla arvo 0, jolloin todennäköisyys arvioitiin niin pieneksi, ettei se ollut mahdollinen. Näin saavutettiin tilanne, jossa turvamekanismia ei tarvitse kehittää tällaiselle uhalle. Tulevaisuudessa arviointitaulukkoa voidaan tarkentaa esimerkiksi viisiportaiseksi, jolloin saavutetaan tarkempi priorisointi riskeille.

Tietoturvamekanismien priorisointi suoritettiin kertomalla todennäköisyys- ja kriittisyysarvot. Näin saatu numeerinen arvo osoitti prioriteetin eli aikataulun, jonka mukaan turvamekanismi tulee ottaa käyttöön. Prioriteetin arvo on näin arvioituna nollan ja yhdeksän (0 – 9) välillä. Arvo nolla (0) tarkoittaa, ettei toimenpiteitä tarvita. Arvot kuusi (6) ja yhdeksän (9) tarkoittavat, että turvamekanismi tulee ottaa välittömästi käyttöön. Taulukkoon lisättiin värit vihreä, keltainen ja punainen eri sävyissä, jotka havainnollistavat tarvittavien toimenpiteiden tärkeyden. Tällä tavoin taulukosta saatiin visuaalisesti helposti ymmärrettävä.

		Häiriöskenaarion todennäköisyys	Ei todennäköinen (0)	Pieni (1)	Keskisuuri (2)	Suuri (3)
	Liiketoimintaan kohdistuva vaikutusarvo	Pieni (1)	0	1	2	3
		Keskisuuri (2)	0	2	4	6
		Suuri (3)	0	3	6	9

Riskin taso	**Riskin numerinen arvo**	**Toimenpiteet**
Ei riskiä	0	Ei toimenpiteitä, otettu huomioon riskianalyysissä
Pieni riski	1	Ei välittömiä toimenpiteitä, kirjataan ylös ja seurataan tilannetta
Keskitasoinen riski	2,3,4	Ennen seuraavaa katselmointia alennettava riskiä valitulla
Suuri riski	6,9	Korjattava välittömästi valitulla turvamekanismilla

KUVIO 5. Riskien tasot

Häiriöskenaarion todennäköisyyden arvioinnissa otettiin huomioon

- Kohteen valvonta
- Kohteen pääsynhallinta
- Kohteen aiheuttama mielenkiinto
- Uhan ilmenemistaajuus

- Kohteen ohjeistus
- Käyttäjämäärä, jolle uhan toteutus mahdollinen.

Liiketoimintaan kohdistuvan vaikutuksen eli kriittisyyden arvioinnissa otettiin huomioon

- Toiminnan keskeytys
- Vaikutus organisaation toimintaan
- Taloudelliset kustannukset
- Aiheutuvat toimenpiteet.

11.3 Turvamekanismien valinta

Riskien arvioinnin jälkeen aloitettiin toimenpiteiden määritys uhkia vastaan eli turvamekanismien valinta. Mikäli kohteille ei arvioitu riskiä, kirjattiin se ylös eikä turvamekanismia määritelty kyseiselle kohteelle. Turvamekanismien tarkoituksena on pienentää havaittu uhka hyväksyttävälle tasolle. Turvamekanismien määrittämisen yhteydessä määriteltiin myös jokaiselle toimenpiteelle vastuuhenkilö, joka vastaa turvamekanismien integroinnista järjestelmään. Tällä toimenpiteellä haluttiin varmistaa, että turvamekanismit otetaan käyttöön.

12 TIETOTURVAN KOULUTTAMISSUUNNITELMA

Tietoturvakoulutuksessa käydään läpi hankkeen tietoturvapolitiikka. JYVSECTEC -hankkeella ei opinnäytetyön aikana ollut omaa tietoturvapolitiikkaa, mutta hankkeessa oli käytettävissä Jyväskylän ammattikorkeakoulun tietoturvapolitiikka. Tietoturvakoulutuksen tärkeimpänä tavoitteena voidaan pitää tietoturvatietouden kohottamista hankkeen sisällä. Tietoturvakoulutuksen avulla voidaan yhtenäistää hankkeen työntekijöiden tietoturvan tuntemusta ja sopia yhteisistä pelisäännöistä tietoturvan osalta hankkeessa. Tietoturvakoulutuksessa

käydään myös läpi yleistä, tietoturvaan liittyvää termistöä, jolloin henkilökunnalla on yhteinen kieli tietoturvasta puhuttaessa. (Tietoturvallisuus on asenne!, VAHTI 6/2008 2008, 21.)

Tässä luvussa käydään läpi muutamia yksittäisiä tietoturvan kouluttamissuunnitelmassa huomioon otettavia asioita. Tietoturvan kouluttamissuunnitelmaa kehitettäessä tulee huomioida koulutuksen kohderyhmä. Tässä hankkeessa suurin osa kohderyhmästä on tietotekniikan ammattilaisia ja heillä on siis tietotekniikan puolelta tietoturvallisuudesta jonkinlainen käsitys. Tietoturvallisuus on kuitenkin paljon muutakin, kuin tietotekninen tietoturva. Tietoturvakoulutus on tärkeä osa hankkeen tietoturvaa.

12.1 Sisäiset uhat

Käyttäjä eli ihminen aiheuttaa suurimman osan tietoturvatapahtumista. Käyttäjä voi aiheuttaa joko tahattomasti tai tahallisesti vahinkoa järjestelmissä. Tahallisesti aiheutetussa vahingossa taustalla voi olla esimerkiksi omien taitojen testaaminen tai kiusanteko. Tahattomat vahingot aiheutuvat esimerkiksi kokemattomista käyttäjistä tai vääristä käyttäjäoikeuksista, jolloin käyttäjä pääsee käsiksi järjestelmiin, joihin hänellä ei pitäisi olla oikeuksia ja voi näin tietämättömyydellään aiheuttaa vikoja järjestelmään. (Tietoturvallisuus on asenne!, VAHTI 6/2008 2008, 17,19,43,45.)

12.2 Ulkopuoliset uhat

Hankkeen ulkopuolisten uhkien lista voi olla hyvinkin pitkä, seuraavaksi käydään läpi tällä hetkellä maailman laajuisesti pinnalla olevia ulkopuolisia uhkia. Tänä päivänä sosiaalinen media ja niin sanotut Phishing- hyökkäykset luovat merkittävän tietoturvauhan, joka kohdistuu hankkeeseen ulkopuolelta. Sosiaalisessa mediassa voidaan jakaa reaaliaikaisesti ajankohtaista tietoa organisaatiota koskevista asioista suurelle määrälle käyttäjiä. Varomaton so-

siaalisen median käyttö saattaa tuottaa suurta vahinkoa organisaation imagolle ja jopa taloudelle, mikäli jaetaan organisaation kannalta herkkää tai väärää informaatiota. (Sosiaalisen median tietoturvaohje, VAHTI 4/2010 2010, 13.)

Phishing- hyökkäyksillä tarkoitetaan usein sähköpostin kautta leviäviä tiedon urkintaviestejä. Viestit on naamioitu jonkin olemassa olevan yrityksen nimiin ja niiden kautta kysellään muun muassa pankkitunnuksia. Viime aikoina ovat yleistyneet myös phishing- sivustot, jotka näyttävät esimerkiksi pankin omilta verkkosivuilta, mutta ovat naamioituja tietojen keräämiseen tarkoitettuja sivustoja. (1/2005 Suojautuminen phishing-hyökkäyksiltä 2005.)

Hankkeen työntekijät voivat kohdata työnantajaansa kohdistuvia phishing-hyökkäyksiä. Sähköpostien välityksellä levitetään viestejä, joissa kysellään hanketta koskevia arkaluontoisia asioita, joita ei saa hankkeen ulkopuolelle levittää. Nämä asiat voivat olla hankkeen yhteistyökumppaneihin tai hankkeen omaan talouteen liittyviä seikkoja. Ennen Internetin yleistymistä olivat suosiossa puhelimen välityksellä tehdyt phishing- hyökkäykset, joiden avulla kalasteltiin organisaatioon liittyviä tietoja.

12.3 Motivointi

Tietoturvakoulutuksessa tulee korostaa työntekijöiden merkitystä tietoturvallisen työympäristön saavuttamisessa. Tietoturvakoulutuksen tärkein tavoite on kasvattaa henkilöstön tietoturvan tietoisuutta. Motivoitunut työntekijä on aidosti kiinnostunut aiheesta ja omaksuu helpommin asioita. Motivointikeinona tietoturvakoulutuksessa voidaan käyttää esimerkkejä ja perusteluja, miksi tietynlainen toiminta tietyissä tilanteissa on tärkeää tietoturvan kannalta. (Tietoturvallisuus on asenne!, VAHTI 6/2008. 2008, 22.)

12.4 Tietojen käsittely

Hankkeen sisällä tulee luoda omat käytännöt tietojen käsittelyä varten. Käytännöt tulee käydä läpi tietoturvakoulutuksessa henkilöstölle, näin pyritään varmistamaan yhtenäinen toimintatapa tietojen käsittelyssä. Tiedolle tulee aina merkitä omistaja hankkeen sisällä, joka on vastuussa tiedon tallentamisesta, tuhoamisesta ja kopioimisesta. Tietoon tulee olla pääsy vain sellaisilla henkilöillä, joilla on perusteltu syy päästä käsiksi kyseessä olevaan materiaaliin. (SFS ISO/IEC 17799:fi. 2006, 100.)
Hyviä käytäntöjä ovat myös puhtaan pöydän ja puhtaan näytön politiikat. Puhtaan pöydän politiikalla tarkoitetaan, että työntekijä pitää huolen, ettei hänen työpöydällään ole arkaluonteista materiaalia, jonka paljastuminen ulkopuolisille tahoille aiheuttaisi tiedon luottamuksellisuuden tai eheyden menetyksen. Puhtaan pöydän politiikka kannustaa toisaalta työpisteen siisteyteen. (SFS ISO/IEC 17799:fi, 132.)

Puhtaan näytön politiikassa noudatetaan käytäntöä, jossa käyttäjä varmistaa, ettei ulkopuolisille välity arkaluontoista tietoa oman tietokoneen ruudulta. Suositellaan käytettäväksi salasanalukittua näytönsäästäjää tai uloskirjautumista valvomattomissa tietokoneissa ja päätelaitteissa. Näillä toimenpiteillä pyritään varmistamaan, että työpisteeltä poistuttaessa ulkopuoliset pääse käsiksi tietokoneella olevaan tietoon. (SFS ISO/IEC 17799:fi, 132.)

12.5 Vierailijakäytännöt

JYVSECTEC -hanke toimii Jyväskylän ammattikorkeakoulun tiloissa, tästä johtuen sen tilojen läheisyydessä liikkuu runsaasti päivittäin ulkopuolisia henkilöitä. Lisäksi tullaan järjestämään vierailuja hankkeen tiloihin. Nämä seikat muodostavat uhan, jossa ulkopuoliset tahot pääsevät käsiksi hankkeen sisäisiin tietoihin.

Vierailijoita varten on luotava selkeät käytännöt sellaisista tavoista, joilla hankkeeseen liittyvät vierailijat pystytään tunnistamaan. Lisäksi hankkeen henkilöstöä on ohjeistettava oikeanlaisista vierailijakäytännöistä. Esimerkiksi jokaiselle vieraalle on määritettävä isäntä vierailun ajaksi sekä vierailijoille on annettava vierailijakortit, jonka avulla vieraat pystytään tunnistamaan.

13 TURVALLISUUSAUDITOINTI

JYVSECTEC -hankkeen turvallisuutta haluttiin testata toimeksiantajan aloitteesta. Toimeksiantajan kanssa sovittiin, että JYVSECTEC -hankkeelle suoritetaan auditointi kansallisen turvallisuusauditointikriteeristön version II (KATAKRI II) pohjalta. Täysimittaiselle auditoinnille tässä vaiheessa hankkeen elinkaarta ei ollut toimeksiantajan mielestä tarvetta, joten auditointi suoritettiin soveltuvin osin hankkeelle.

Turvallisuusauditoinnin avulla suoritettu turvallisuustason määrittely kohdeorganisaatiolle on haastavaa. Virallisen turvallisuusauditoinnin suorittamista varten täytyy auditoijan suorittaa erillinen turvallisuusauditoijan koulutus, joka on valtionhallinnon hyväksymä. Turvallisuusauditointi koulutusta annetaan ammattikorkeakoulutasoisena sekä täydennyskoulutuksena. (Kansallinen turvallisuusauditointikriteeristö versio II. 2010, 4.).

Tämän opinnäytetyön puitteissa suoritettu turvallisuusauditointi nosti esille sellaisia asioita, joita hankkeessa täytyy parantaa mikäli halutaan täyttää suojaustaso 4 asettamat vaatimukset.

13.1 Kansallinen turvallisuusauditointikriteeristö, versio II

JYVSECTEC -hankkeessa suoritettiin Kansalliseen turvallisuusauditointikriteeristöön versio II (KATAKRI II) pohjautuva turvallisuusauditointi. Kansallinen

turvallisuusauditointikriteeristö on luotu yhtenäistämään ja ohjeistamaan viranomaisten suorittamaa turvallisuusauditointia yrityksissä ja yhteisöissä. Turvallisuusauditoinnin tarkoituksena on tarkistaa täyttääkö auditoinnin kohteen turvallisuuden taso vaadittavan. Lisäksi turvallisuusauditointi antaa hyvän kuvan auditoinnin kohteena olevan yrityksen tai yhteisön tämän hetkisestä tietoturvatasosta. Kriteeristö sisältää myös elinkeinoelämän suosituksia, jotka antavat hyviä vinkkejä turvallisuustason nostamiseen. Kansallisessa turvallisuusauditointikriteeristössä ei oteta kantaa korkeimman turvallisuusluokituksen, suojaustaso I (turvallisuusluokitusmerkintä ERITTÄIN SALAINEN) tasoiseen materiaaliin, koska tällaisen materiaalin luovuttaminen eteenpäin on erittäin harvinaista. (Kansallinen turvallisuusauditointikriteeristö versio II. 2010, 3.)

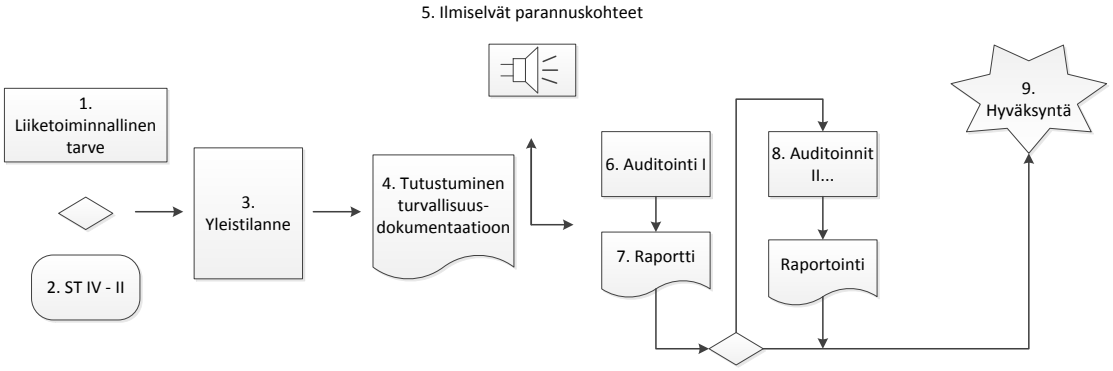
Kansallinen turvallisuusauditointikriteeristö on luotu turvallisuustarkastajille eli auditoijille, jotka toimivat viranomaisille tai viranomaisten valtuuttamina. Auditoijille on annettu valtuudet, joilla voidaan todentaa, että auditoinnin kohteen turvallisuuden taso on KATAKRI II:n vaatimusten mukainen. (Kansallinen turvallisuusauditointikriteeristö versio II. 2010, 4.)

13.2 Turvallisuusauditointiprosessi

Tämän opinnäytetyön kohteena oli JYVSECTEC -hankkeen tiloissa tapahtuvan laitteiston ja ohjelmiston teknisen testauksen tietoturvallisuuden hallintajärjestelmä. Turvallisuusauditointi suoritettiin testaukseen välittömästi liittyville kohteille, joita olivat

- Tilat
- Laitteistot
- Ohjelmistot
- Henkilöstö.

On syytä ottaa huomioon, että opinnäytetyöntekijä ei ollut viranomaisten valtuuttama auditoija, joten turvallisuusauditointi ei ollut kaikenkattava eikä JYV-SECTEC -hanke voi markkinoida itseään KATAKRI II auditoituna. Tämän opinnäytetyön puitteissa suoritetun auditoinnin tarkoituksena oli löytää JYV-SECTEC -hankkeesta sellaisia kohteita, jotka tarvitsevat parannusta, mikäli hankkeessa halutaan saavuttaa KATAKRI II määrittelemä viranomaisvaatimus. Kuviossa 6 on havainnollistettuna auditointiprosessin tekninen suoritus.



KUVIO 6. Auditointiprosessi (tekninen suoritus)

(Kansallinen turvallisuusauditointikriteeristö versio II. 2010, 5.)

Opinnäytetyön puitteissa suoritettiin auditointi kuvion 6 mukaisesti kohtaan 5 asti. Liiketoiminnan tarpeina otettiin huomioon JYVSECTEC hankkeen tiloissa tapahtuvan laitteiston ja ohjelmiston tekninen testaus ja siihen liittyvät tarpeet henkilöstö-, tieto-, ja fyysisen turvallisuuden osalta. Hallinnollinen turvallisuus -osio jätettiin tämän opinnäytetyön aihe-alueen ulkopuolelle.

Tavoite suojaustasoksi JYVSECTEC -hankkeen henkilöstö asetti alimman viranomaisvaatimuksen eli perustaso (IV). Hankkeen tämän hetkistä tilannetta kartoitettiin keskittyen valitun liiketoiminnan tarpeisiin. KATAKRI II kysymyslista käytiin läpi palaverimuotoisena hankkeen henkilöstön kanssa ja saatuja tuloksia verrattiin viranomaisvaatimukseen perustaso (IV) (ST4). Liitteissä 1-9 on Microsoft Office Excel- työkalulla luodut taulukot, joita käytettiin apuna KATAKRI II mukaisen kysymyslistan läpikäynnissä. Taulukot eivät sisällä kaikkia

KATAKRI II löytyviä kysymyksiä, vain oleelliset kysymykset JYVSECTEC -hankkeeseen liittyen. Taulukot eivät sisällä kerättyä tietoa, koska se on tarkoitettu vain JYVSECTEC -hankkeen sisäiseen käyttöön.

Kysymyslistan läpi käynnin ja palaverin aikana tuotetun taulukon avulla opinnäytetyön tekijä laati JYVSECTEC -hankkeelle dokumentin, joka sisälsi eriteltynä kohteet, jotka vaativat toimenpiteitä, mikäli hankkeessa halutaan saavuttaa viranomaisvaatimuksen perustaso (IV). Edellä mainittu dokumentti toimii JYVSECTEC -hankkeelle tarkistuslistana niistä asioista, joihin täytyy kiinnittää huomiota ja suorittaa korjaavia toimenpiteitä, mikäli JYVSECTEC -hanke halutaan auditoida täyttämään viranomaisvaatimuksen perustaso (IV).

JYVSECTEC -hankkeen kannalta turvallisuusauditointiprosessi suoritettiin hyvään ajankohtaan. Hankkeen ydintoiminta eli tietoturvan testaaminen ei ollut vielä käynnistynyt ja havaitut, huomioon otettavat puutteet laitteistojen, ohjelmistojen, henkilöstön sekä tilojen osalta pystyttiin korjaamaan ennen virallisen toiminnan alkamista.

14 TIETOTURVALLISUUDEN KEHITTÄMINEN

JYVSECTEC -hankkeessa tullaan jatkossa kehittämään tietoturvallisuutta tämän opinnäytetyön pohjalta. Vaikka opinnäytetyössä keskityttiin vain yhden osa-alueen tietoturvallisuuden hallintajärjestelmän luomiseen, voidaan tätä hyödyntää myös muiden osa-alueiden tietoturvallisuuden kehittämisessä. Varsinaista tietoturvallisuuden kehittämissuunnitelmaa ei tämän opinnäytetyön puitteissa luotu, vaan hankkeessa hyödynnetään opinnäytetyön aikana tuotettuja dokumentteja tietoturvallisuuden kehittämisessä.

Turvallisuusauditoinnin avulla tuotetun 18 -sivuisen dokumentin pohjalta JYVSECTEC -hankkeessa pyritään täyttämään KATAKRI II viranomaisvaatimuk-

sen perustason (IV) asettamat vaatimukset. Suojattavien kohteiden listausta voidaan hyödyntää muiden hankkeen osa-alueiden riskianalyyseissä. Suoritetun riskianalyysin pohjalta saatujen tulosten perusteella hankkeeseen sisällytetään tietoturvamekanismit, joiden avulla hankkeeseen kohdistuvia uhkia pienennetään. Lisäksi jokaiselle tietoturvamekanismille on määritetty vastuuhenkilö, joka vastaa mekanismin käyttöön otosta. Opinnäytetyön aikana hankkeeseen tuotiin tietoturvallisuutta aktiivisesti esille ja pyrittiin luomaan tietoturvallisuuden huomioiminen rutiiniksi hankkeeseen.

15 YHTEENVETO

15.1 Toteutus

Ennen opinnäytetyön tekoa olin tutustunut tietoturvallisuuden hallintajärjestelmiin pintaraapaisulta kurssilla, joka oli järjestetty Jyväskylän ammattikorkeakoulussa tietotekniikan opintoihin liittyen. Opinnäytetyön aikana tutustuin syvällisemmin useisiin standardeihin ja sain hyvää teoriapohjaa tietoturvan toteutuksesta organisaatioissa.

Opinnäytetyön aiheeksi valittiin toukokuun alussa JYVSECTEC -hankkeen tietoturvallisuuden hallintajärjestelmän toteuttaminen. Samaan aikaan JYVSECTEC -hankkeessa rekrytoitiin työntekijöitä. Olimme sopineet ohjaavan opettajani kanssa käytännön toteutuksen alkavan syyskuussa, kun kesälomat olivat ohitse. Koko opinnäytetyön oli määrä olla valmis joulukuussa 2012.

Aloitin opinnäytetyön tekemisen tutustumalla ISO standardeihin 17799, 27001 ja 27003. Tarkoituksenani oli standardien lukemisen ohella kirjoittaa käytännön toteutusta tukevaa teoriapohjaa ja pohtia mahdollisia toimintamalleja käytännön toteutusta ajatellen. Standardien läpikäyminen oli työlästä ja aikaa vievää, mutta kesän aikana sain käytyä standardit läpi.

Kun teoriaosuus alkoi olla syyskuussa valmis, ilmeni opinnäytepalaverissa, ettei JYVSECTEC -hankkeella ollut resursseja oman aikatauluni mukaiseen toteutukseen. Kesän aikana JYVSECTEC -hanke oli palkannut tietoturva-asiantuntijan ja hankkeen aikataulu oli kiristynyt. Toimeksiantajan resurssipulan vuoksi opinnäytetyön aihetta rajattiin koskemaan vain JYVSECTEC -hankkeen tiloissa tapahtuvan laitteiston ja ohjelmiston teknistä testausta. Näin jälkikäteen ajateltuna tuon aihealueen rajauksen olisi voinut tehdä jo aikaisemmin, koska koko tietoturvallisuuden hallintajärjestelmän luomiseen eivät opinnäytetyöhön varatut tunnit olisi mitenkään riittäneet. Lopullinen rajaus oli onnistunut ja opinnäytetyön puitteissa saatiin luotua halutut dokumentit JYVSECTEC -hankkeelle.

Aihealueen kavennuksen yhteydessä teoriamateriaaleiksi lisättiin ISO 27005 standardi, Kansallinen turvallisuusauditointikriteeristö versio II (KATAKRI II), sekä Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, 2/2010 (VAHTI 2/2010). Edellä mainituista materiaaleista sain hyviä vinkkejä käytännöntoteutukseen. KATAKRI II ja VAHTI 2/2010 sisältävät paljon käytäntöön soveltuvia esimerkkejä ja malleja, joiden avulla pystyin luomaan toimeksiantajan haluamia dokumentteja.

Käytännön toteutuksessa jouduin luonnollisesti olemaan paljon yhteydessä toimeksiantajaan, koska tarkoituksena oli tehdä heidän tarpeisiinsa soveltuva tietoturvallisuuden hallintajärjestelmä, joka tukisi mahdollisimman paljon heidän toimintaa. Yhteisen ajan sopiminen tuntui välillä olevan hankalaa, sillä toimeksiantajalla oli useampi henkilö, joita täytyi konsultoida opinnäytetyön etenemisestä. Toimeksiantajan kanssa kävimme palavereja, joissa keskustelimme työn etenemistä ja sain samalla palautetta ja ohjeistusta tekemästäni työstä. Lisäksi palavereissa keskustelimme JYVSECTEC -hankkeen henkilöstön kanssa sen hetkisestä tietoturvan tasosta ja parannusehdotuksista sen hetkiseen tilanteeseen. Näiden parannusehdotusten pohjalta toteutimme tietoturvallisuuden hallintajärjestelmää hankkeeseen.

15.2 Tulokset

Opinnäytetyön tuloksena JYVSECTEC -hankkeelle luotiin pohja tietoturvallisuuden hallintajärjestelmälle testauksen osalta. JYVSECTEC -hankkeella ei ollut minkäänlaista tietoturvallisuuden hallintajärjestelmää aikaisemmin. JYVSECTEC -hanke sai kattavan katsauksen sen hetkisen tietoturvan tasosta sekä kehitysehdotuksia tietoturvan parantamiseen. JYVSECTEC -hankkeelle arvokkaana tietona voidaan pitää suojattavien kohteiden kartoituksen tuloksena tuotettua listaa. Listassa on listattuna testaukseen liittyvä kohteita, joihin voidaan olettaa liittyvän haavoittuvuuksia. Riskianalyysin pohjalta hankkeessa kiinnitetään huomiota esille nousseisiin haavoittuvuuksiin ja niistä mahdollisesti aiheutuviin uhkiin. Uhkia pyritään pienentämään opinnäytetyön puitteissa laadituilla tietoturvamenetelmillä. Tämän opinnäytetyön aikana laadittiin myös tietoturvan kouluttamissuunnitelmalle runkoa. Suunnitelman tarkoituksena on nostaa esille niitä asioita, joita tulee ottaa huomioon tietoturvaa koulutettaessa JYVSECTEC -hankkeen henkilöstölle. KATAKRI II mukainen turvallisuusauditointi nosti esille monia puutteita hankkeen tietoturvallisuudessa. Opinnäytetyön aikana luotu dokumentti antaa ohjeistuksen, kuinka havaitut puutteet tulee korjata. Korjausten jälkeen JYVSECTEC -hankkeella on mahdollisuus täyttää viranomaisvaatimuksen perustaso (IV) vaatimukset.

15.3 Pohdinta

Opinnäytetyön aikana opin paljon tietoturvallisuudesta. Standardeissa esille tuli asioita, joita en ollut aikaisemmin ajatellut liittyvän tietoturvallisuuteen. Sain kattavan kuvan tietoturvallisuuden luomisesta organisaatioon, vaikka tarkempiin yksittäisiin teknisiin tietoturvatoteutuksiin ei opinnäytetyön aikana otettu kantaa. Mielestäni onkin tärkeä hahmottaa ensin kokonaiskuva. Tämän jälkeen on helpompi lähteä tutkimaan tarkemmin yksittäisiä toteutuksia. JYVSECTEC -hankkeeseen palkatulta tietoturva-asiantuntijalta opin myös paljon

asioita liittyen tietoturvallisuuteen. Opin myös opinnäytetyön aikana erilaisia työskentelymalleja, joita hyödynsin opinnäytetyössä.

Omien työskentelytapojen muokkautuminen tehokkaaksi tarvitsee aikaa, mutta nyt opittuja taitoja voin soveltaa tulevaisuudessa uusissa projekteissani. Huomasin monesti, että ensimmäisenä kehittämäni toimintamalli ei välttämättä ollut paras. Pienillä muokkauksilla toimintamallit yleensä tehostuivat ja ne olivat käyttökelpoisia.

Toimin opinnäytetyön ajan eräänlaisena projektipäällikkönä tietoturvallisuuden luonnissa hankkeeseen, joten minulla oli vastuu tietoturvatyön etenemisestä. Tehtävä oli vastuullinen ja opettavainen. Uskon, että jatkossa tästä vastuullisesta tehtävästä on minulle hyötyä työelämässä.

Jatkossa tietoturvaa pystytään kehittämään JYVSECTEC -hankkeessa tämän opinnäytetyön tuloksena saatujen dokumenttien pohjalta. Opinnäytetyön aikana tuli esiin useita kohteita, joista voidaan teettää uusia opinnäytetöitä tietoturvaan liittyen JYVSECTEC -hankkeelle. Pohja tietoturvallisuuden hallintajärjestelmälle on luotu ja tämän jälkeen tietoturvaa helpompi lähteä kehittämään. Tämän opinnäytetyön tuloksina saaduista tiedoista ja dokumenteista on paljon hyötyä JYVSECTEC -hankkeelle.

On syytä muistaa, ettei tietoturvan toteuttamista voida ajatella projektina, koska tietoturvasta ei voida koskaan sanoa sen olevan valmis. Tekniikka kehittyy kokoajan ja samalla hyökkäys- ja puolustusmenetelmät. Uusia puolustusmenetelmiä kehittelevät tahot ovat jatkuvassa kilpajuoksussa hyökkäysmenetelmiä kehittelevien tahojen kanssa. Tietoturvan toteuttaminen on enemmän prosessimuotoista, jolloin siinä tapahtuu jatkuvaa kehitystä ja se on tärkeä osa organisaatiota koko organisaation elinkaaren ajan.

LÄHTEET

1/2005 Suojautuminen phishing-hyökkäyksiltä. 2005. Cert-fi:n ohje 31.10.2005. Viitattu 5.11.2012. Viestintävirasto cert-fi. Http://www.cert.fi. Ohjeet, 2005.

A 1.7.2010/681. 1.7.2010. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. Viitattu 30.10.2010. Valtion säädöstietopankki Finlex. Http://www.finlex.fi, ajantasainen lainsäädäntö.

JYVSECTEC – Jyväskylä Security Technology. 2012. JYVSECTEC-hankkeen kotisivut. Viitattu 18.9.2012. Http://www.jyvsectec.fi.

Kansallinen turvallisuusauditointikriteeristö versio II. 2010. Viitattu 30.10.2012. Http://www.defmin.fi Puolustushallinnon voimavarat, PLM:n turvallisuuden sivusto.

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, 2/2010. 2010. Valtiovarainministeriö. Viitattu 30.10.2012. Http://www.vm.fi, Julkaisut ja asiakirjat, Julkaisut, Valtionhallinnon tietoturvallisuus.

SFS ISO/IEC 17799:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 9.8.2012. Http://www.jamk.fi/kirjasto, Neli-portaali, SFS-online.

SFS ISO/IEC 27001:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 11.9.2012. Http://www.jamk.fi/kirjasto, Neli-portaali, SFS-online.

SFS ISO/IEC 27003. 2010. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 31.10.2012. Http://www.jamk.fi/kirjasto, Nelli-portaali, SFS-online.

SFS ISO/IEC 27005. 2009. Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. Helsinki: Suomen Standardoimisliitto SFS. Viitattu 3.10.2012. Http://www.jamk.fi/kirjasto, Neli-portaali, SFS-online.

Sosiaalisen median tietoturvaohje, VAHTI 4/2010. 2010. Valtiovarainministeriö. Viitattu 5.11.2012. Http://vm.fi. Julkaisut ja asiakirjat, Julkaisut, Valtiohallinnon tietoturvallisuus, 2010.

Tietoturvalliseen yhteiskuntaan. 2012. Viestintäviraston 4.5.2012 päivittämä ohjeistus. Viitattu 30.10.2012. Http://www.ficora.fi, Viestintävirasto A-Ö, Tietoturva ja –suoja.

Tietoturvallisuus on asenne!, VAHTI 6/2008. 2008. Valtiovarainministeriö. Viitattu 5.11.2012. Http://www.vm.fi. Julkaisut ja asiakirjat, Julkaisut, Valtionhallinnon tietoturvallisuus, 2008.

LIITTEET

Liite 1. KATAKRI II vaatimuksia henkilöstön osalta

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Henkilöstöä koskevat vaatimukset			
Onko käytössä ns. puhtaan pöydän politiikka? Koskeeko sama periaate myös näyttöjä?	1) Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka on käytössä. 2) Huolehditaan siitä, ettei neuvottelutiloihin jää suojattavaa tietoa sisältäviä asiakirjoja tai muita muistiinpanoja kokousten jälkeen.		
Onko huolehdittu riittävästä työtehtävien eriyttämisestä niin, ettei synny ns. vaarallisia työyhdistelmiä?	Tehtävät ja vastuualueet on riskienarvioinnin mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai vää- rinkäytön riskiä.		Tyypillinen vaatimus erityisesti kansainvälistä turvaluokiteltua tietoa käsittelevälle järjestelmälle on se, että järjestelmälle vaaditaan erilliset roolit (ja henkilöt) järjestelmän ylläpitoon (security administrator) ja lokien tarkkailuun (audit administrator). Esimerkki valvontamekanismista: Kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän (two man rule).

Liite 2. KATAKRI II vaatimuksia ohjelmiston osalta osa I

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Miten on pienennetty haittaohjelmien aiheuttamia riskejä?	1) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat yleisesti alttiita haittaohjelmatartunnoille (erityisesti työasemat, kannettavat tietokoneet ja palvelimet). 2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä. 3) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja. 4) Haittaohjelmatunnisteet päivittyvät säännöllisesti. 5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta. 6) Haittaohjelmahavaintoja seurataan.		Suositellaan, että torjuntaohjelmistojen tuottamia havaintoja seurataan keskitetyllä hallintajärjestelmällä. Järjestelmissä, joita ei kytketä julkiseen verkkoon, haittaohjelmatunnisteiden päivitys voidaan järjestää esimerkiksi käyttämällä hallittua suojattua päivitystenhakupalvelinta, jonka tunnistekanta pidetään ajan tasalla esimerkiksi erillisestä Internetiin kytketystä järjestelmästä tunnisteet käsin siirtämällä (esim. kerran vuorokaudessa). Erityisesti II-tason järjestelmissä päivitykset joudutaan usein asentamaan käsin. Kummassakin tapauksessa tulee varmistua päivitysten eheydestä (lähde, tarkistussummat, jne.).Suojaustasoja III ja II koskevat vaatimukset pyrkivät pienentämään erityisesti USB-muistien välityksellä leviävien haittaohjelmien riskiä. Tapauskohtaisesti voidaan edellyttää esimerkiksi sitä, että järjestelmään kytketään vain erikseen määritettyjä luotettavaksi todennettuja muistitikkuja (ja vastaavia), joita ei kytketä mihinkään muuhun järjestelmään. Tapauskohtaisesti voidaan hyväksyä esimerkiksi järjestely, jossa vain organisaation tietohallinnon (tai vast.) jakamia muistivälineitä voidaan kytkeä organisaation järjestelmiin, ja että kaikkien muiden muistivälineiden kytkeminen on kielletty ja/tai teknisesti estetty. Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, on määriteltävä menetelmät, jolla pienennetään tämän aiheuttamaa riskiä. Menetelmänä voidaan tapauskohtaisesti hyväksyä esimerkiksi se, että ei-luotetusta lähteestä tuleva muisti kytketään eristettyyn tarkastusjärjestelmään, jonne siirrettävä tieto siirretään, ja josta siirrettävä tieto viedään edelleen luotettuun järjestelmään erillistä muistivälinettä käyttäen. Huom: Järjestelyn on huomioitava suojaustasolla III vähintään muistialueen tarkastaminen. Suojaustasolla II on huomioitava myös muistivälineen kontrolleritason räätälöinnin uhat.
Ovatko organisaation teknisten laitteiden ja palveluiden lokimenettelyt kunnossa?	1) Tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. 2) Keskeisiä tallenteita säilytetään 6 kk tai erillisessä sopimuksessa määrätty aika. 3) Suojattavaa tietoa sisältävät lokitiedot on suojattu asianmukaisesti (pääsynvalvonta, käsittely, poisto)		
Miten on varmistuttu siitä, että käytetyt salausratkaisut ovat riittävän turvallisia?	Salausratkaisujen (ja -tuotteiden) tietoturvallisuus on tarkastettu ja hyväksytty ko. suojaustasolle a) kansainvälisen tietoturvaviranomaisen toimesta, b) kansallisen tietoturvaviranomaisen toimesta, tai c) erillisessä ratkaisulle suoritetussa tarkastuksessa.		Erityisesti kansainvälisen turvaluokitellun tiedon salaamisessa edellytetään käytettävän käytännössä vain tiedon omistajan (esim. EU) hyväksymiä salausratkaisuja. Kansallisella salaustuotteiden hyväksyntäviranomaisella (CAA, Crypto Approval Authority, Suomessa NCSA-FI) on tietyin rajauksin mahdollisuus hyväksyä myös muita tuotteita/ratkaisuja kansainvälisen turvaluokitellun tiedon suojaamiseen. Usean kansainvälisen turvallisuusviranomaisen salaustuotehyväksynnät edellyttävät tuotteelta erinäisiä sertifikaatteja (erityisesti Common Criteria, toisinaan myös esim. FIPS 140), ja lisäksi tiettyjen erityisvaatimusten (esim. lähdekoodin luovutus ja tarkastus, hajasäteilysuojaukset) täyttämistä.
Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita?	1) Käytössä on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä. 4) Organisaatiossa on olemassa uusien järjestelmien, järjestelmäpäivitysten ja vastaavien hyväksymiskriteerit. Vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä käytetään . 5) Suojattavan tiedon käsittelyyn käytetään vain viranomaisen hyväksymiä verkkoja ja järjestelmiä.		

Liite 3. KATAKRI II vaatimuksia ohjelmiston osalta osa II

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Onko organisaatiossa otettu käyttöön periaatteet ja turvamekanismit etä- ja matkatyönriskejä vastaan?	1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan. 2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle. 3) Turvallisesta etä- ja matkatyöskentelystä on henkilöstön saatavilla ohje. 4) Laitteita, tietoaineistoja tai ohjelmia ei siirretä pois työpaikalta ilman ennalta saatua valtuutusta. 5) Järjestelmien etähallinnassa tai -käytössä käytetään vahvoja todennusmenettelyjä. 6) Suojattavaa tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle. 7) Toimitilojen ulkopuolelle vietyjä laitteita ja tietovälineitä ei jätetä valvomatta julkisille paikoille, kannettavat tietokoneet kuljetetaan matkustaessa käsimatkatavarana. 8) Vain luotettavia ja käyttöympäristöön hyväksyttyjä laitteita (esim. työnantajan tarjoama kannettava tietokone) ja etätyöyhteyksiä käytetään.		Suojaustasolla IV hyväksyttävä etäkäyttö- ja etähallintaratkaisu edellyttää liikenteen luotettavan salauksen lisäksi tyypillisesti vahvaa käyttäjätunnistusta ja käytön teknistä sitomista työnantajan tarjoamaan etäkäyttölaitteistoon (esim. laitetunnistus). Erityisesti etähallinnassa huomioitava myös etähallintapisteen looginen ja fyysinen sijainti. Suojaustasolla III hyväksyttävä etähallintamenettely huomioi mm. etähallintapisteiden fyysisen ja loogisen pääsynvalvonnan, hallintaan käytetyt laitteistot ja ohjelmistot, hallintaliikenteen salauksen, ja edellä mainittujen elementtien luotettavuuden erityisesti luottamuksellisuuden ja eheyden suhteen. Viranomaisten suojaustason II järjestelmissä voidaan tapauskohtaisesti hyväksyä rajattu etähallinta. Tapauskohtaisesti hyväksyttävällä etähallinnalla tarkoitetaan tässä yhteydessä lähes poikkeuksetta turvapäivitysten ja haittaohjelmatunnistekantojen keskitettyä jakelua. Jotta etähallinta voidaan hyväksyä, tulee viranomaisen tekemässä järjestelmällisessä ja kokonaisvaltaisessa riskienarvioinnissa päätyä aina tulokseen, jossa etähallinta on paikallista hallintaa merkittävästi pienempi riski. Tällaisen etähallinnan hyväksyminen edellyttää aina myös päivityspalvelimen sisällyttämistä samaan tietojärjestelmään ja sen fyysistä eristämistä muista järjestelmistä.
Ovatko kehitys-/testaus ja tuotantojärjestelmät erilliset?	1) Kehitys-/testaus- ja tuotantojärjestelmien on oltava erilliset. 2) Ennen uuden järjestelmän käyttöönottoa, testidatat, oletus- ja testikäyttäjätilit ja vastaavat poistetaan. 3) Suojattavaa tietoa ei kopioida testaus- tai kehitysympäristöön, mikäli niiden suojaustaso on alhaisempi kuin tuotantoympäristön.		Tuotantojärjestelmän on oltava erillinen, jotta kehitys- tai testaustoimet eivät aiheuta tuotantokatkoksia tai turvallisuuspuutteita.Tuotantodataa voidaan kopioida kehitys-/testausympäristöön, mikäli data sanitoidaan siten, että luottamuksellisuus ei vaarannu.
Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?	1) Viranomaisten (esim. CERT-toimijat), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti. 2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat skannataan vuosittain haavoittuvuuksien löytämiseksi.		Esimerkkejä käytännön toteutuksesta: Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen, ja ne asennetaan käyttöjärjestelmiin, verkkolaitteisiin (lähinnä firmwaret), palvelinsovelluksiin jne. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eris-tetyssä testiympäristössä tai pienellä käyttäjäjoukolla. “Merkittäviin muutoksiin” voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien mukaan tuonnit ja/tai vanhojen merkittävät päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne.

Liite 4. KATAKRI II vaatimuksia laitteiston osalta osa I

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Onko tietoliikenneverkon rakenne turvallinen?	1) Ei-luotettuihin verkkoihin ei kytkeydytä ilman palomuuriratkaisua. Erityisesti Internet-verkon on oltava erotettu palomuurilla organisaation tietoverkoista ja -järjestelmistä. 2) Palomuuri- ja VPN- konfiguraatiot ovat organisaation tietoturvaperiaatteiden mukaisia ja dokumentoituja. 3) Tietoliikenneverkko on jaettu vyöhykkeisiin ja segmentteihin asianmukaisesti. Eri suojaustarpeen järjestelmät on sijoitettu erillisille verkkoalueille (esim. DMZ-erottelu). 4) Vyöhykkeisiinjakoperusteet on kuvattu. 5) Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain luvallinen liikenne sallitaan. 6) Valvonnan ja rajoitusten periaatteet on kuvattu. 7) Työasemilla, kannettavilla tietokoneilla ja vastaavilla on käytössä (host-based) palomuuriratkaisu, myös organisaatioverkon sisällä. 8) Fyysinen verkko on jaettu turvavyöhykkeisiin. Käytännössä vaaditaan, että hallitun fyysisen tilan ulkopuolelle menevä liikenne salataan siirrettäessä ST IV –tason (turvallisuusluokitusmerkintä KÄYTTÖ RAJOITETTU) mukaisia tietoaineistoja		
Pääkysymys: Ovatko palomuurien ja vastaavien liikennettä suodattavien laitteiden säännöstöt hyvien tietoturvaperiaatteiden mukaisia?	1) Säännöstöt estävät oletuksena kaiken liikenteen, mitä ei ole erik-seen sallittu (default-deny). Säännöstöt sallivat vain erikseen määritellyn, toiminnalle välttämättömän liikennöinnin. 2) Määrittelemätön liikennöinti on estetty molempiin suuntiin. 3) Organisaatiopalomuurin takana sisäverkossa olevien työasemien, kannettavien tietokoneiden ja vastaavien ohjelmistopalomuurit sallivat vain erikseen määriteltyjen, toiminnalle välttämättömien ohjelmistojen/protokollien liikennöinnin. 4) Estetyt paketit kirjataan lokiin . Mikäli teknisesti mahdollista, kirjauksesta on voitava yksilöidä lähettäjätaho esim. MAC-osoitteen tarkkuudella. 5) Web-selailua suodatetaan toimintavaatimusten mukaisesti. 6) Yleisiin verkkohyökkäyksiin on varauduttu: a) Osoitteiden väärentäminen (spoofing) estetty. b) Liikenne, joka käyttää IP-lisämääreitä (IP options) ja erityisesti lähdereititystä (source routing), on oletuksena estetty kaikissa verkkolaitteissa. c) Proxy ARP -toiminnallisuus on estetty kaikissa verkkolaitteissa. d) Liikenne, jonka lähde- tai kohdeosoite on lähiverkon broadcast-osoite, on estetty. e) Liikenne, jonka lähde- tai kohdeosoitteena on 127.0.0.1 tai 0.0.0.0, on estetty. f) SNMP-liikenne sallitaan vain erikseen määritellyistä lähteistä. g) On määritetty mitä ICMP- liikennettä sallitaan. Erityisesti on huomioitava, että ICMP-tyypin 3 (unreachable) liikenne tulee estetyksi. h) Varattuja osoitteita (RFC 1918) käyttävä liikenne, joka joko saapuu organisaation verkon ulkopuolelta tai suuntaa sinne, on estetty. i) Palomuurit on konfiguroitu kokoamaan sirpaloituneet (fragment) paketit ennen suodatuspäätöksen tekemistä. j) Palvelunestohyökkäysten (DoS, DDoS, roskapostitulva) uhka on arvioitu ja tarpeelliset torjunta- ja ehkäisykeinot toteutettu		
Miten varmistutaan siitä, että liikennettä suodattavat tai valvovat järjestelmät toimivat halutulla tavalla?	1) Organisaatiossa on vastuutettu ja organisoitu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. 2) Suodatussäännöt on dokumentoitu. 3) Palomuurien, reitittimien, IDS-järjestelmien ja muiden liikennettä suodattavien tai valvovien järjestelmien säännöstöt ja haluttu toiminta varmistetaan tarkastuksilla.		
Onko hallintayhteydet suojattu asianmukaisesti?	1)Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. 2)Verkon aktiivilaitteisiin sallitaan hallintayhteydenotot vain erikseen määritellyistä lähteistä tai vain fyysisesti laitteeseen kytkeytymällä.		Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Mikäli verkkolaitteita hallitaan muuten kuin laitteeseen fyysisesti kytkeytymällä, ja mikäli hallintayhteys ei ole fyysisesti eriytetty, hallintaliikenteen tulee olla salattua. Vaatimus voidaan toteuttaa usein helpoiten siten, että estetään verkkolaitteidenhallinta telnetiä käyttäen ja käytetään hallinnassa SSH-yhteyttä. Vastaavasti vältettävä muitakin salaamattomia hallintatoteutuksia (käytettävä esim. HTTPS:ää HTTP:n sijaan web-selaimella hallittavissa järjestelmissä).
Miten verkon aktiivilaitteet on kovennettu? I 502.0 liite katakri versio II	Verkon aktiivilaitteet on kovennettu organisaation yhtenäisen menettelytavan mukaisesti. Käytännössä vaaditaan, että 1) oletussalasanat on vaihdettu, 2) vain tarpeellisia verkkopalveluita on päällä, 3) verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset, 4) hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista, 5) Laitteistot on konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti. 6) Kytkimen työasemaportit on erotettu toisistaan ja työasemat eivät voi suoraan kommunikoida keskenään. Kytkimet eivät saa olla verkkoliikennettä kaiuttavassa toimintatilassa (HUB- toiminnallisuus). 7) Mikäli kytkimissä käytetään VTP-toimialuetta (VLAN Trunking Protocol domain), on VTP-salasana asetettu ja otettu käyttöön. 8) Kytkimissä ei käytetä oletus-VLAN:ia (tyypillisesti VLAN 1) operatiiviselle liikenteelle.		Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Mikäli verkkolaitteen hallinta ei ole mahdollista käyttäjän yksilöivällä käyttäjätunnuksella, tulee yhteiskäyttöisten (ylläpito) tunnusten käyttöön olla sovittu turvalliset käyttösäännöt Mikäli ympäristön koko (lähinnä verkkolaitteiden, erityisesti reitittimien määrä) on suurehko todennuksen järjes-tämiseen suositellaan kahdennettujen AAA-palvelimien (erityisesti TACACS+, RADIUS, tai Kerberos) hyödyntämistä. Huomattava lisäksi, että oletussalasanojen vaihto kattaa myös SNMP:n yhteisösalasanat (Community Strings). Suojaustason IV vaatimuksen 6 menettelylle on valmis-tajakohtaisia nimeämiskäytäntöjä, mm.“private VLAN” ja/tai “protected port.”Suojaustason III vaatimus 1:n toteuttamisessa suositellaan käytettävän kaikkien syötettyjen hallintakomentojen nauhoittamista.

Liite 5. KATAKRI II vaatimuksia laitteiston osalta osa II

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Miten langattomia verkkoja suojataan?	1) "Vierasverkoille", joista ei ole pääsyä organisaation sisäverkkoon, suositellaan, mutta ei vaadita salausta ja käyttäjien tunnistamista. 2) Organisaation hallinnoimien langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. 3) Liikenne salataan luotettavasti.		III- ja II-tasot: Riittävän turvatason käytännön toteutus on usein helpompaa langallisia yhteyksiä käyttäen.
Onko sisäverkon rakenteen näkyminen Internetiin ja muihin ei-luotettuihin verkkoihin estetty?	1) Sisäverkoissa käytetään julkiseen verkkoon kuulumattomia, ns. privaattiosoitteita. 2) Sisäverkon rakenteen ja liikenteen tarpeeton näkyminen on estetty sisäverkossa		
Miten verkkoa, järjestelmiä ja niiden käyttöä valvotaan?	1) Verkkoliikenteen normaali tila (baseline) on tiedossa. On vähintään oltava tiedossa normaalit liikennemäärät ja käytetyt protokollat verkon eri osissa. 2) Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaa- liliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti.		Vaatimukset toimivuudelle normaaliliikenteestä poikkeavilla liikennemäärillä arvioidaan tapauskohtaisesti toiminnan käytettävyysvaatimusten mukaisesti.
Miten IPv6:n turvallisuuteen vaikuttavat erityispiirteet on huomioitu verkoissa ja järjestelmissä?	1) IPv6-toiminnallisuus on huomioitu verkon/järjestelmän kokonaissuunnittelussa järkevästi tai se on poistettu käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa sille ei ole todellista käyttöperustetta. 2) IPv6 Privacy Extensions (RFC 4941) estetty organisaation verkossa, ellei tälle ole todellista toimintaperus- tetta.		Mikäli työasemissa, palvelimissa, verkkolaitteissa tai muissa vastaavissa järjestelmissä käytetään IPv6-toiminnallisuutta, tulee huomioida sen vaikutukset erityisesti liikenteen suodatukseen (palomuurauksen tulee kattaa myös IPv6-liikenne) sekä reititykseen. Huomattava myös, että sisäverkon käyttäjät olisi pystyttävä tunnistamaan jälkikäteen esim. tietoturvaloukkausten selvittelyssä. IPv6 Privacy Extensions voi vaikeuttaa tunnistamista merkittävästi.
Miten reitityksen turvallisuudesta on huolehdittu?	1) Reitityksen sanomat todennetaan. 2) Todennus päällä vyöhykekohtaisesti jokaisen naapurin kanssa. 3) Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen.		
Tunnistetaanko ja todennetaanko käyttäjät ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin?	Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin: 1) Käytössä yksilölliset henkilökohtaiset käyttäjätunnisteet. 2) Kaikki käyttäjät tunnistetaan ja todennetaan. 3) Pääsyä käyttöjärjestelmään valvotaan turvallisen sisäänkirjausmenettelyn avulla. 4) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti. 5) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 6) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen. 7) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/ sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteis- käyttöisille tunnuksille.		Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennus-menetelmä on suojattu välimieshyök-käyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuskredentiaalit ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force –hyökkäyksiä vastaan. Suojaustasojen III ja II vaatimukset vahvasta käyttäjätunnistuksesta voidaan joissain tapauksissa täyttää siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisestä tilasta, jonka pääsynvalvonnassa käytetään vahvaa, kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tieto-järjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.
Onko organisaatiossa menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus? I 502.0 liite katakri versio II	Käytössä on menettelytapa, jolla uudet järjestelmät (työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, ja vastaavat) asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.		Järjestelmäkovennuksissa edellytetään suojaustasollaIII FDCC:tä tai vastaavaa tasoa. Osalle kansainvälisistä aineistoista edellytetään FDCC:tä vastaavaa tasoa jo suojaustasolla IV. Katso kohdennetut vaatimukset liitteen 1 huomautuksista Suojaus-tason II vaatimus voidaan toteuttaa esimerkiksi tiedostojärjestelmän eheyttä tarkkailevalla ohjelmistolla. Lisätietoa löytyy esimerkiksi osoitteesta http://nsrc.org/security/#integrity.
Miten varmistutaan, ettei organisaation verkossa ole luvattomia laitteita tai järjestelmiä?	1) Laitteista pidetään laiterekisteriä, johon kirjataan myös hävitetyt/käytöstä poistetut laitteet. 2) Ohjelmistoista pidetään rekisteriä, johon kirjataan käytössä olevat ohjelmistot ja lisenssit. 3) Konesalit, kytkentäkaapit ja vastaavat tilat tarkistetaan todennettavaan suunnitelmaan pohjautuen säännöllisesti luvattomien lait- teistojen (pakettikaappaimet, key-loggerit, luvattomat langattomat tukiasemat, jne.) löytämiseksi.		Suojaustason III vaatimus 3 voidaan toteuttaa hyödyntämällä esimerkiksi 802.1X-menettelyä. Suojaustason II vaatimusten toteutus voi edellyttää esim. a) laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan, b) peukalointia vastaan suojattujen laitteiden käyttämistä, tai c) jotain vastaavaa menettelyä (esim. käytettävien laitteiden sinetöintiä). Sähkö- ja tietoliikennekaapeloinnin suojausta edellytetään osalle kansainvälisistä aineistoista jo suojaustasolta III lähtien.
Kuinka varmistutaan siitä, että organisaatioon hankittavat laitteistot ovat tietoturvaperiaatteiden mukaisia ja käyttötarkoitukseensa nähden riittävän tietoturvallisia?	Tietoturva-asiat otetaan huomioon laitehankinnoissa. Tulee huomioida ainakin 1) mahdollistaako laite riittävän turvallisen pääsynvalvonnan (esim. puhelin, tulostin, verkkolaite, kannettava tietokone), 2) jääkö käsitellyt dokumentit laitteen muistiin (esim. tulostimet, monitoimilaitteet), 3) mahdollistaako laite muistinsa salakirjoituksen (esim. tulostin, kannettava tietokone, puhelin), 4) tarjoaako laitevalmistaja kuinka hyvää tukea (turvapäivitykset, lisenssi- ja takuuehdot, jne.), 5) mitä muita turvaominaisuuksia laitteessa on, 6) onko laitetta mahdollista muokata itse turvallisemmaksi.		Hankittavalle laitteistolle asetettavat tietoturvavaatimukset riippuvat suuresti laitteen käyttötarkoituksesta. Esimerkiksi tulostimelle voidaan asettaa hyvin erilaisia vaatimuksia riippuen siitä, minkä suojaus-tason aineistojen tulostamiseen sitä käytetään. Vaatimuksia voivat olla esimer-kiksi pääsynvalvonta (pelkkä lukitus vs. käyttäjän tunnistaminen ja todentaminen), lokienkeruun mahdollisuudet, muistin/ kiintolevyn salauksen ja tyhjennyksen mahdollisuudet, kytkentä (paikallinen vs. verkkotulostin), verkkoliikenteen salaus, etähallinnan turvaratkaisut, hajasäteilysuojaukset, jne.

Liite 6. KATAKRI II vaatimuksia laitteiston osalta osa III

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Onko huolehdittu, että organisaatiolla on toimintaansa nähden riittävät jatkuvuuden varmistavat suunnitelmat?	1) Järjestelmien käytettävyysvaatimukset on määritetty. 2) On varmistettu, että kriittisten verkkojen (ml. Internet- yhteys), verkkolaitteiden, tietojärjestelmien, palvelinten ja vastaavien vikaantumisesta pystytään toipumaan toimintavaatimuksiin nähden riittävässä ajassa. 3) Suunnitelmissa otetaan huomioon suojattavien tietojen suojaus hätätilanteissa. Suojauksen on katettava tiedon luottamuksellisuus, eheys ja käytettävyys. 4) Suunnitelmiin sisältyy ennalta ehkäiseviä ja vaarantumistilanteen korjaamistoimenpiteitä.		
Onko organisaatiossa selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita?	1) Käytössä on selkeät peri- aatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja oheislaitteita. 2) Periaatteiden noudattamista valvotaan ja varmistetaan teknisin keinoin (esimerkiksi rajoittamalla asennus- ja asetusten muokkausoikeus vain ylläpitäjille). 3) Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä. 4) Organisaatiossa on olemassa uusien järjestelmien, järjestelmäpäivitysten ja vastaavien hyväksymiskriteerit. Vain hyväksymisprosessin läpäisseitä verkkoja ja järjestelmiä käytetään . 5) Suojattavan tiedon käsittelyyn käytetään vain viranomaisen hyväksymiä verkkoja ja järjestelmiä.		Korkeiden käytettävyysvaatimusten ympäristöille vaaditaan jatkuvuus-/toipumissuunnitelmaa, ja suunnitelman säännöllistä testaamista.
Miten varmistetaan, että verkossa ja sen palveluissa ei ole tunnettuja haavoittuvuuksia?	1) Viranomaisten (esim. CERT-toimijat), laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset turvapäivitykset asennetaan hallitusti. 2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat skannataan vuosittain haavoittuvuuksien löytämiseksi.		Esimerkkejä käytännön toteutuksesta: Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen, ja ne asennetaan käyttöjärjestelmiin, verkkolaitteisiin (lähinnä firmwaret), palvelinsovelluksiin jne. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eristetyssä testiympäristössä tai pienellä käyttäjäjoukolla."Merkittäviin muutoksiin" voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien mukaan tuonnit ja/tai vanhojen merkittävät päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne.
Miten varmistutaan siitä, että työskentelytauoilla tai työskentelyn jälkeen laitteet eivät jää ilman riittävää suojaa?	1) Käyttäjät velvoitetaan seuraavantapaiseen käytäntöön: a) Työasema, pääte, kannettava tietokone tai vastaava lukitaan aina (esim. salasanasuojatulla näytönsäästäjällä tai muulla menettelyllä), kun laitteelta poistutaan. b) Aktiiviset istunnot päätetään työn päättyessä ja pitemmillä tauoilla (esim. etäyhteydet ja palvelinistunnot puretaan). c) Laitteesta/järjestelmästä kirjaudutaan ulos työn päättyessä. 2) Mikäli suojattavaa tietoa sisältävä laite joudutaan jät- tämään tilaan, jossa siihen on fyysinen pääsy ei-luotetuilla (arvioitava tapauskohtaisesti: esim. organisaation ulkopuolisilla), suojaus on aktivoitava laitteelta poistuttaessa (esim. sammuttamalla kannettava tietokone, jolloin salaus aktivoituu).		
Ovatko näyttöpäätteet asetetut siten, ettei suojattavaa tietoa paljastu ohikulkijoille tai muille asiattomille?	1) Näyttöpäätteet on asetettu harkiten siten, ettei tieto paljastu asiattomille. 2) Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuoja.		Näyttösuojaa ei vaadita, mikäli kannattavaa tietokonetta käytetään vain suojatussa tilassa vastaavasti kuin työaseman näyttöäkin.

Liite 7. KATAKRI II vaatimuksia tilojen osalta I

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Rakenteelliset ratkaisut			
Elektronisen tiedustelun huomioiminen parkkipaikalta tai tiestöltä	Ei vaatimuksia		
Elektronisen tiedustelun huomioiminen lastaus- ja purkualueelta	Ei vaatimuksia		
Seinä-, katto- ja lattiamateriaalit	Kuoren rakenne normaalia toimistorakennetta.		
Onko ikkunoita alle 4m korkeudella?			Heikoista ikkuna-aukoista on helpompi murtautua kuin ovesta.
Onko tilan kuoressa muita aukkoja, joita voitaisiin käyttää tunkeutumiseen?	Ei vaatimuksia		IV- ja kaapeli-kanavia, savunpoisto- ja ilmanottoaukkoja voidaan käyttää tunkeutumiseen.
Minkälaiset ovat tilaan johtavat ovet?	Ovien äänieristyksen tulee olla sellainen, että asiattomat eivät pääse kuulemaan työtilassa käytyjä keskusteluja.		Kaksilehtisten ovien osalta omat vaatimukset: kysy yksityiskohdat valtionhallinnon vastuuviranomaisilta. Ovirakenteet: murtosuojattujen ovien osalta on suosituksena käyttää ns. kombi-ovia, joissa on huomioitu ääneneristyksen lisäksi myös paloturvallisuusvaatimukset
Äänen liikkuminen naapuritiloihin	Tilan äänieristyksen tulee olla sellainen, että asiattomat eivät pääse kuulemaan työtilassa normaaliäänellä käytyjä keskusteluja.		Suojattavasta tilasta ei saa välittyä puhetta suojaamattomiin naapuritiloihin.
Kassakaappi tai holvi tiloissa	Tilassa kassakaappi (ei standardivaatimusta), tai jos suojaustason IV tietoaineistoa säilytetään lukitussa kaapissa, tulee tila olla valvottu rikosilmoitinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovet ja tilat valvottava.		
Minkälainen tilan lukitus on?	Tilan lukituksen on oltava kunnossa. Tila on lukittava aina, kun se ei ole miehitetty. Käyttölukko vyöhykkeen rajalla FK:n varmuusluokka 3.		Lukot on luokiteltu eri tasoihin murtosuojan perusteella.
Onko LVIS-järjestelyt varmistettu niin, että ne vastaavat organisaation toimintavaatimuksia?	1) LVIS-järjestelyt on varmistettu toimintavaatimusten mukaisesti. 2) Kriittiset laitteistot on tunnistettu ja varmennettu toimintavaatimusten mukaisesti		Määritykselläkin "toimintavaatimusten mukaisesti" tarkoitetaan sitä, että mikäli järjestelmän käytettävyysvaatimukset ovat korkeat, soveltuvia varmistuksia vaaditaan. Varmistukset voivat käytännössä tarkoittaa esimerkiksi tärkeiden laitteiden ja laitetilojen suojaamista ympäristötekijöitä vastaan (mm. murto, palo, lämpö, kaasut, pöly, tärinä, vesi). Varmentavia toimia voivat olla myös toimintakriittisten laitteistojen kahdentaminen ja/tai varustaminen häiriöttömällä sähkönsyötöllä (UPS). Korkeiden käytettävyysvaatimusten järjestelmille vaaditaan varmennusten toiminnan säännöllistä testaamista.

Liite 8. KATAKRI II vaatimuksia tilojen osalta II

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Valvontajärjestelmät			
Onko tilassa rikos-ilmoitinjärjestelmä?	Tila on valvottu rikosilmoi- tinjärjestelmällä (rikosilmoitinkeskuksen taso oltava vähintään 2-luokka FK). Ovia ja tiloja valvotaan. Järjestelmää tarvitaan, jos suojaustason IV luokiteltua aineistoa säilytetään tavallisessa lukitussa kaapissa/ laatikossa.		Rikosilmoitinjärjestelmäantaa ilmaisun ja käynnistää vastatoimenpiteet.
Onko tilassa kulun-valvontajärjestelmää?	Tila on valvottava kulunvalvonnalla siten, että vain hankkeeseen tai projektiin oikeutetuilla henkilöillä on pääsy tilaan, ja että tilaan kulku voidaan myöhemmin todentaa.		Suojattuun tilaan kulku voidaan myöhemmin todentaa.
Onko tilassa kamera-valvontajärjestelmä?			Palvelintilan kameravalvonnalla nostetaan oman henkilöstön kynnystä luvattomaan toimintaan.
Onko palvelintilassa kameravalvontajärjestelmä?	Ei vaatimuksia.		Palvelintilan kameravalvonnalla nostetaan oman henkilöstön kynnystä luvattomaan toimintaan.
Onko rikosilmoitinjärjestelmä toimintakunnossa?	Järjestelmä on toimintakuntoinen		Toimimattomasta rikosilmoitinjärjes-telmästä ei ole hyötyä. Vastaako vartioinnin vasteaika ja vartijan toiminta sopimusta? Liian pitkä vasteaika tai vartijan virheellinen toiminta poistaa rakenteellisella suojauksella saavutettua turvaa.
Miten kulunvalvonta-järjestelmän hallinnointi on järjestetty?	Ei vaatimuksia.		Kulunvalvontajärjestelmänhallinnoija voi luoda tai poistaa turvatilan kulkutunnisteita sekä ohjata ovia etäkäyttöisesti.
Miten rikosilmoitinjärjestelmän hallinnointi on järjestetty?	Ei vaatimuksia.		Kulunvalvontajärjestelmänhallinnoija voi luoda tai poistaa turvatilan kulkutunnisteita sekä ohjata ovia etäkäyttöisesti.
Miten LVI-automaation hallinta on järjestetty?	Ei vaatimuksia.		LVI-automaation etähallinnan avulla voidaan tilan olosuhdemuutoksilla vahingoittaa laitteita ja tietoa.
Käyttöoikeudet			
Pääsyoikeuksien hallinta	Pääsyoikeudet ko. tiloihin myöntää nimetty vastuuhenkilö.		Tiloihin liittyvien pääsyoikeuksien tulee olla prosessissa yksiselitteisesti vastuutettu.
Hallitaanko kaikkien käyttäjien pääsy- ja käyttöoikeuksia hyvän tiedonhallintatavan mukaisesti?	1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö. 2) Järjestelmän käyttäjistä on olemassa lista. 3) Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtä-viensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tie-toihin ja järjestelmiin. 4) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. 5) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. 6) On olemassa selkeä ja toimiva tapa henki-löstössä tapahtuvien muutosten ilmoitta-miseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. 7) Käyttö- ja pääsyoikeuksien muutokset välittyvät sekä fyysiseen että loogiseen pääsyyn ja käyttöön. 8) Käyttö- ja pääsyoikeudet katselmoidaan säännöl-lisesti. 9) Yhteistyökumppanien/ muiden ulkopuo-listen oikeutetusta henkilöstöstä on olema-ssa oma rekisterinsä. 10) Jokaisesta myön-netystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).		Voidaan käytännössä toteuttaa esimerkiksi siten, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esim. 6 kuukauden välein. Lisäksi muutoksissa, kuten ylennyksissä, alennuksissa, työn-kierron yhteydessä ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuu-henkilöille, jolloin kaikki oikeudet saadaan pidettyä sopivina. Tämä voi tarkoittaa käytännössä esimerkiksi sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen.

Liite 9. KATAKRI II vaatimuksia tilojen osalta III

	Käyttörajoitettu ST 4	TÄYTTÄÄKÖ JST	Huomioita
Miten (mekaanisten) avainten hallinta on järjestetty?	Avainten / kulkuoikeuksien hallinta on oltava kunnossa. Asiaa hoitaa vastuuhenkilö ja hänellä on luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortti.		Tilan hallinnan vuoksi on tarkastettava myös ylimääräisten avainten säilytys, sekä lisäavainten hallittu teettäminen.
Kenellä suojattavaan tilaan on avaimia?	Vain nimetyillä saa olla avaimet / kulkuoikeudet suojattuihin työskentelytiloihin.		Tilan hallinnan vuoksion aina tiedettävä kenellä avaimia suojattavaan tilaan on.
Mihin tiloihin yleisavaimella pääsee?	Ei vaatimuksia.		Yleisavaimella ei pääse suojattuun tilaan.
Onko vartiointi- ja kiinteistönhoitohenkilöstölle jaettu avaimia suojattuun tilaan?	Ei vaatimuksia.		Vartiointi- ja kiinteistönhoitohenkilöstöllä ei saa olla hallitsematonta pääsyä suojattavaan tilaan.
Miten tilan huoltotoimenpiteet on ohjeistettu tapahtuvaksi?	Ei vaatimuksia.		
Tapahtuvatko laitetilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet vain valvottuina?	Tilan ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain suojaustasolle hyväksytyn henkilön toimes- ta tai oman henkilökunnan valvonnassa.		
Miten on varauduttu salakuunteluun, hajasäteilyyn ja vastaaviin uhkiin?	1) Tilojen äänieristyksen täytyy olla riittävä, jottei normaali puheääni kuulu sellaisen tilan ulkopuolelle, jossa keskustellaan suojattavista asioista. 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakka-kopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista. 3) Huoneen ovet ja ikkunat on pidettävä kiinni keskusteltaessa suojattavista asioista.		Elektronisten laitteiden vientikielto voidaan joissain tilanteissa korvata esim. irrottamalla akut. Käsiteltäessä kansainvälisen yhteisön (esim. EU) turvaluokiteltua tietoa, hajasät-eilysuojaus vaaditaan pääsääntöisesti suojaustasolta III (Confidential) lähtien. Käsiteltäessä kansallista tai yksittäisen toisen valtion turvaluokiteltua tietoa, hajasäteilysuojaus edellytetään yleensä joko suojaustasolta III (Confidential) tai suojaus-tasolta II (Secret) lähtien. Hajasäteilyltä suojautuminen on hoidettava toimitilan fyysisen sijainnin valinnalla, vuorauksella tai käyttämällä suojattu- ja laitteistoja ja kaapelointeja.
Vierailijat			
Millaisia menettelytapoja organisaatiolla on tunnistaa ulkopuoliset työntekijät sekä vierailijat?	1) Henkilöstö on ohjeistettu vierailijoiden isännöintiä varten		Näkyvät tunnisteet eivät tarpeen jos organisaatiossa työskentelee vain muutama henkilö, jotka varmasti tuntevat toisensa ja toistensa työsuhteiden keston. Vieraat voivat jäädä valvomatta julkisiin tiloihin.