HAAGA-HELIA
ammattikorkeakoulu

Tietoturvakartoitus yritys X:lle

Mikko Saarnisto

Opinnäytetyö

25.11.2012

HAAGA-HELIA ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

Tiivistelmä

25.11.2012

Tekijä tai tekijät Mikko Saarnisto	**Ryhmätunnus tai aloitusvuosi** 2009
Raportin nimi Tietoturvakartoitus yritys X:lle	**Sivu- ja liitesivumäärä** 43+14
Opettajat tai ohjaajat Titta Ahlberg	

Tässä työssä keskityttiin tietoturvallisuuden aihepiiriin. Tutkimuksen teoreettisena tavoitteena oli selvittää, mitä on tietoturva, mitä ovat tietoturvatasot ja millaiset ovat perustason tietoturvavaatimukset sekä miten tietoturvakartoitus tehdään konsultin näkökulmasta katsoen. Käytännön tavoitteena oli kartoittaa kohdeyrityksen tietoturvallisuuden nykytila ja kartoituksen perusteella parantaa yrityksen tietoturvallisuutta.

Tutkimus tehtiin toimeksiantona liiketoiminnan kehityspalveluita tarjoavalle yritykselle.

Tutkimuksen teoriaosassa tutkittiin tietoturvallisuuden käsitteistöä. Tietoturvallisuus prosessiin luotiin katsaus jossa esiteltiin tietoturvakartoitus sekä tietoturvatasot. Tietoturvallisuuden perustason vaatimukset selvitettiin ja katselmoitiin yrityksen tietoturvallisuuden kannalta tärkeimpiä dokumentteja. Tietoturvakartoitusta avattiin konsultin näkökulmasta katsoen.

Empiirinen tutkimus jaettiin kahteen osaan. Ensimmäisessä osassa selvitettiin kohdeyrityksen tietoturvan nykytila kyselytutkimuksella. Toisessa osassa arvioitiin yrityksen liiketoimintaprosesseja. Valitulle ydinprosessille tehtiin suppea riskikartoitus. Kartoituksen pohjalta annettiin suosituksia ja korjausehdotuksia tietoturvallisuuden parantamiseksi yrityksessä.

Asiasanat
tietoturva, tietoturva kartoitus, riskianalyysi, tietoturvatasot

HAAGA-HELIA
University of Applied Sciences

Abstract

25.11.2012

Degree programme in Information Technology

Authors Mikko Saarnisto	**Group or year of entry** 2009
The title of thesis Information security assessment for a company X	**Number of pages and appendices** 43+14
Supervisor(s) Titta Ahlberg	

The theoretical objective of this thesis was to clarify the concept of information security. The study focused on looking into what information security levels are and what the information security demands of the basic level are like and how the information security assessment is made from a consultant's point of view. The practical objective was to assess the present state of the information security of the target company and to improve the information security of the company on the basis of the assessment. The study was assigned by a company that offers development of business services for other companies.

In the theoretical part of the study, the concepts of the information security were studied. A view to the information security process, including information security assessment, was created. In addition, the information security levels were defined.

Furthermore, the demands for the basic level of the information security were clarified and the most important documents from the point of view of the information security of the company were inspected. The information security assessment was investigated from the consultant's point of view.

The empiric part of the study was divided into two parts. In the first part, the target company's present state of the information security was clarified with a questionnaire survey. In the second part, the business processes of the company were evaluated. Additionally, a small risk survey was carried out to a chosen core process.

Based on the completed information security assessment, recommendations and correction proposals were given to improve the information security in the target company.

Key words
information security, security analysis, information security assessment, risk analysis, information security levels

Sisällys

Sanasto

Bugi, Ohjelmointi virhe, joka aiheuttaa epävakauden ohjelmassa esim. kaatamalla sen

Haavoittuvuus, tietoturvallisuutta uhkaaville tekijöille alttius, heikkoudet ja puutteet suojauksissa ja turvatoimissa

Kypsyys, kyky ohjata tietoturvatoimintaa

Kyvykkyys, kyky ohjata yksittäisen prosessin toimintaa

Riski, uhkan toteutumisen todennäköisyys aiheuttaa tietty menetys, rahallinen tai odotusarvo (arvo x todennäköisyys)

ROI, Eng. Return of Investment, investoinnin tuotto aste.

ROSI, Eng. Return on Security Investment, Tietoturva investoinnin tuotto, lasketaan seuraavan kaavan mukaisesti.
(R-E) + T = ALE
R-ALE = ROSI, jossa
R = vuosittainen euromääräinen summa, joka olisi maksettava vuosittain ilman investointia.
E = säästöt joita saadaan vuodessa käyttämällä investointia.
T = tietoturvainvestoinnin hinta.
ALE = vuosittainen tappio arvio (Annual Loss Expectancy)

SLA, Eng. Service level agreement. Palvelutasosopimus

Tietoturvapoikkeama, tahaton tai tahallinen tapahtuma, jonka seuraksena yrityksen vastuulla olevien tietojen tai palvelujen eheys, luottamuksellisuus tai käytettävyys on tai saattaa olla vaarantunut

Tietoturvauhka, tietoturvaan kohdistuva sisäinen tai ulkoinen uhka

Tietoturvataso, kuvaa kykyä ohjata tietoturvatapahtumia tietyllä tasolla

Tietovara, Eng. information asset on omaisuuserä, resurssi, prosessi, tuote, tietojenkäsittelyinrastruktuuri ja niin edelleen jonka yritys on päättänyt suojata.

Ydinprosessi, suoraan asiakkaalle arvoa tuottava prosessi

1 Johdanto

Tieto on yksi tärkeimpiä voimavaroja joista yritys saa arvoa toiminnalleen. Tämän tiedon tulee olla paikkaansa pitävää, oikea-aikaista ja täydellistä jotta sillä olisi arvoa yritykselle. Arvokkaat tiedot tulee suojata niin, etteivät ne päädy kilpailijalle tai ulkopuolisten haltuun. Tietoturvallisuudessa on kyse nimenomaan tiedon suojaamisesta. Tiedon suojaamisen tulee olla kokonaisvaltainen prosessi. Ei riitä, että dokumentti jolla tieto sijaitsee suojataan salasanalla, vaan koko tietojärjestelmä ja sitä ympäröivä infrastruktuuri tulee olla riittävän hyvin uhkilta suojattu.

Työn lähtökohtana on tutkia mitä on tietoturvallisuus ja miten tietoturvakartoitus tehdään konsultin näkökulmasta katsoen, käyttäen apuna kirjallisia lähteitä sekä selvittää yritys X:n tietoturvallisuuden nykytila sekä miten sitä on mahdollista kehittää. Tarve työlle on lähtenyt yritys x:n halusta kartoittaa ja parantaa tietoturvallisuuttaan sekä ennalta ehkäistä tietoturvaongelmia.

Tietoturvakartoitusta on tarkoitus tutkia niin, että tutkimuksen pohjalta on mahdollista kehittää PK-yritysten tietoturvallisuutta tutkiva metodi.

Työ rajataan koskemaan hallinnollista turvallisuutta, henkilöstöturvallisuutta, tietoaineisto turvallisuutta sekä laitteistoturvallisuutta.

2 Tutkimusongelmat

Kirjallisuuteen perustuva tutkimus selvittää mitä on tietoturva sekä mitä ovat tietoturvatasot, että miten tietoturvallisuudenkartoitus tehdään ulkopuolisen konsultin näkökulmasta katsoen.

Empiirisen tutkimisen osassa selvitetään millainen on yritys X:n tietoturvan nykytila ja miten sitä on mahdollista kehittää.

3 Tietoturvallisuus

Jotta tietoturvan laajaa aihepiiriä voisi ymmärtää, tulee sitä avata perehtymällä tietoturvallisuuden taustaan ja osa-alueisiin.

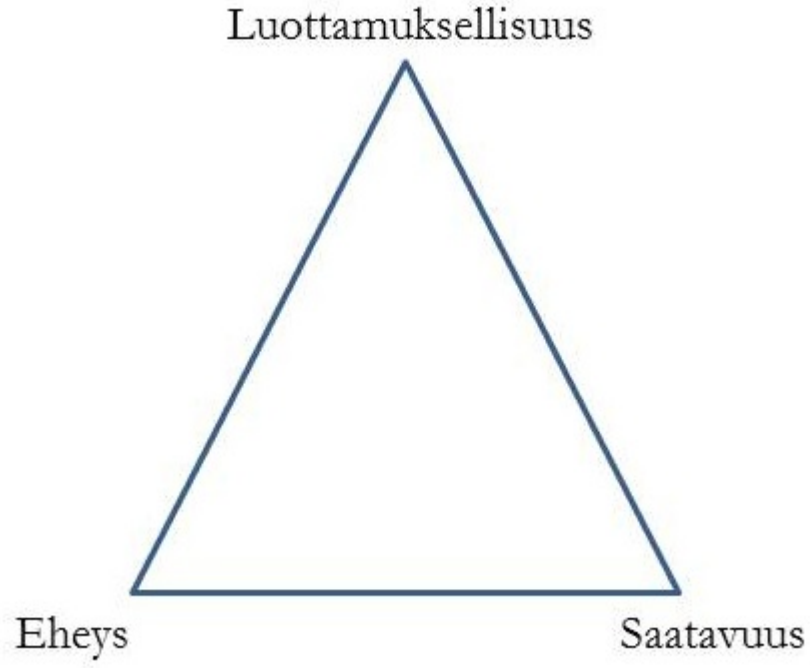
3.1 Tietoturvallisuuden määritelmä

Tietoturvallisuus on perusta, jolle tärkeiden ja luottamuksellisten tietojen käsittely rakentuu. Monille tietoturvasta tulee mieleen jokin toimenpide, kuten varmuuskopiointi tai jokin ohjelma, kuten virusskanneri. Nämä kuuluvat olennaisesti tietoturvaan mutta ovat vain pieni osa sitä. Usein tietoturva mielletään tekniseksi ratkaisuksi, vaikka tietoturvan muut osa-alueet kuuluvat erottamattomasti yhteen. Laajasti ymmärrettynä tietoturvallisuus kattaa kaiken sen, mikä liittyy tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuden säilymiseen käsittelyn, säilytyksen ja tiedonsiirron aikana (Järvinen2002, 21).

Liiketoiminnan kannalta katsottuna tietoturvallisuus tarkoittaa tiedon suojaamista monenlaisilta uhkilta tarkoituksena varmistaa liiketoiminnan jatkuvuus, minimoida liiketoiminnalliset riskit sekä maksimoida investoinneista ja liiketoiminnan mahdollisuuksista saatu tuotto (SFS. 2006, 14).

Tietosuoja liittyy läheisesti tietoturvallisuuteen. Termiä kutsutaan usein myös yksityisyyden suojaksi. Tietosuojavaltuutetun mukaan tällä tarkoitetaan ihmisten yksityiselämän suojaa sekä muita sitä turvaavia oikeuksia henkilötietoja käsiteltäessä. (Tietosuojavaltuutetun toimisto 2010.) Järvinen rajaa termit tarkoittamaan ihmisen henkilötietojen sekä henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista (Järvinen 2010, 15). Luottokorttia käytettäessä liikutaan sekä tietoturvan että tietosuojan osa-alueilla. Pitämällä kortti sekä tunnusluku visusti poissa ulkopuolisten katseilta toimitaan tietoturvallisesti ja tämä parantaa yksityisyyden suojaa.

Klassisen tiedonarvoon perustuvan määritelmän mukaan tietoturvallisuus koostuu kolmesta osatekijästä, luottamuksellisuus (Confidentiality), eheys (Integrity) sekä saatavuus (Availability). Näistä muodostuu helppo muistisääntö CIA, sanojen englanninkielisten alkukirjainten mukaan. Alla esitellään CIA kolmio, sen sakarat edustavat kuta-



rvinen 2002,

Kuvio 1. CIA kolmio

3.2 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä. (Hakala ym. 2006, 4). Luottamuksellisuus on tietoturvan tärkein tukipilari ja osatekijä. Luokittelemalla tieto voidaan määritellä sille käyttäjät. Jotta valtuutetut käyttäjät voidaan tunnistaa, tulee heidät ensin todentaa (Järvinen 2002, 22). Todennus voidaan tehdä monin eri tavoin, esim. salasanoilla, sormenjäljillä, esineillä tai silmän pohjan kuvauksella.

Luottamuksellisuutta voidaan suojata esimerkiksi salaamalla tieto tai sijoittamalla se siten, että ulkopuoliset eivät pääse siihen käsiksi. (Hakala ym. 2006, 4). Salaisen aineiston päätyminen sellaisten henkilöiden käsiin jolla ei ole oikeutta aineistoon, on esimerkki luottamuksen menettämisestä. Hallussapidon luokkaamista ei pidä sekoittaa luottamuksellisuuden menettämiseen, salaisen aineiston päätyminen oikeudettomalle henkilölle on esimerkki hallussapidon loukkaamisesta.

3.3 Eheys

Eheys tarkoittaa sitä, että tietojärjestelmän sisältämät tiedot pitävät paikkansa eivätkä sisällä tahallisia tai tahattomia virheitä. (Hakala ym. 2006, 4). Järvisen mukaan eheys tarkoittaa sitä, ettei mikään ulkopuolinen taho pysty luvatta muuttamaan tiedon sisältöä

(Järvinen 2002, 22). Tietojen muutos käsittää tiedoston sisällön muuttamisen, tiedoston poistamisen sekä tiedoston vahingoittumisen. Lyhyesti sanottuna eheys on sitä, että tieto säilyy muuttumattomana.

Eheys voi rikkoontua monin eri tavoin, Www- sivujen eheys rikotaan laittamalla sivuille alun perin kuulumatonta aineisto näkyviin. Tiedostojen eheyden rikkovat usein vialliset tallennusmediat. Virukset rikkovat tiedostojen eheyden tarttumalla niihin.

Eheyteen pyritään vaikuttamaan pääasiassa ohjelmistoteknisin ratkaisuin. Tiedostossa olevaa tietoa ja sen siirtoa voidaan suojata tarkastussumman avulla. Sovelluksiin ohjelmoidaan erilaisia tarkisteita ja syöttörajoitteita. Virus- ja haittaohjelmien torjuntaan tarkoitetut sovellukset turvaavat omalta osaltaan eheyttä. (Hakala ym. 2006, 5)

3.4 Saatavuus

Saatavuudella eli käytettävyydellä tarkoitetaan sitä, että palvelut ja tiedot ovat käytettävissä silloin, kun niitä tarvitaan. Hakala ym. mainitsevat kirjassaan käytettävyyden merkitsevän sitä, että sekä palvelut että tiedot ovat saatavilla tietojärjestelmästä oikeassa muodossa ja riittävän nopeasti. (Hakala ym. 2006, 4).

Verkossa olevan palvelun tulisi olla saatavilla vuorokauden jokaisena hetkenä, seitsemänä päivänä viikossa. Palvelua saatetaan tahallisesti kuormittaa erilaisilla hyökkäyksillä, jolloin palomuurin tulee olla kunnossa.

Toisinaan saatetaan tarvita tietoa, joka on varastoituna vanhoihin, jopa kymmeniä vuosia vanhoihin tiedostoihin. Vaikka tiedot olisivatkin kunnossa, saattaa teettää vaikeuksia integroida nykyisiä systeemejä vanhojen tiedostomuotojen tai tallennusmedioiden kanssa. Tärkeät tiedot on varmuuskopioitava riittävän usein, jotta yhteensopivuus tiedostojen ja järjestelmien kanssa pystytään takaamaan. Tärkeätä on myös varmistaa katkeamaton virransyöttö järjestelmiin esim. UPS-laitteen avulla.

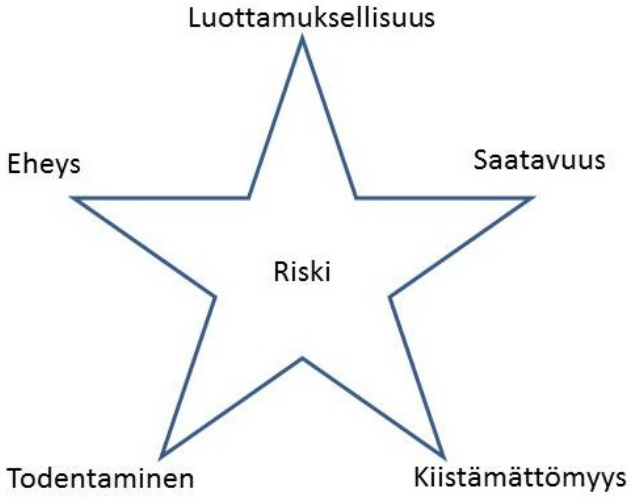
3.5 Muut tietoturvallisuuden osatekijät

Luottamuksellisuus, eheys ja saatavuus muodostavat tietoturvallisuuden perustan, niin sanotun CIA kolmion. Tätä klassista mallia pidetään nykyään riittämättömänä. Useat eri lähteet esittävät laajennuksia tähän malliin. Hakala ym. sekä Raggad esittävät osatekijöihin kahta lisätekijää, kiistämättömyyttä ja todennusta. (Hakala ym. 2006, 5.),(Raggad 2010, 22).

Todentamisella varmistetaan, että käyttäjä, laite tai tiedon alkuperä on juuri se, mikä pitääkin. Käyttäjät todennetaan useimmiten salasanan perusteella. Nykyään myös biometrinen tunnistaminen on lisääntynyt. Ihmisen on vaikea todentaa laitetta, kun taas toinen laite voi helposti todentaa toisen laitteen sen osoitteen perusteella. Verkossa oleva tieto on vaikeata todentaa, koska sen alkuperä on hankala selvittää. (Järvinen 2002, 27.)

Kiistämättömyys tarkoittaa sitä, että järjestelmä pystyy luotettavasti tunnistamaan ja kirjaamaan käyttäjän tiedot talteen. Kiistämättömyyden tarve tulee hyvin esille elektronisessa kaupankäynnissä. Myyjän on kiistämättömästi pystyttävä näyttämään, kuka tilauksen on tehnyt. Todennus liittyy läheisesti kiistämättömyyteen. Tiedonsiirrossa kiistämättömyys tarkoittaa sitä että kumpikaan ei pysty kiistämään osallisuuttaan tiedonsiirtoon. Lähettäjä ei pysty kiistämään viestin lähetystä eikä vastaanottaja voi kiistää viestin saapumista. Internetissä digitaalista allekirjoitusta voidaan käyttää varmistamaan kiistämättömyys. (Raggad 2010, 23.)

CIA kolmio ja siihen lisätyt todennus sekä kiistämättömyys muodostavat tietoturvallisuus tähden siten että tähden jokainen sakara edustaa tietoturvallisuus tavoitetta ja tähden ydin riskiä. (Raggad 2010, 22.)



Kuvio 2. Tietoturvallisuus tähti (Raggad 2010,22)

3.6 Tietoturvan osa-alueet

Tietoturvan osa-alueet voidaan pilkkoa helpommin käsiteltäviksi osiksi. Eri lähteet luokittelevat osa-alueita hieman eri tavoin, koska niitä käsitellään eri näkökulmista. Tässä työssä käytetään yleisesti käytössä olevaa kahdeksaan eri toimenpide-alueeseen tapahtuvaa jakoa:

- Hallinnollinen turvallisuus
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus (Viestintävirasto 2009; Vahti 8/2006.)

3.6.1 Hallinnollinen tietoturvallisuus

Hallinnollisella tietoturvalla tarkoitetaan organisaatiossa noudatettavia tietoturvallisuuden organisointia, periaatteita ja toimintalinjoja. Hallinnollisen tietoturvan tehtävänä on tietoturvaperiaatteiden ja toimintalinjojen määrittely, toimintojen organisointi, johdon ja henkilöstön sitoutuminen tietoturvallisuuteen sekä toiminnan jatkuvuuden turvaaminen. Organisaation tietoturvallisuuden hallintajärjestelmä toimii hallinnollisen tietoturvan kulmakivenä. (Viestintävirasto 2004, Suositus määräyksen 47B/2004M soveltamisesta teleyrityksen tietoturvasta. 4.)

Tieturvallisuuden hallintajärjestelmä rakennetaan standardien pohjalta. Suomessa käytössä ovat SFS ISO/IEC 27001 ja SFS ISO/IEC 27002 (korvaa SFS 2006. ISO/IEC17799:fi standardin). Ensimmäinen auttaa luomaan järjestelmän, ja toisessa ohjeistetaan tietoturvan hallinnan menettelyä.

3.6.2 Henkilöstöturvallisuus

Henkilöturvallisuudella tarkoitetaan henkilöstöön liittyvien tietoturvariskien hallintaa, sen tavoitteena on torjua henkilöstöstä organisaation toiminnalle aiheutuvia uhkateki-

jöitä (Viestintävirasto 2004, Suositus määräyksen 47B/2004M soveltamisesta teleyrityksen tietoturvasta, 4).

Käytännön toimina henkilöstöturvallisuuteen kuuluvat henkilöstön taustojen selvittäminen turvallisuusselvityksen avulla, salassapitosopimukset sekä varamiesjärjestelyt.

3.6.3 Fyysinen turvallisuus

Fyysinen tietoturvallisuus käsittelee uhkia, jotka kohdistuvat toimitiloihin ja niihin sijoitettuihin laitteisiin. Fyysisiä uhkia ovat esim. murto, varkaus, tulipalo, luonnon mullistus, vesivahinko sekä erilaiset onnettomuudet. (Hakala ym. 2006, 11.)

Uhkia voidaan pienentää esim. lukitsemalla tilat, palo- ja sammutusjärjestelmällä sekä kulunvalvontajärjestelmällä. Usein fyysisen turvallisuuden ylläpidosta vastaavat yrityksen ulkopuoliset henkilöt, kuten vartijat tai huoltomiehet.

3.6.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus on viestintäverkoissa välitettävien viestien luottamuksellisuuden, eheyden ja käytettävyyden turvaamista (Viestintävirasto 2004, 7). Vahtiohjeistuksen mukaan tietoliikenneturvallisuutta ylläpitäviä keinoja ovat mm. verkonhallinta, laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. (Vahti 7/2003, 57.)

3.6.5 Laitteistoturvallisuus

Valtionhallinnon tietoturva käsitteistön mukaan laitteistoturvallisuudella tarkoitetaan, ”tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.” (Vahti 4/2003, 23.)

3.6.6 Ohjelmistoturvallisuus

Valtiovarainministeriön laatimien Valtionhallinnon tietoturvallisuuden johtoryhmän Vahti-ohjeiston mukaan ”ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistamis-, suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä. ” (Valtiovarainministeriö Vahtiohjeet 2009.)

3.6.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan eri tallennusmuodoissa olevien dokumenttien käytettävyyden, eheyden ja luottamuksellisuuden varmistamista. Dokumentti voi olla esim. asiakirja, kuva tai tiedosto.

Tietoaineistonturvallisuuden perustana käytetään tietoaineiston luokittelujärjestelmää, joka sisältää ohjeet tietoaineiston käsittelystä. Luokitusjärjestelmän pitää antaa ohjeistus muun muassa seuraaviin asioihin:

- Mitä tietoa yrityksessä käsitellään?
- Millaisia eri turvaluokkia on käytössä?
- Kuka tietoa saa käyttää?
- Miten tieto säilytetään, siirretään, kopioidaan, jaellaan ja tuhotaan? (Viestintävirasto 2004, 11.)

3.6.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan tietojenkäsittelypalveluiden asianmukaisen ja turvallisen käytön varmistamista (SFS ISO/IEC 17799, 2006, 80). Käyttöturvallisuus käsittää käytettävien ohjelmistojen riittävän osaamisen, riittävän käsityksen yrityksen tietoturvakäytännöistä ja menettelytavoista.

4 Tietoturvatasot

Tietoturvatasot kuvaavat yrityksen kykyä ohjata tietoturvatapahtumia. Tietoturvatasot mitoitetaan yrityksen toimintaan kohdistuviin riskeihin ja uhkiin. Yrityksen johdolla tulee olla näkemys ja ohjeistus siitä, millainen on tietoturvallisuuden rooli yrityksessä. Johdon tulee määrittää resurssit ja kohdistaa ne yrityksen toiminnan kannalta oikeisiin kohteisiin. Tällaista yrityksen kykyä ohjata tietoturvatoimintaa kutsutaan termillä kypsyys. Termi kyvykkyys kuvaa yrityksen kykyä ohjata yksittäisen prosessin toimintaa. (Valtiovarainministeriö tietoturvatasot käsikirja, 2008, 2.)

Yrityksen tietoturvatasot on kypsyysajattelun mukaisesti porrastettu viiteen eri portaaseen seuraavasti:

1. Aloittava
2. Toistettava
3. Määritelty
4. Hallittu
5. Optimoitu

Aloittavalla tasolla yrityksessä toimitaan satunnaisesti prosessin kohdalla, yhteisiä ohjeita ei ole laadittu. Harvat toiminnot ovat selkeästi määriteltyjä. Prosessin tulos riippuu paljon sen suorittajan taitotasosta. Laadussa voi esiintyä suuria heittoja. (VM, 2008, 3.)

Toistettavalla tasolla, josta käytetään myös nimitystä perustaso, on yhteisesti sovittu miten prosessien tulisi toimia ja kuka niistä on vastuussa. Prosessit on vastuutettu, toiminta organisoitu ja toimivaa. Prosessia voidaan jossain määrin toistaa. Prosessin hoitajan vaihtuessa voi virheiden määrä kasvaa.
(VM, 2008, 3.)

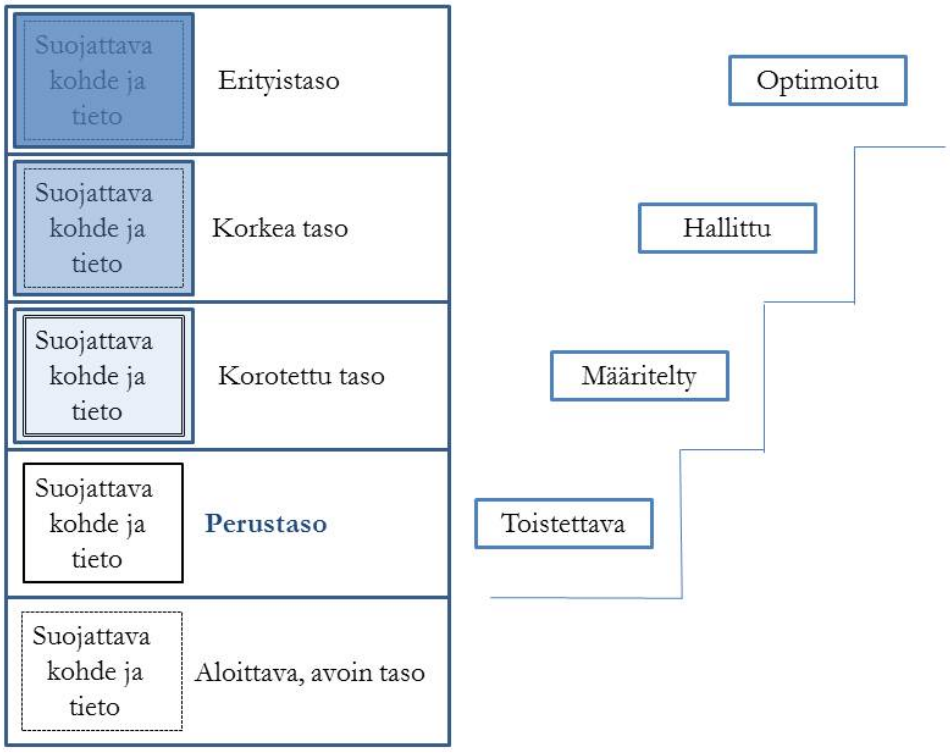
Määritellyllä tasolla eli korotetulla tasolla, yrityksen prosessien toimintaa ohjaavat ohjeet on kirjattu dokumentteihin ja henkilöstö koulutettu niiden mukaan. Prosessin hoitajan vaihdos ei vaikuta laatuun. Määritellyn tason toimintaa kuvaa sana dokumentoitu. Tälle tasolle yrityksen tulisi pyrkiä. (VM, 2008, 3.)

Hallitulla eli korkealla tasolla prosessien laatua valvotaan erilaisin mittarein. Havaituista häiriöistä tehdään selvitykset ja niiden perusteella pyritään oppimaan virheistä ja varmistamaan ennustettava tasainen laatu. (VM, 2008, 3.)

Optimoidulla tasolla käytetään parhaita mahdollisia käytänteitä. Prosessi ja seuranta menetelmät optimoivat itseään mittaustulosten perusteella.
(VM, 2008, 4.)

Päästäkseen tietylle tasolle on yrityksen toteutettava kaikki halutun tason ja sitä alempien tasojen vaatimukset. (Valtiovarainministeriö tietoturvatasot käsikirja, 2008, 4.)

Kuviossa 3. on kuvattu tietoturvatasot, aloittava taso on kuvassa alimpana. Kuvassa ylöspäin mentäessä suojattavan kohteen turvallisuus kasvaa.



Kuvio 3. Tietoturvatasot (Valtiovarainministeriö tietoturvatasot käsikirja, 2008, 3)

4.1 Perustason vaatimukset

Perustason vaatimukset löytyvät liitteestä 1. Alla käsiteltävät vaatimukset edustavat niitä keskeisiä vaatimuksia joihin konsultin pitää kiinnittää huomiota, yrityksen tietoturvatasoa arvioitaessa.

4.1.1 Johtajuudelle asetettavat vaatimukset

Strateginen ohjaus

Valtiovarainministeriön laatiman tietoturvatasot käsikirjan mukaan strategisen ohjauksen tavoitteena on, että yritys tunnistaa ydintoimintoihinsa liittyvät erityistilanteiden ja

jatkuvuuden hallintaa sekä tietoturvallisuutta ohjaavat tekijät ja velvoitteet. Yrityksen johdon tulee olla sitoutunut tietoturvallisuuteen ja osattava tulkita ydintoimintojensa vaatimuksen tietoturvallisuuden ohjaukseksi. Perustason vaatimuksena on, että yrityksellä on tiedossa toimintaansa koskeva lainsäädäntö. Yritys on tunnistanut ydintoimintonsa ja –prosessinsa sekä organisoinut ja vastuuttanut ne. Yrityksellä on kirjallinen johdon hyväksymä tietoturvapolitiikka. (Valtiovarainministeriö tietoturvatasot käsikirja liite 1, 2008, 2.)

Resurssointi ja organisointi

Resurssoinnin ja organisoinnin tavoitteena on, että yritys on asettanut jatkuvuuden hallinalle ja tiedon turvaamiselle tavoitteisiin nähden riittävät resurssit. Perustason vaatimuksena on, että yritykseen on nimetty tietoturvavastaava sekä että tietoturvavastaavalla on aikaa tietoturvavastuidensa hoitamiseen. (VM VAHTI 2/2010, 2010, 97.)

Raportointi ja viestintä sidosryhmille

Yrityksen tulee määritellä sidosryhmien kanssa viestinnässä ja raportoinnissa käytettävä toimintamalli, siten että tarvittavat tiedot ovat käytössä toimintaan, kehittämiseen ja päätöksentekoon. Ydinajatuksena on, että yritys tunnistaa ne tahot jolle sen tulee tietoturvallisuudesta raportoida. Perustason vaatimuksena on, että yritys on tunnistanut sidosryhmät joille se on tietoturvallisuudesta vastuussa, kontaktihenkilöt tulee olla selvitettynä. Sidosryhmiin vaikuttava tietoturva-asioista raportointi ja tietoturvapoikkeamista raportointi tulee olla vastuutettu. (Valtiovarainministeriö VAHTI 2/2010 liite 5, 2010, 99.)

Johtaminen erityistilanteissa

Erityistilanteessa johtamisen tavoitteena on, että erityistilanteiden hallinta on organisoitu ja huomioitu toimintamalleissa. Perustason vaatimuksena on, että tietoturvapoikkeamien käsittely on vastuutettu ja organisoitu. Yrityksessä pidetään kirjaa vakavista tietoturvapoikkeamista sekä että niistä raportoidaan viivytyksettä johdolle. ((VM VAHTI 2/2010, liite 5, 99.)

Yhteistyön koordinointi

Yrityksen tulee toteuttaa jatkuvuuden hallinta ja tiedon turvaaminen ydin- ja tukitoimintojensa yhteistyönä. Yhteistyön koordinoinnin tavoitteena on, että organisaation ylin johto ja tietoturvavastaavat keskustelevat keskenään. Perustason vaatimuksena jatkuvuuden hallinnalle on, että yrityksellä on säännöllisesti kokoontuva tietoturva-asioita käsittelevä työryhmä sekä, että tietoturvavastaavat ja ylin johto keskustelevat säännöllisesti keskenään. (VM VAHTI 2/2010, liite 5, 98.)

4.1.2 Toiminnan suunnittelulle asetettavat vaatimukset

Toimintaympäristön vaikutus

Yrityksen tulisi tuntea oma tietojenkäsittely toimintaympäristö ja sen vaikutus tietoturvallisuuteen. Toimintaympäristön yhtenäisyyden tai hajanaisuuden tunnistaminen on tärkeää. Toimintaympäristöllä on vaikutusta moneen tietoturvallisuuden osa-alueeseen riskianalyysin kautta. Perustason vaatimuksena on, että yritys on tunnistanut erilliset tietojenkäsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät ja toiminnot. Kunkin toimintaympäristön erityisvaatimukset ja tavoitteet on tietoturvallisuuden osalta tunnistettu. (VM VAHTI 2/2010, liite 5, 101.)

Tavoitteiden määrittely

Tietoturvallisuuden tavoitteet tulee määritellä yrityksen ydintoimintojen näkökulmasta. Tietoturvatavoitteiden asettamisessa ovat, ydintoimintojen suojattavien kohteiden (tietoaineistot, tietojärjestelmät, rekisterit yms.) määrittely ja kohteiden tietoturvavaatimukset merkittävä taustatekijä. Kun tavoitteet on saatu selville, tehdään riskien arviointi, jolla selvitetään mitä riskejä tavoitteiden toteutumisessa tässä toimintaympäristössä on. Perustason vaatimuksena on, että kunkin avaintoiminnon ja –prosessin kannalta suojattavat kohteet on tunnistettu ja luokiteltu vaadittavan tietoturvatason mukaisesti. Avaintoimintojen tai –prosessien tavoitteisiin on liitetty myös tietoturvatavoitteita. (VM tietoturvatasot liite 1, 2008, 9.)

Toiminnan kehittäminen riskien avulla

Yrityksen tulisi kehittää toimintaansa riskien arvioinnin avulla. Riskien arvioinnin tavoitteena on varmistaa, että tietoturvallisuuden taso vastaa organisaation strategisia tavoitteita. Riskianalyysin perusteella suunnitellaan tarvittavat tietoturvallisuuden hallin-

taprosessit ja tarvittavat tekniset suojaustoimenpiteet, jotta tietoturvallisuudelle asetetut tavoitteet saavutetaan ja riskit pysyvät hyväksyttävällä tasolla. Perustason vaatimuksena on, että yrityksessä tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia ja, että yrityksellä on tietoturvariskien arvioinnin yleinen menetelmä käytössään. Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä. (VM VAHTI 2/2010, liite 5, 103.)

Erityistilanteiden hallinta

Yrityksen tulee olla varautunut erityistilanteisiin. Erityistilanteiden hallinnan menettelyt tulee olla suunniteltu, koulutettu ja harjoiteltu. Erityistilanteiden hallinnalle asetettu perustason vaatimus on, että yrityksellä on jatkuvuussuunnitelma tai –suunnitelmia, joita testataan säännöllisesti. Jatkuvuudella tarkoitetaan yrityksen toimintojen jatkuvuutta erilaisissa häiriötilanteissa. (VM tietoturvatasot liite 1, 2008, 12.)

4.1.3 Henkilöstölle asetettavat vaatimukset

Osaamisen ja tietoisuuden kehittäminen sekä sanktiot

Henkilöstön tietämättömyydestä johtuvien tietoturvapoikkeamien estämisen avainasemassa ovat henkilöstön tietoturva tietoisuus sekä positiivinen asenne tietoturvallisuuteen. Henkilöstö saattaa mieltää tietoturvallisuuden negatiivisena jopa työntekoa haittaavana asiana, näin ollen, ei positiivisen palautteen vaikutusta kannata aliarvioida. Yrityksen tulisi kannustaa henkilöstöä noudattamaan ja kehittämään hyvää tiedon turvaamisen ja jatkuvuuden kehittämisen toimintamallia. Yrityksen tulee asettaa rooli- tai tehtäväkohtaiset vaatimukset jatkuvuuden hallinnan ja tiedon turvaamisen osaamiselle. Yrityksellä tulee olla käytössä sovittu tapa toimia turvallisuuspoikkeamissa ja väärinkäytöstilanteissa. Perustason vaatimuksina on, että yritys järjestää säännöllisesti tietoturvakoulutusta henkilöstölle. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään. Perehdyttämistilanteissa käsitellään myös tietoturva-asioita. Muuttuneista tietoturvaohjeista ja –käytännöistä tiedotetaan kaikille yrityksessä toimiville. Sääntöjen noudattamista seurataan ja poikkeamiin puututaan. Suomen erityisvaateena on lisäksi että työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§). (VM VAHTI 2/2010, liite 5, 106.)

4.1.4 Tietojärjestelmien hallinnan vaatimukset

Omaisuuden hallinta

Omaisuuden hallinnan tavoitteena on tunnistaa yrityksen vastuulla olevat laitteet, niiden sisältämät ohjelmistot ja näistä koostuvat tietojärjestelmät jotta näiden turvallisuudesta voidaan huolehtia. Tärkeää on tunnistaa suojattavat kohteet ja asettaa niille omistaja jolla on oikeus tehdä kohdetta koskevia muutoksia esim. käytöstä poistaminen. Perustason vaatimuksena on, että yritys on luetteloinut omistamansa fyysiset ja virtuaaliset laitteensa, palvelunsa, ohjelmistonsa sekä lisenssinsä. Laitteiden, rekisterien ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu. (Valtiovarainministeriö tietoturvatasot käsikirja liite tietoturvatasot 2, 2008, 2.)

Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto

Tietojärjestelmien teknisen tietoturvallisuuden kulmakivi on huolellinen perusasennus jossa otetaan huomioon tietoturvallisuus. Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto tulee tehdä niin että varmistutaan tietoturvallisuudesta. Perustasolle vaaditaan, että tietojärjestelmien ja työasemien käyttöönottoasennuksessa ja käytöstä poistamisessa otetaan huomioon järjestelmien tietosisällön tietoturvavaatimukset. Tietojärjestelmien ja työasemien käyttöönottoon ja käytöstä poistamiseen liittyvät toimenpiteet on vastuutettu. (VM tietoturvatasot liite 2, 2008, 3.)

Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta

Tietojenkäsittely-ympäristön päivitys ja muutoshallinnan tavoitteena on varmistua siitä, että tietojenkäsittely-ympäristöt päivitetään hallitusti, tällä estetään haavoittuvuuksien hyväksikäyttö ja tietoturvaongelmien synty. Perustason vaatimuksena on, että laitteiden ja tietojärjestelmien päivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on vastuutettu erityisesti tietoturvapäivitysten osalta. Laitteiden ja tietojärjestelmien muutostarpeen seuranta, muutospäätösten teko ja muutosten toteutus on vastuutettu. Yrityksellä on periaatteet, jotka kertovat millaiset päivitykset tai muutokset voidaan asentaa välittömästi ja millaisiin päivityksiin tai muutoksiin käytetään riskitason huomioivaa tarveharkintaa. (VM VAHTI 2/2010, liite 5, 115.)

Turva-alueiden muodostus ja niiden välinen suodatus

Verkkoliikenteen suodatus ja tietoverkkojen eriyttäminen on olennaista tietoverkoista tulevien uhkien torjunnassa. Yrityksen tulee muodostaa turva-alueet ja suodattaa niiden välinen liikenne, tällä varmistetaan, että tieto kulkee tietoverkosta toiseen vain valtuutetusti. Perustason vaatimuksena on, että Yrityksessä on tunnistettu ja eriytetty tietoverkon eri suojaustasoa vaativat osat ja eri suojaustason verkkojen välistä liikennettä rajoitetaan ja suodatetaan. Yrityksessä on vastuutettu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen. Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu. Julkisesta verkosta yritykseen sisäänpäin tulevaa liikennettä rajoitetaan ja suodatetaan ”kaikki liikenne on kielletty ellei erikseen sallittu” -periaatteella. Yrityksellä on etäkäyttöperiaatteet. (VM tietoturvatasot liite 2, 2008, 5.)

Pääsynvalvonta

Tietoturvatoimenpiteistä tärkeimpiä on pääsynvalvonta. Pääsynvalvonnan tavoitteena on varmistaa, että tietoon pääsevät käsiksi vain valtuutetut käyttäjät. Perustason vaatimuksena on, että tietojärjestelmän omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan. Sekä onnistuneet, että epäonnistuneet sisäänkirjautumiset järjestelmään kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti. Huonolaatuisten salasanojen käyttöä estetään. (VM tietoturvatasot liite 2, 2008, 6.)

Haittaohjelmasuojaus

Haittaohjelma suojauksen tavoitteena on, että yrityksen tietovarannot ovat suojassa haittaohjelmien aiheuttamilta vahingoilta. Perustason vaatimuksena on, että yrityksessä suodatetaan haittaohjelmia sekä työasematasolla että kaikissa sähköposti ja WWW–liikenteen sisääntulo- ja ulosmenopisteissä. Haittaohjelmakuvaukset päivittyvät automaattisesti ja säännöllisesti. ((VM VAHTI 2/2010, liite 5, 120.)

Varmuuskopiointi

Varmuuskopioinnin tarkoituksena on estää tiedon katoaminen yrityksestä ja vähentää erilaisten häiriötilanteiden vaikutusta yrityksen toimintaan. Suunniteltaessa varmuusko-

piointia on tärkeää miettiä mitä varmuuskopioidaan ja miten usein. Perustason vaatimuksen varmuuskopioinnille on, että yrityksessä on vastuutettu ja organisoitu varmuuskopioiden ottaminen. Yrityksessä on tunnistettu varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti. (VM liite tietoturvatasot 2, 2008, 9.)

4.2 Tietoturvallisuuden perustason dokumentteja

Yrityksen tietoturvaa tutkittaessa, tulee tietoturvakartoituksen aikana tutkia yrityksen olemassa olevaa dokumentaatiota. Perustasolla yrityksellä tulisi olla käytössään ainakin seuraavat dokumentit: tietoturvapolitiikka ja jatkuvuussuunnitelma. Konsultin tulee tietää millaisia dokumenttien tulee olla ja jos dokumentteja ei ole olemassa tulee konsultin voida laatia puuttuva dokumentaatio asiakkaalle. Tässä luvussa tutustutaan tietoturvan perustasolla vaadittavaan dokumentaatioon tietoturvapolitiikan ja jatkuvuussuunnitelman osalta sekä tietojen luokitteluun yrityksessä.

4.2.1 Tietoturvapolitiikka

Tietoturvapolitiikka ohjaa yrityksen tietoturvakäytänteitä ja tietoturvallisuusprosesseja. Politiikka luo perustan tietoturvaohjeistukselle ja -koulutukselle. Tietoturvapolitiikassa yritysjohto julkilausuu karkean tason tietoturva linjaukset. Yritysjohto osoittaa politiikan avulla tukensa ja sitoutumisensa turvallisuuden kehittämisen. Laadittava dokumentti on julkinen. Politiikka pitää kirjoittaa niin, että sen ymmärtävät myös muut kuin tietojenkäsittelyn tai hallinnon ammattilaiset. Tietoturvapolitiikassa otetaan yleensä huomioon seuraavat asiat:

- Johto tuo esille näkemyksensä tietoturvallisuuden merkityksestä yritykselle ja määrittelee tietoturvallisuuden keskeisimmät kohteet ja laajuuden.
- Politiikassa otetaan kantaa tietoturvallisuuden tavoitteiden saavuttamiseen ja siihen liittyvien periaatteiden noudattamiseen osana liiketoimintastrategiaa
- Tietoturvallisuuden roolit ja vastuut määritellään.
- Yrityksen tulee linjata miten se ottaa huomioon juridiset ja kauppatapojen asettamat vaatimukset

- Tietoturvakäytänteistä, noudatettavista standardeista ja yleisperiaatteista laaditaan yhteenveto
- Turvallisuusajattelun edistämisestä ja turvallisuuskoulutuksesta laaditaan yhteenveto
- Liiketoiminnan jatkuvuuden hallinta ja toipumissuunnittelu kuvataan yleisellä tasolla
- Määritellään suuntaviivat tietojenkäsittelyn suojaamiseen
- Otetaan kantaa tietoturvapolitiikan laiminlyönnin seurauksiin. (Hakala ym. 2006, 7-9 ; Laaksonen ym. 2006, 146-148.)

4.2.2 Jatkuvuussuunnitelma

Yrityksen tulee olla varautunut tietojärjestelmissä, tietoyhteyksissä ja palveluissa tapahtuviin keskeytyksiin. Vahinkoihin varaudutaan tekemällä jatkuvuussuunnitelma. Siinä otetaan huomioon vakavat onnettomuustilanteet jotka kohdistuvat paikallisiin, toimintaan tai tietojenkäsittelytiloihin. Onnettomuustilanteita voivat aiheuttaa kaasuvuodot, räjähdykset, tulipalot, vesivahingot. Jatkuvuussuunnitelmassa otetaan huomioon myös tietotekniikkaan kohdistuvat uhkat ja vahingot kuten verkkohyökkäykset. Varautuminen edellyttää, että varmuuskopionti on luotettavaa ja, että tietokantojen eheys säilyy. (Vahti, 3/2007, 75.)

Valtiovarainministeriön tietoturvallisuuden johtoryhmän laatiman tietoturvaohjeistuksen, vahtiohjeen mukaan tärkeimpiä huomioitavia seikkoja jatkuvuuden varmistamisessa tietotekniikan näkökulmasta ovat:

- keskeisten toimintojen ja palvelujen määrittely
- keskeisille toiminnoille välttämättömän tietojenkäsittelyn määrittely
- keskeytysten vaikutukset tuotantoon, palveluihin, asiakkaisiin ja toimituksiin
- toimintojen tietojenkäsittelyriippuvuudet
- muiden tahojen välilliset riippuvuudet palvelujen keskeytymisestä
- kriittisiksi muodostuvat keskeytysajat
- kausiluonteiset kriittiset ajankohdat

- arviot keskeytystilanteessa syntyvistä taloudellisista menetyksistä sovelluksittain
- tietotekniikan käytön rajoittuessa ylläpidettävien sovellusten ja varmistamistoimenpiteiden prioriteetit. (Vahti, 3/2007, 76.)

Vahtiohjeen mukaan ” Jatkuvuussuunnitelmaan sisällytetään kaikki ne toimenpiteet, joita tarvitaan toiminnan jatkamiseen keskeytystilanteissa siihen asti, kunnes toiminta voidaan palauttaa alkuperäiselle käyttötasolle”. (Vahti, 3/2007, 76.) Suunnitelman tule sisältää:

- järjestelmien varmistamisen suunnitelman
- varajärjestelmän käyttöympäristön suunnittelu laitteineen, yhteyksineen, ohjelmineen ja käyttötoimintoineen
- toipumissuunnitelman. (Vahti, 3/2007, 76.)

4.2.3 Toipumissuunnitelma

Toipumissuunnitelmassa kuvataan miten varajärjestelmistä palaudutaan tuotantojärjestelmiin ja mitkä varmistavat toimenpiteet tulee tehdä, että palvelut voidaan riskittä käynnistää. (Vahti, 3/2007, 77.)

4.2.4 Tietojen ja järjestelmien luokittelu yrityksessä

Tietojen luokittelun lähtökohta on tietojen oikeantasoinen suojaaminen. Tietojen luokittelu vaikuttaa siihen, miten tietoja käsitellään. Tietojen luokittelujärjestelmän tarkoituksena on antaa suuntaviivat tietojen turvaamistavoitteiden asettamiseksi. Tietojen luokitusjärjestelmässä on kaksi osa-aluetta: tiedon luottamuksellisuus ja vaikutus toimintaan. Järjestelmää luotaessa on päätettävä siitä kuinka moniportainen järjestelmä luodaan. Luokittelusta ei tule tehdä liian monimutkaista. Seuraavassa taulukossa esitetään esimerkki tietojen luokittelusta. Taulukossa esitellään tiedon tärkeysluokat julkisesta salaiseen ja niiden käsittelysäännöt. Taulukon ylimmällä rivillä ovat tiedon tärkeysluokat. Taulukon vasemmanpuoleisimmalla sarakkeella on käsittelysäännöt ja näiden yhtymäkohdassa ohjeistus säännöstä. (Hakala ym. 2006, 62-64 ; Laaksonen ym. 2006, 156-157.)

Taulukko 1. Esimerkki tietojen luokittelusta (Laaksonen ym. 2006, 157)

Tiedon tärkeysluokka / käsittelysääntö	Julkinen	Sisäinen	Luottamuksellinen	Salainen
Merkintä	Julkinen	Sisäinen	Luottamuksellinen	Salainen, dokumentissa jokaiselle sivulle
Tiedonjakelu	Kaikille	Kaikille työntekijöille	Rajoitetulle määrälle henkilöstöä	Erittäin rajatulle määrälle henkilöstöä
Tiedon salaus	Ei pakollista	Ei pakollista	Pakollista, jos kuljetetaan tai lähetetään yrityksen ulkopuolelle	Aina pakollista
Lähetys sähköpostilla	Sallittu	Sallittu	Salattuna sallittu	Salattuna sallittu
Tietojen tallennus	Ei rajoituksia	Ei rajoituksia	Asianmukaisilla käyttöoikeuksilla	Asianmukaisilla käyttöoikeuksilla, salattuna
Tallennus muistikortille tms.	Sallittu	Sallittu, salaus suositeltavaa	Salattuna sallittu	Salattuna sallittu

Järjestelmien tärkeysluokittelu tulee tehdä vähintään järjestelmän käytettävyyden ja sen sisältämien tietojen kriittisyyden mukaan. Järjestelmän käytettävyysluokkaa tarvitaan jatkuvuus- ja toipumissuunnittelussa ja kriittisyys vaikuttaa järjestelmien suojaustarpeisiin. Järjestelmä tulee aina luokitella siihen luokkaan jossa se saa korkeimman arvon. Seuraavassa taulukossa esitetään esimerkki järjestelmien luokittelusta. Taulukon ylin rivi kertoo järjestelmän tärkeysluokan. Seuraavalla rivillä kuvataan millainen järjestelmä on kyseessä. Kolmas rivi kertoo suurimman sallitun keskeytysajan. Alimmalla rivillä kuvataan järjestelmä sisältämien tietojen kriittisyyttä. (Hakala ym. 2006, 158.)

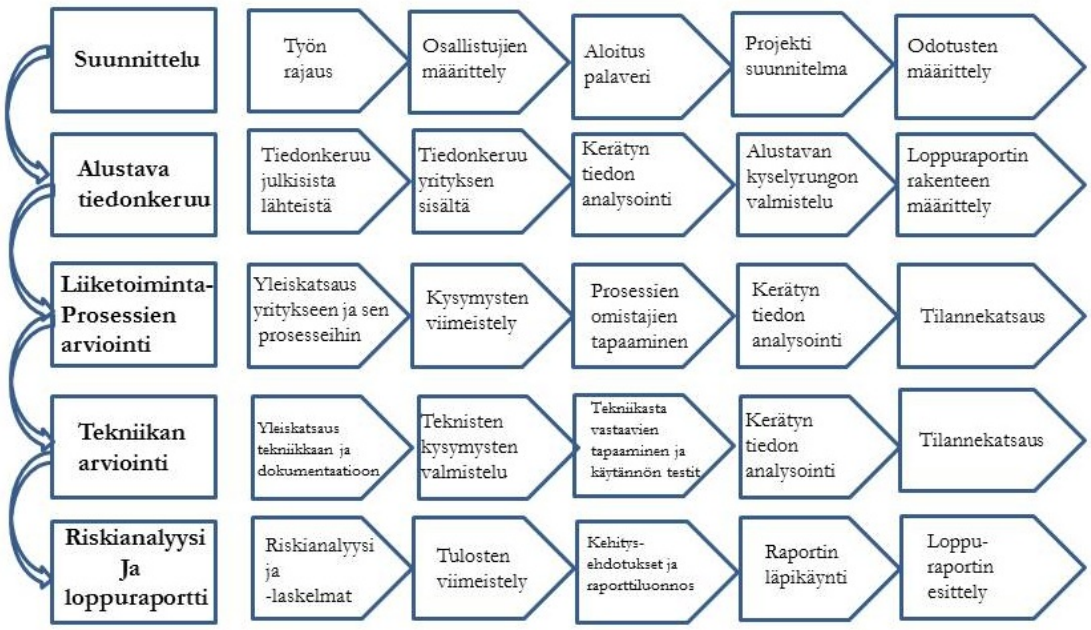
Taulukko 2. Esimerkki järjestelmien luokittelusta. (Hakala ym. 2006, 159)

Tärkeysluokka / ominaisuus	Kriittinen järjestelmä	Tärkeä järjestelmä	Melko tärkeä järjestelmä	Ei-tärkeä järjestelmä
Järjestelmän kuvaus	Erittäin keskeinen järjestelmä yrityksen toiminnalle, toiminta ei ole mahdollista ilman kyseistä järjestelmää	Tukee yrityksen keskeisiä liiketoiminta prosesseja. Toiminta voi jatkua jonkun aikaa ilman kyseistä järjestelmää	Järjestelmää ei välttämättä tarvita yrityksen ydinliiketoimintaan, mutta jonka toiminta helpottaa toiminnan harjoittamista	Tukijärjestelmä, ei välttämätön liiketoiminnan ylläpitämiseksi
Sallittu keskeytysaika	< 5 minuuttia	< 4 tuntia	< 5 päivää	< 1 kuukausi
Järjestelmän sisältämien tietojen kriittisyys	Tietojen säilyminen, oikea prosessointi ja saatavuus tulee turvata kaikissa olosuhteissa	Tietojen säilyminen ja oikea prosessointi tulee turvata	Tietojen säilyminen, oikea prosessointi ja saatavuus tulee pyrkiä turvaamaan, mutta tietojen menettäminen ei ole liiketoiminnalle kriittistä	Tietojen säilyminen, oikea prosessointi ja saatavuus tulee pyrkiä turvaamaan, mutta tietojen menettäminen ei ole liiketoiminnalle kriittistä

5 Tietoturvakartoitus

Käynnistettäessä tietoturvallisuus prosessia on ensimmäinen työvaihe yleensä tietoturvakartoitus. Kartoituksella hankitaan perustieto yrityksen ja sen tietojärjestelmien nykytilasta. Riskikohteet ja tarvittavat toimenpiteet niiden suojaamiseen voidaan määritellä kartoituksella kerätyn tiedon perusteella. Kartoitus tulisi uusia säännöllisin väliajoin tai kun tietoturvan toteuttamisessa tapahtuu oleellisia muutoksia. (ISO 17799, 2006 , 40.)

Kuviossa 4. esitellään tietoturvakartoitus Kairabin mallin mukaisesti. Mallissa on viisi päävaihetta, joista kukin sisältää viisi alivaihetta. Kairab on laatinut mallin joka on joustava. Tietoturvakartoitusten ollessa yksilöllisiä, vaatii niiden suorittaminen usein yrityskohtaisia ratkaisuja, kartoitustyön on oltava joustavaa ja mukauduttava yrityksen tarpeisiin. Kairabin mallin hyvänä puolena voidaan pitää sitä, että eri työvaiheita voidaan tarpeen mukaan yhdistää ja työmäärää painottaa yritykselle tärkeisiin prosesseihin ja toimintoihin. Työvaiheita voidaan myös joissain tapauksissa suorittaa eri järjestyksessä tai jopa harvoin jättää tekemättä. Tietoturvakartoituksen tärkein lähtökohta on yrityksen liiketoiminnan perusteellinen ymmärtäminen, jotta kartoitettavia riskejä voidaan ymmärtää. (Kairab, 2005, 64-65.)



Kuvio 4. Tietoturvakartoituksen vaiheet (Kairab, 2005, 63)

Tietoturvakartoituksen tekeminen jaetaan viiteen päävaiheeseen seuraavasti:

- Suunnittelu
- Alustava tiedonkeruu
- Liiketoimintaprosessien arviointi
- Tekniikan arviointi
- Riskianalyysi ja loppuraportti

5.1 Suunnittelu

Suunnittelu vaihe on jaettu viiteen alivaiheeseen:

- Työn rajaus
- Osallistujien määrittely
- Aloitus palaveri
- Projekti suunnitelma
- Odotusten määrittely

Suunnittelua aloitettaessa tulee ensimmäiseksi selvittää mitkä ovat liiketoiminnalliset motiivit tai syyt tietoturvakartoitukseen. Liiketoiminnallisia motiiveja ovat mm. johdon asenne tietoturvan tärkeydestä, muutokset yrityksen liiketoiminnassa sekä yrityksessä tapahtunut tietoturvapoikkeama, että yrityksen johto haluaa ennalta ehkäistä tietoturvapoikkeamia. Liiketoiminnalliset motiivit auttavat määrittelemän miten laajasti tietoturvallisuuden eri osa-alueita kartoitetaan. (Kairab, 2005, 67-70.)

Suunnitteluvaiheessa aloitetaan henkilöstön haastattelut, työn laajuutta suunniteltaessa tulee haastatella yrityksen johtoa, prosessien omistajia ja ICT-turvallisuus henkilöstöä. (Kairab, 2005, 77). Käytettävät standardit otetaan esille suunnitteluvaiheessa. Työtä tehtäessä tulee huolehtia siitä, että työn rajaus ei muutu ja jos se muuttuu, tulee muutokseen olla hyvä syy ja muutos tulee tehdä muutoksen hallinta prosessin kautta. (Kairab, 2005, 100.)

Kun työ on saatu rajattua, perustetaan tiimi tekemään työtä. Asiakkaan tulee tässä vaiheessa päättää käytetäänko kartoitukseen omaa vai kolmannen osapuolen henkilöstöä. Konsultin näkökulmasta katsottuna tulee tässä vaiheessa pohtia millaista tietotaitoa projekti tarvitsee. Asiakkaan näkökulmasta katsottuna tulee miettiä millaisella budjetilla projektia lähdetään tekemään, millaisia resursseja käytetään ja miten liiketoiminnalliset motiivit täytetään. (Kairab, 2005, 82-83.)

Varsinainen kartoitustyö alkaa aloituspalaverista, se on ensimmäinen kerta kun kartoitustiimi ja asiakkaan edustajat keskustelevat projektista keskenään. Palaverissa käydään läpi projektin aikataulu sekä projektin työskentelytavat. Projektin vetäjä esittelee kartoitusprosessin karkealla tasolla. Tulevat tapaamiset sovitaan tässä vaiheessa, jotta mahdollisille muutoksille jää riittävästi aikaa. Onnistuneen palaverin ja koko projektin varmistamiseksi paikalla tulee olla asiakasyrityksen johtoa antamassa tukensa ja hyväksyntänsä projektille. (Kairab, 2005, 87-91.)

Projektisuunnitelmaan kirjataan projektia koskevat tiedot tarkasti ylös. Projektisuunnitelmassa kerrotaan projektin tausta, tehtävä, tavoitteet, lopputulokset, tehtävän rajaus, riskit, toteutusympäristö, budjetti ja aikataulu. Työsuunnitelmassa kuvataan vaiheittain mitä tehdään ja miten sekä projektihallinnolliset menettelytavat. (Kairab, 2005, 91; HAAGA-HELIA, projektisuunnitelma, 2005.)

Asiakkaan odotukset projektista tulee määrittää. Asiakkaalle tulee kertoa mitä tietoturvakartoitus on ja mitä ei, sekä mitä asiakas projektin lopuksi saa ja mitä ei. Jos asiakkaan odotuksista projektia kohtaan ei keskustella riittävästi, asiakkaan luulo siitä mitä tehdään verrattuna varsinaiseen tekemiseen jää puutteelliseksi ja koko projekti tulee epäonnistumaan. Asiakkaalle tulee siis antaa riittävät tiedot projektista. (Kairab, 2005, 94.)

5.2 Alustava tiedonkeruu

Alustava tiedonkeruu vaihe on jaettu viiteen alivaiheeseen:

- Tiedonkeruu julkisista lähteistä

- Tiedonkeruu yrityksen sisältä
- Kerätyn tiedon analysointi
- Alustavan kyselyrungon valmistelu
- Loppuraportin rakenteen määrittely

Alustavan tiedonkeruun tarkoitus on kerätä tietoa ja oppia tuntemaan asiakas. yleisen tiedon kerääminen asiakkaasta luo vahvan perustan asiakkaan henkilökunnalle tehtäviin haastatteluihin. Tiedon keräämisen hyötynä on uskottavuus asiakkaan silmissä ja se helpottaa oikeiden kysymysten tekemistä. (Kairab, 2005, 103.)

Julkisia lähteitä hyväksikäyttäen tulee selvittää ainakin seuraavat asiat:

- Millainen on yrityksen taloudellinen tilanne?
- Onko yrityksen ylimmässä johdossa tapahtunut muutoksia?
- Onko yritysjärjestelyissä tapahtunut muutoksia, sulautumisia tai yrityskauppoja?
- Onko yrityksessä ollut tietoturvapoikkeamia?
- Onko yritys laajentamassa tai pienentämässä toimintaansa?
- Onko yrityksellä laillisia velvoitteita koskien tietoturvallisuutta?

(Kairab, 2005, 103-105.)

Julkisista lähteistä kerätyn tiedon perusteella haastatellaan asiakkaan henkilökuntaa. Haastattelujen apuna voidaan käyttää kyselykaavakkeita. Valmiita kyselymalleja ei voi suoraan käyttää haastaatteluun, vaan kysymykset on valmisteltava perustuen asiakkaasta kerättyyn tietoon. Haastateltavan henkilön tulee olla esimiestasolta ja hänen tulee tuntea yrityksen liiketoiminta sekä hänen tulee voida keskustella yrityksen toiminnasta yleisellä tasolla. Haastateltavalle tulee esittää ainakin seuraavanlaisia kysymyksiä:

- Millainen on yrityksen demografia?
- Kuinka monta toimipistettä yrityksellä on?
- Millainen on yrityksen tietojenkäsittely-ympäristö?
- Onko yrityksellä tietoturvallisuusohjelma?

Tässä vaiheessa tulee myös tarkastella jo olemassa olevaa dokumentaatiota ainakin seuraavilta osin: Laaditut tietoturvapolitiikat ja toimenpiteet. Tekniset dokumentit tietoturvallisuuden näkökulmasta katsottuna. Aikaisemmat auditoinnin tai tietoturvallisuuden kartoitukset. (Kairab, 2005, 117-123.)

Haastattelujen jälkeen analysoidaan kerättyä aineistoa. Haastattelut on hyvä tallentaa digitaaliseen muotoon, jolloin vältytään käsinkirjoitettujen muistiinpanojen muistamisesta myöhempänä ajankohtana. Käsinkirjoitettuja muistiinpanoja on hyvä käyttää digitaalisen tallenteen apuna. Kerätyn tiedon analysoinnin tarkoituksena on dokumentoida keskustelut asiakkaan henkilöstön kanssa sekä dokumentoida kaikki asiaankuuluvat julkisista läheteistä kerätyt tiedot, että dokumentoida tietoturvaan liittyvät potentiaaliset löydöt ja määritellä, miten kerätyt tiedot auttavat kyselerungon valmistelussa. (Kairab, 2005, 123.)

Kyselyrungon valmistelussa tulee ottaa huomioon, että kysymysten tulee perustua julkisista lähteistä sekä yrityksen sisältä kerättyihin tietoihin. Kysymyksiä on kahdenlaisia, liiketoimintaprosesseihin liittyviä ja perinteisiin tietoturvallisuuden prosesseihin liittyviä. Kysymykset suunnataan liiketoimintaprosessien omistajille. (Kairab, 2005, 123-125.)

Liiketoimintaprosesseja arvioivaan kyselyrunkoon on aina hyvä sisällyttää yleisellä tasolla olevia kysymyksiä. Seuraavat alueet tulee huomioida kyselyä tehtäessä:

- Tärkeimmät liiketoimintaprosessit ja niitä tukevat teknologiat.
- Integraatio eri toimipisteiden välillä.
- Aikaisemmat tietoturvapoikkeamat.
- Mahdolliset muutokset liiketoiminnassa. (Kairab, 2005, 125-132.)

Perinteisiä tietoturvallisuuteen liittyviä kysymyksiä laatiessa tulee apuna käyttää standardeja esim. COBIT tai ISO 27001 tai ISO 27002 tai Valtiovarainministeriön laatimat VAHTI-ohjeet. Yleisellä tasolla kysymyksiä tulee esittää seuraavista aihepiireistä:

- Käyttäjätunnukset

- Tietojen luokittelu
- Varmuuskopiointi
- Liiketoiminnan jatkuvuus ja varmuuskopionti
- tietoturva poikkeamien hallinta
- Muutoshallinta
- Fyysinenturvallisuus
- ICT-resurssien käyttöpolitiikka (Kairab, 2005, 132-134.)

Loppuraportin rakenteen määrittely tulee aloittaa hyvissä ajoin. Tehdyn työn laatu määrittyy pitkälti loppuraportin perusteella. Loppuraportin tulisi toimia tietoturvallisuuden suunnannäyttäjänä asiakkaalle. Tässä vaiheessa loppuraporttiin voidaan kirjata seuraavat osat, karkean tason kuvaus kartoituksesta, liiketoiminnalliset motiivit, yrityksen liiketoiminnan kuvaus, tärkeimmät löydökset tähän mennessä, työn rajaus sekä käytettävät metodit. Loppuraporttiin kirjataan löydetyt tiedot sen mukaan kuin niitä ilmenee. (Kairab, 2005, 134-136.)

5.3 Liiketoimintaprosessien arviointi

Liiketoimintaprosessien arviointi jaetaan viiteen alivaiheeseen seuraavasti:

- Yleiskatsaus yritykseen ja sen prosesseihin
- Kysymysten viimeistely
- Prosessien omistajien tapaaminen
- Kerätyn tiedon analysointi
- Tilannekatsaus

Tässä vaiheessa on hyvä muistaa, että yrityksen liiketoimintaprosessien arvioinnille annetaan riitävästi aikaa, muuten vaarana on, ettei yrityksen ydintoimintaa ymmärretä tarpeeksi tarkasti, jolloin koko kartoitus on vaarassa epäonnistua.

Asiakasyrityksen johdon kanssa keskustelemalla selvitetään yrityksen ydinprosessit ja niitä tukevat prosessit. Aluksi liiketoimintaprosesseja tarkastellaan yleisellä tasolla ja

lopuksi yksityiskohtaisemmin. Yrityksen ydinprosessien selvittäminen on kriitinen vaihe kartoitusta tehtäessä, koska ilman perustavanlaatuista ymmärrystä siitä mitä yritys tekee, on mahdotonta tehdä kunnollista kartoitusta. Johtoa haastateltaessa tulee selvittää:

- Mitkä ovat johdon mielestä kriittiset liiketoimintaprosessit?
- Millainen on liiketoiminta-ympäristö?
- Onko tiedossa muutoksia, jotka vaikuttavat tietoturvallisuuteen?
- Millainen on yrityksen organisaation rakenne?
- Millaiset asiat johtoa tietoturvallisuudessa huolestuttavat? (Kairab, 2005, 142-145.)

Kun yrityksen liiketoiminnan ydinprosessit on saatu selvitettyä, viimeistellään kysymykset liiketoimintaprosessien omistajille. (Kairab, 2005, 151.)

Liiketoimintaprosessien omistajien tapaamisissa selvitetään yrityksen liiketoimintaprosessit yksityiskohtaisesti. Koska asiakkaan liiketoiminnan ymmärtäminen on avainasemassa kartoituksessa, myös liiketoimintaprosessien omistajien tulee valmistautua tapaamisiin. Tulee siis varmistaa, että he ovat tietoisia kartoituksesta. Kysymykset on hyvä toimittaa haastateltaville etukäteen. (Kairab 2005, 155-156.)

Liiketoimintaprosessien omistajien haastatteluiden jälkeen analysoidaan ja dokumentoidaan kerätyt tiedot. Tässä vaiheessa analysoitavasta tiedosta pitää tunnistaa heikkoudet turvallisuudessa. Tietojen analysointi tulee tehdä koko kartoitusta suorittavan tiimin voimin. Havaitut löydökset kirjataan suoraan loppuraporttiin. Havaitut riskit tulee dokumentoida niin, että niiden liiketoiminnalliset vaikutukset tulevat esille. Ehdotukset turvallisuuden parantamiseksi dokumentoidaan. (Kairab 2005, 156-158.)

Liiketoimintaprosessien arvioinnin viimeinen toimenpide on pitää asiakkaalle tilannekatsaus, jossa kerrotaan löydökset, esitellään ehdotukset turvallisuuden parantamiseksi, keskustellaan siitä, että mitä kriittistä teknologiaa aiotaan testata ja tarkastellaan tilannetta projektisuunnitelmaan näkökulmasta. (Kairab 2005, 158.)

5.4 Tekniikan arviointi

Tekniikan arviointi on jaettu viiten alavaiheeseen seuraavasti:

- Yleiskatsaus tekniikkaan ja dokumentaatioon
- Teknisten kysymysten viimeistely
- Tekniikasta vastaavien tapaaminen ja käytännön testit
- Kerätyn tiedon analysointi
- Tilannekatsaus

Lähtökohta tekniikan arviointiin on samanlainen kuin liiketoimintaprosesseja arvioitaessa. Aluksi tekniikkaa tarkastellaan yleisellä tasolla ja lopuksi kriittisiä teknologioita yksityiskohtaisesti. Tekniikan arvioinnin tarkoituksena on arvioida tietojenkäsittely-ympäristöä ja kartoittaa miten turvallinen se on liiketoimintaprosessien kannalta. Tärkeintä on suojata yrityksen ydinprosessit. Kaikkia prosesseja ei ole tarvetta suojata samantasoisesti. Sopiva suojaustaso saadaan selville analysoimalla liiketoimintaprosessien omistajien haastatteluja. Tietojenkäsittely-ympäristöä arvioitaessa tulee kiinnittää huomiota tietoturvatoimenpiteisiin verraten niitä riskitasoon ja teknologian kriittisyyteen. (Kairab 2005, 165.)

Yleiskatsaus tekniikkaan ja dokumentaatioon tulee aloittaa selvittämällä millaista teknologiaa yritys käyttää nyt ja millaista se aikoo käyttää tulevaisuudessa. Selvitystyö tulee tehdä yhteistyössä ICT-asioihin perehtyneen johtajatasolla olevan asiakkaan työntekijän kanssa. Pienissä yrityksissä tämä ei välttämättä ole mahdollista. Niissä selvitystyö tulee tehdä ICT-asioihin perehtyneen henkilön kanssa. Selvittämällä tekniikkaa ja dokumentaatiota saadaan selville ovatko liiketoimintaprosessien omistajat ja tekniikan omistajat samalla linjalla turvallisuuden suhteen. Seuraavat dokumentit tulee pyytää nähtäväksi, verkon topologia, tietojärjestelmien asetuksia koskeva dokumentaatio, lokitiedostot, aikaisemmat auditointi tai tietoturvakartoitus dokumentaatiot. (Kairab 2005, 165-166.)

Dokumentaation analysoinin jälkeen haastatellaan ICT-johtajia. Haastattelussa tulisi esittää ainakin seuraavanlaisia kysymyksiä:

- Kuvaile millainen on yrityksen turvallisuus arkkitehtuuri?
- Kuvaile millaisia tietoturvallisuus prosesseja on käytössä?
- Missä kriittinen tieto sijaitsee?
- Missä kriittiset tietojärjestelmät sijaitsevat?
- Kuvaile karkean tason ICT-käyttäjien roolit ja vastuut.
- Kuvaile yhteistyö pääyhteistyökumppanin ja laitteistotoimittajien kanssa.
- Miten turvallisuus otetaan huomioon yrityksen ICT-organisaatiossa?
- Onko tietoturvallisuuspoikkeamia tapahtunut?
- Millaisia mekanismeja turvallisuuspoikkeamien havaintiin on käytössä?
- Millaisia muutoksia tietojenkäsittely-ympäristöön on tulossa?
- Millaisia huolenaiheita ICT-johdolla on tietoturvallisuuteen liityen?
- Miten kommunikaatio ICT-organisaation ja yrityksen muiden toimijoiden välillä toimii? (Kairab 2005, 166-170.)

Tekniikasta vastaavien tapaamiseen tulee valmistella kysymykset samaan tapaan kuin liiketoimintaprosesseita vastaaville. Kysymysten valmistelussa on otettava huomioon mitä on opittu asiakkaan liiketoimintaprosesseista, ICT-johdon haastatteluista ja muusta tiedosta mitä yriyksestä on tähän mennessä opittu. Kysymykset tulee suunnata koskemaan sitä teknologiaa josta kyseinen haastateltava on vastuussa. Yleisellä tasolla haastateltavalle tulee esittää vähintään seuraavanlaisia kysymyksiä:

- Millaisesta teknologiasta olet vastuussa ja mitä liiketoimintaprosessia se tukee?
- Miten vastaamasi teknologia sopii kokonaisarkkitehtuuriin?
- Millaiset ovat teknologian tietoturva vaatimukset?
- Miten tekniikka on suojattu?
- Onko tekniikan suojaamiseen pakollisia toimia?
- Sijaitseeko vastuullasi olevassa systeemissä krittiistä tietoa?
- Jos vastuullasi oleva systeemi ei ole käytettävissä, miten nopeasti sen saa takaisin käyttöön?
- Millaisia lokeja ja valvontatoimia te teette?

- Noudatetaanko muutoshallinnan toimenpiteitä mahdollisiin muutoksiin systeemissä?
- Onko vastuullasi olevissa systeemeissä ilmennyt tietoturvapoikkeamia?
- Onko vastuullasi oleviin systeemeihin tulossa muutoksia? (Kairab 2005, 170-174.)

Käytännön testaus pitää suunnitella huolellisesti asiakkaan henkilöstön kanssa. Tärkeää on ymmärtää mitä testataan ja miksi. Testattavien teknologioiden identifiointi tulee perustaa liiketoimintaprosesseihin perustuviin haastatteluihin ja ICT-johdon tapaamisissa hankittuihin tietoihin. Testausta suunniteltaessa tulee harkita testataanko manuaalisesti vai automaatttisin välinein. Jos on tarvetta hankkia maksullista ohjelmistoa testaukseen, tulee asiakkaalle esittää pääoman tuottoaste laskelma (ROI). (Kairab 2005, 174,182.)

Testausprosessi etenee karkeasti kuvattuna seuraavasti:

1. Teknologian omistajille ilmoitetaan testauksesta ja sovitaan aikataulu.
2. Hankitaan johdon hyväksyntä ja vastuuvapautus testaukselle.
3. Hankitaan tarvittava pääsy systeemeihin.
4. Testataan manuaalisesti ja automaattisin välinein.
5. Kerätään tietoa ja analysoidaan se. (Kairab 2005, 184.)

Yleisiä testauskohteita ovat mm. seuraavat:

- LAN, paikallinen verkko
- Kriittiset serverit
- Palomuurit
- IDS, tunkeutumisen tunnistusjärjestelmät. (Kairab 2005, 185-186.)

Testauksen apuna on hyvä käyttää erilaisia parhaiden käytänteiden standardeja kuten esim. OWASP (Open Web Application Security Project).

Tekniikan arvioinnin tuloksena saadaan tietoa haavoittuvuuksista ja suosituksista niiden korjaamiseksi. Tuloksia arvioitaessa tulee huomioida arvioitavaa tekniikkaa koskevat parhaat käytänteet ja standardit. Tässä vaiheessa pitää miettiä miten tekniikka tukee liiketoimintaa. Esille saattaa tulla haavoittuvuuksia jotka ovat välttämättömiä liiketoiminnan kannalta. Tällaiset haavoittuvuudet pitää hyväksyttää yrityksen johdolla ja samalla miettiä suositusta jolla minimoidaan vahingot liiketoiminnalle. Löydökset ja suositukset kirjataan loppuraporttiin. (Kairab 2005, 187.)

Tekniikan arvioinnin tilannekatsaus asiakkaan kanssa on tärkeä vaihe kokonaisuuden kannalta koska, se on ensimmäinen kerta kun asiakas saa tietoonsa kaikki kartoituksen löydökset. Löydöksistä tulee keskustella asiakkaan kanssa. Asiakkaalla saattaa olla ehdotuksia löydettyjen uhkien lieventämiseksi sekä asiakas saattaa pitää joitain löydöksiä hyväksyttävinä uhkina. (Kairab 2005, 189.)

5.5 Riskianalyysi ja loppuraportti

Riskianalyysin ja loppuraporttointi jaetaan viiteen osaan seuraavasti:

- Riskianalyysi ja –laskelmat
- Tulosten viimeistely
- Kehitysehdotukset ja raporttiluonnos
- Raportin läpikäynti
- Loppuraportin esittely

Riskien analysointiin käytetään kaikkea edellisissä osioissa kerättyä tietoa kokonaisuutena. Asiakkaan johto on tärkeää saada ymmärtämään riskien vaikutus liiketoimintaan. (Kairab 2005, 193.)

Valtiovarainministeriön tietoturvallisuuden johtoryhmän laatiman tietoturvaohjeistuksen, vahtiohjeen mukaan riskianalyysin tarkoituksena on:

- selvittää toiminnan ja palveluiden tietoturvatarpeet ja vaatimukset
- arvioida ulkoiset ja sisäiset riskit

- selvittää säädöksistä ja määräyksistä johtuvat tietoturvavaatimukset
- arvioida toiminnan ja tietotekniikan muutoksien vaikutukset tietoturvallisuuteen
- selvittää sidosryhmien odotukset
- määritellä tietoturvallisuuden tarpeet, periaatteet ja toteutustapa. (Vahti 1/2001, 25.)

Riskianalyysi tulee aina aloittaa kvalitatiivisella uhkien ja vaaratekijöiden analysoinnilla. Kvalitatiivisessa riskianalyysissa käsitellään aineettomia tietovarantoja kuten esimerkiksi tietoa. Taulukkoa 3. tai vastaavia voidaan käyttää kvalitatiivisen analyysin apuna. (Vahti 7/2003, 44 ; Krutz & Vines 2003, 18,23.) Taulukolla määritellään riskin merkittävyys. Yritys joutuu itse päättämään riskien merkittävyyden. Taulukkoon asetetaan uhkan todennäköisyys asteikolla alhainen, keskimääräinen ja korkea sekä uhkan seurausten vakavuus asteikolla vähäinen, vakava tai erittäin vakava. Tuloksena esim. keskimääräiselle uhkalle ja vakaville seurauksille saadaan kohtalainen riski.

Taulukko 3. Riskitaulukko (Vahti 7/2003, 43)

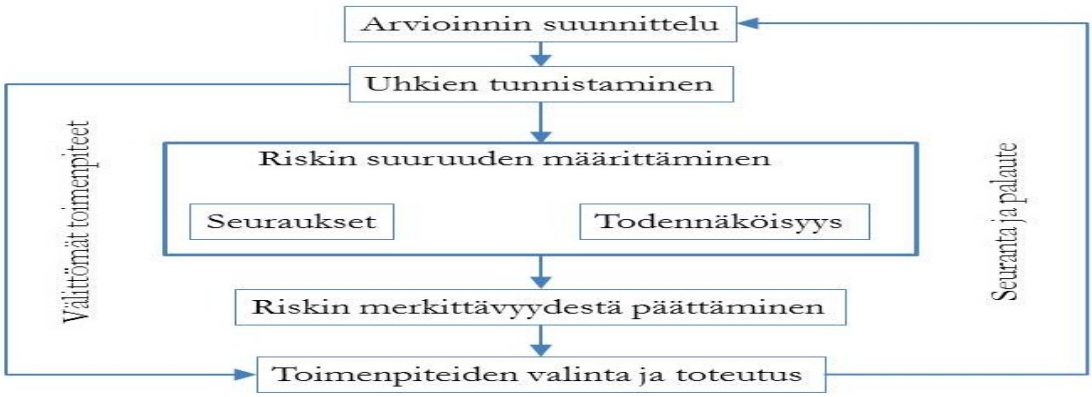
Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	Korkea (3)	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski
	Keskimääräinen (2)	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
	Alhainen (1)	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski

Riskien analysointia on mahdollista jatkaa kvantitatiivisella analyysilla, sillä pyritään määrittämään numeeriset arvot mahdollisille menetyksille. Kvantitatiivisen analyysin kolme tärkeintä vaihetta ovat:

1. omaisuuseriin kohdistuvien mahdollisten menetysten arvioiminen määrittämällä niille arvot
2. omaisuuseriin kohdistuvien mahdollisten uhkien analysoiminen
3. odotettavien vuotuisten menetysten määrittäminen. (Krutz & Vines 2003, 18-19.)

Riskin suuruuteen vaikuttavat uhkan toteutumisen seurausten vakavuus ja todennäköisyys. Usein uhkia löytyy niin paljon, että niitä kaikkia on mahdotonta yhdellä kertaa hoitaa. Kaikkiin uhkiin ei tarvitse kerralla löytää ratkaisua, vaan pitää pyrkiä tunnistamaan isoimmat riskit, jotka tulee kiireimmin ratkaista. (Vahti 7/2003, 41.)

Kuviossa 5. esitellään riskien arvioinnin ja hallinnan vaiheet. Aluksi uhkat tulee tunnistaa, riskin suuruus määritellään ja sen merkittävyys päätetään. Vakaville uhkille tehdään välittömät toimenpiteet, muita uhkia seurataan ja säännöllisin väliajoin uhkia arvioidaan uudelleen.



Kuvio 5. Riskien arvioinnin ja hallinnan vaiheet (Vahti7/2003, 16)

Kun riskit on saatu tunnistettua, tulee niitä pystyä hallitsemaan. Vahinkojen syntyminen on pyrittävä estämään tai vähentämään niiden seurauksia. Toimenpiteet riippuvat riskin suuruudesta. Kolme yleisintä vastakeinoa, joista voidaan valita yksi tai useampi käytettäväksi ovat:

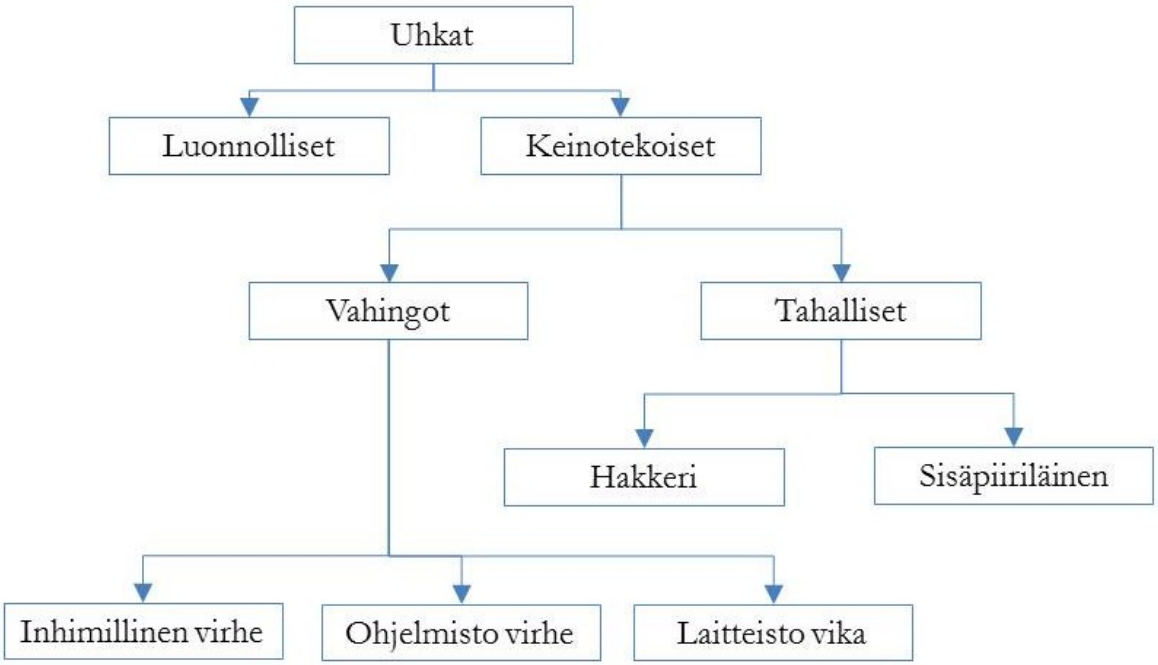
1. riskin pienentäminen, toimenpiteillä parannetaan tietovarannon asemaa riskiin nähden
2. riskin siirtäminen, siirretään riski toiselle esim. ottamalla vakuutus
3. riskin hyväksyminen, hyväksytään menetykset. (Vahti 7/2003, 45 ; Krutz & Vines 2003, 21.)

Riskianalyysin tuloksena tulisi syntyä seuraavat tiedot:

- kriittisten omaisuuserien arvo rahassa mitattuna
- luettelo merkittävistä uhkista
- uhkien toteutuessa omaisuuseriin kohdistuvista menetyksistä aiheutuvat kulut
- kunkin uhkan todennäköisyys ja sen mahdollinen esiintymistiheys
- suositeltavat parannustoimet ja turvamekanismit tai vastatoimet.(Krutz & Vines 2003, 20-21.)

Jotta Riskianalyysi voidaan suorittaa, tulee tunnistaa erilaiset uhkat. Uhkat jaetaan luonnollisiin ja keinotekoisiin uhkiin. Luonnolliset uhkat riippuvat siitä ympäristöstä jossa yritys sijaitsee. Luonnolliset uhkat esiintyvät satunnaisesti eivätkä ne ole mitenkään sidoksissa siihen millainen tietovaranto on. Pahin luonnollisen uhkan aiheuttama seuraamus on todennäköisesti palvelun saatavuuden heikentyminen. Vahinkoja voi sattua koska vaan ja kenelle tahansa. Vahingot eivät voi ennalta määritellä minne ne osuvat, eikä niiden seuraamuksia siten voida ennalta arvioida. Bugit ym. arvaamattomat vahingot voivat aiheuttaa vakavia vahinkoja tietovarannolle. Tahalliset uhkat ovat usein tarkoituksella tiettyä uhria kohtaan suunnattuja. Tahalliset uhkat ovat vaarallisimpia koska yleensä hyökkääjät ovat etukäteen laskeneet mitä voivat hyökkäämällä saavuttaa. (Raggad 2010, 82-83.)

Kuviossa 6. esitellään uhkien luokittelu. Uhkat jaetaan luonnollisiin ja keinotekoisiin uhkiin. Keinotekoiset puolestaan jaetaan vahinkoihin ja tahallisiin uhkiin. Vahingot jakautuvat inhimillisiin virheisiin, ohjelmisto virheisiin ja laitteistovikoihin. Tahalliset uhkat jaetaan hakkereiden ja sisäpiiriläisten aiheuttamiin.



Kuvio 6. Uhkien luokittelu. (Raggad 2010, 84)

Uhkia voidaan tarkastella monella eri tasolla. Ensimmäisen tason uhkia kutsutaan juuriuhkiksi. Oletetaan että yrityksen toimitilat joutuvat maanjäristyksen ruhjomiksi. Tällöin juuriuhka on maanjäristys. Kuvitellaan, että maanjäristyksen johdosta kiinteistö jossa yritys sijaitsee syttyy tuleen, tällainen uhka on toisen tason uhka. Tulipalon seurauksena sähköt menevät poikki ja sähköjen katkeaminen aiheuttaa jäähdytyksen katkeamiseen, tällöin kyseessä on neljännen tason uhka, uhkat alenevat portaittain. Alla selvennys uhkien porrastuksesta:

- juuriuhka - maanjäristys
- toisen tason uhka – tulipalo
- kolmannen tason uhka – sähköjen katkeaminen
- neljännen tason uhka – jäähdytyksen katkeaminen. (Raggad 2010, 83-86.)

Uhkien Todennäköisyyttä voidaan mitata erilaisilla asteikoilla, lähteistä riippuen asteikot vaihtelevat kolme- neljä- ja viisiportaisiin.

Riskianalyysin tulokset kirjataan loppuraporttiin. Kirjattaessa riskejä tulee huolellisesti miettiä miten tulokset esitetään. Tarkoituksena ei ole yksilöidä riskejä henkilötasolle,

ellei se ole aivan välttämätöntä. Kerrottaessa riskeistä tulee myös mainita, olevassa olevat turvallisuustoimet riskikohtaisesti. Yleisesti ottaen, tulosten esittämisen valmisteluun tulee käyttää tervettä maalaisjärkeä. (Kairab 2005, 205-208.)

Tässä vaiheessa loppuraportista puuttuu vain suositukset. Asiakas on yleensä erittäin kiinnostunut suosituksista. Usein suositukset ovat syy käyttää ulkopuolista konsultointia tietoturvakartoituksen apuna. Suositusten valmisteluun tulee paneutua huolellisesti, koska ne ovat sekä konsultin, että asiakkaan näkökulmasta tietoturva-osaamisen näytön paikka. Suositusten tulee toimia tietoturvallisuuden suunnannäyttäjänä asiakkaalle. (Kairab 2005, 210-212.)

Suositusten tulee perustua riskeihin, olla kustannustehokkaita ja tarjota tarpeeksi tietoa asiakkaalle. Päätös tietoturvainvestoinnin tekemisestä tulee usein yrityksen ylimmästä johdosta. Johdolle tulee pystyä selvittämään riski, hinta, aika ja resurssit joita suositus koskee. Loppuraportin muoto tukee tällaista selvitystä, koska löydöksille on oma osionsa, jokaiselle löydökselle oma riski ja jokaiselle löydökselle oma suositus. Raportoinnin avuksi on tässä vaiheessa hyvä ottaa tietoturvainvestoinnin tuottolaskelma (ROSI), joka on kuvailtu sanastossa. (Kairab 2005, 214-218.)

Varsinaisten tietoturvallisuutta koskevien suositusten antamisen jälkeen on syytä antaa suosituksia yleisellä tasolla koskien, muita käynnissä olevia kartoituksia, yrityksen käyttämiä tietoturva yms. palveluja ja palvelutaso-, l. SLA-sopimuksia. Yleisten suositusten ei tarvitse välttämättä koskea riskiä, vaan enemminkin olla strategisella tasolla. (Kairab 2005, 218-219.)

Tässä vaiheessa viimeistellään loppuraportti. Asiakkaalle esitellään riskit ja suositukset sekä raporttia tarkastellaan kokonaisuutena. Tapaamiseen kannattaa kutsua sellaisia asiakkaan edustajia jotka ovat olleet mukana koko kartoituksen ajan, jotta he voivat kommentoida raporttia konaisuutena. Konsultin näkökulmasta katsottuna raportin tarkastelulla on seuraavia hyötyjä. Asiakkaan antamat lisätiedot koskien suosituksia, sekä asiakkaan edustajan antamat suuntaviivat johdon odotuksille raportista. Yrityksen oman henkilöstön hyväksyntä raportille antaa sille johdon silmissä uskottavuutta. Yleinen syy ulkopuolisen kartoitustiimin käyttöön on puolueettomuus, asiakas odottaa että pysyt

ulkopuolisen konsultin puolueettomassa roolissa tapaamisissa läpi projektin myös viimeisessä tapaamisessa. Asiakkaan edustajien ehdotukset suositusten muuttamiseksi kirjataan raporttiin ja raportti viimeistellään esitettävään muotoon.(Kairab 2005, (222-224.)

Lopuksi raportoidaan asiakkaan johdolle. Johdolle on hyvä tehdä erillinen esitys jollakin esitysgrafiikka-ohjelmistolla. Esityksessä tulee mainita, projektin rajaus, käytetyt metodit, löydökset, riskit ja suositukset. (Kairab 2005, 225-226.)

6 Yritys X:n tietoturvallisuuden kartoitus

6.1 Suunnittelu

Tutkimuksen tavoitteena on tarkastella yrityksen tietoturvallisuutta. Tutkimus toteutetaan kahdessa osassa. Ensimmäisessä osassa selvitetään yrityksen tietoturvallisuuden nykytila ja toisessa osassa tarkastellaan esimerkinomaisesti liiketoimintaprosesseja. Tutkimuksen tuloksena saadaan selville yrityksen tietoturvallisuuden nykytila sekä liiketoimintaprosessien uhkatekijöitä. Tulosten perusteella annetaan suosituksia tilanteen parantamiseksi.

Tietoturvallisuuden nykytilan kartoitus tutkimuksen tavoitteena on tutkia miten hyvin yritys täyttää valtiovarainministeriön määrittelemät tietoturvallisuuden perustason tietoturva vaatimukset. Tiedonkeräys metodeina, nykytilan kartoituksessa käytetään kyselytutkimusta sekä toimitilojen silmämääräistä tarkastamista. Kyselytutkimuksen kysymykset perustuvat Valtiovarainministeriön tietoturvatasot, organisaation arviointi taulukkoon. Kaikkia taulukon kysymyksiä ei esitetä, johtuen tutkittavan yrityksen koosta, toimialasta sekä, siitä että kaikki kysymykset eivät ole oleellisia tutkittavan yrityksen kannalta. Tutkimuksen tuloksena saadaan selville yrityksen tietoturvallisuuden nykytila. Tulosten perusteella annetaan suosituksia tietoturvallisuuden parantamiseksi.

Liiketoimintaprosessien tarkastelun tarkoituksena on esimerkinomaisesti tutkia yrityksen liiketoimintaprosesseja. Liiketoimintaprosesseja tarkastellaan sen johdosta, että yrityksellä olisi tulevaisuudessa metodi jolla lähteä kehittämään tietoturvallisuutta liiketoi-

mintaprosessien näkökulmasta. Yrityksen ei ole tarkoituksenmukaista lähteä kehittämään tietoturvaansa liiketoimintaprosessillisista lähtökohdista, ennen kuin se täyttää perustasolle asetetut vaatimukset. Liiketoimintaprosessien arviointi tehdään Kairabin mallin pohjalta. Yrityksen ydinprosessit kartoitetaan, sen henkilökunnalle tehtävin haastatteluin. Haastattelujen kysymykset perustuvat työn teoriataustaan sekä Kairabin teoksessa A practical guide to security assesment esittämiin kyselytutkimusta tukeviin kysymyksiin. Ydinprosesseista valitaan yksi prosessi tarkempaan tarkasteluun. Tarkasteluun valittu prosessi mallinnetaan prosessikarttana. Valitulle prosessille tehdään suppea riskikartoitus haastattelemalla yrityksen henkilökuntaa. Löydetyille riskeille annetaan korjausehdotukset.

6.2 Toteutus

Tutkimus aloitettiin selvittämällä yrityksen liiketoiminnallisia motiiveja tutkimukselle. Yrityksen johtoa haastattelemalla selvisi, että liiketoiminnalliset motiivit kartoitukselle ovat johdon yleinen kiinnostus parantaa yrityksen tietoturvaa sekä aikaisempien tietoturvapoikkeamien kaltaisten tilanteiden ehkäisy. Kohdeyrityksenä oli liiketoiminnan kehittämisen ratkaisuja tarjoava yritys.

Yrityksen tietoturvallisuuden nykytila kartoitettiin tekemällä kyselytutkimus. Kyselyyn käytetyt kysymykset ovat liitteessä 2. Kyselyn kysymykset on valittu niin, että ne sisältävät kysymyksiä hallinnollisen tietoturvan, henkilöstöturvallisuuden sekä laitteistoturvallisuuden osa-alueista.

Kyselytutkimuksen tuloksena saatiin selvitettyä kohdeyrityksen tietoturvallisuuden taso. Löydösten perusteella annettiin suosituksia tietoturvallisuuden parantamiseksi. Kriittisiin löydöksiin pyrittiin löytämään korjaavat toimenpiteet. Yritykselle laadittiin tietoturvapolitiikka, tietoturvan kehittämisen suunnannäyttäjäksi. Löydösten perusteella yrityksen käyttämä varmuuskopionti ratkaisu tarkastettiin ja varmuuskopion palauttaminen testattiin.

Yrityksen johtoa haastattelemalla selvitettiin yrityksen ydinprosessit. Haastattelun kysymykset ovat liitteessä 3. Yksi ydinprosessi valittiin tarkempaan tarkasteluun ja se ku-

vattiin prosessikarttana. Haastattelujen perusteella, tarkempaan tarkasteluun valitulle prosessille tehtiin suppea riskikartoitus. Löydetyille riskeille annettiin korjausehdotukset. Yritykselle laadittiin salasanojen luontiohje, koska tutkimuksen mukaan sille oli tarvetta. Yrityksen kykyä toimia katastrofin sattuessa parannettiin laatimalla jatkuvuussuunnitelma.

7 Johtopäätökset ja pohdinta

Tutkimus keskittyi tietoturvallisuuteen. Lähtökohta tutkimukselle oli kohdeyrityksen halu ja tarve selvittää oma tietoturvallisuuden taso ja kehittää sitä eteenpäin. Työn teoreettisena tavoitteena oli tutkia mitä on tietoturva sekä miten tietoturvakartoitus tehdään konsultin näkökulmasta katsoen sekä empiirisesti tutkia millainen kohdeyrityksen tietoturvallisuuden nykytila on ja miten sitä on mahdollista kehittää.

Tutkimuksen teoriaosassa tutkittiin tietoturvallisuuden käsitteistöä. Aluksi selvitettiin mitä on tietoturva ja millaisista osa-alueista se koostuu. Tietoturvallisuusprosessiin luotiin katsaus jossa esiteltiin tietoturvakartoitus sekä tietoturvatasot. Tietoturvallisuuden perustason vaatimukset selvitettiin. Tarkemmin pohdittiin johtajuudelle, henkilöstölle ja tietojärjestelmille asetettavia vaatimuksia. Tietoturvallisuuden perustasolla vaadittaviin dokumentteihin luotiin katsaus ja pohdittiin miten tiedot ja tietojärjestelmät luokitellaan yrityksessä.

Tietoturvakartoitusta konsultin näkökulmasta tutkittiin perehtymällä kirjallisuuteen. Tietoturvakartoituksen malliksi valittiin Kairabin laatima malli, joka on joustava ja helposti muokattavissa kohdeyrityksen tarpeisiin sopivaksi. Kairabin malli soveltuu hyvin sekä konsultin tekemän kartoituksen että yrityksen sisäisesti tekemän kartoituksen malliksi.

Empiirinen tutkimus jaettiin kahteen osaan. Ensimmäisessä osassa selvitettiin kohdeyrityksen tietoturvallisuuden nykytila. Tutkimusmetodeina käytettiin kyselytutkimusta sekä toimitilojen silmämääräistä tarkastamista.

Tietoturvan nykytilan kartoituksen perusteella havaittiin, että yritys on toteuttanut hyvin monia tietoturvallisuuden kannalta oleellisia asioita. Yrityksessä on ymmärretty tietoturvallisuuden merkitys liiketoiminnalle. Yrityksen tietoturvallisuuden todettiin olevan aloittavalla tasolla. Suurimmat ongelmakohdat yrityksen tietoturvallisuudessa kohdistuivat pääasiassa hallinnolliseen tietoturvaan. Puutteita havaittiin mm. dokumentoinnissa. Kriittiset puutteet korjattiin projektin aikana. Yritykselle laadittiin tietoturvapolitiikka tietoturvan kehittämisen suunnannäyttäjäksi.

Toisessa osassa arvioitiin esimerkinomaisesti yrityksen liiketoimintaprosesseja. Yrityksen johtoa haastattelemalla selvitettiin yrityksen ydinprosessit. Yksi ydinprosessi valittiin tarkempaan tarkasteluun ja sille tehtiin suppea riskikartoitus. Riskikartoituksen pohjalta annettiin suosituksia, riskien korjaamiseksi. Yritykselle laadittiin mm. salasanojen laatimisohjeet.

Yhteenvetona todetaan, että tehty tutkimus vastasi hyvin tutkimusongelmiin. Tietoturvallisuudesta ja tietoturvakartoituksen tekemisestä konsultin näkökulmasta katsoen muodostettiin hyvä yleiskuva. Kartoituksella saatiin selville yrityksen tietoturvallisuuden nykytila. Liiketoimintaprosessit saatiin kartoitettua ja valitulle ydinprosessille tehtyä suppea riskikartoitus. Löydöksille annettiin suosituksia tilanteen parantamiseksi. Kartoituksen pohjalta kohdeyritys pystyy kehittämään omaa tietoturvallisuuttaan. Tutkimusta voidaan jatkaa Kairabin mallin mukaisesti.

Tietoturvakartoituksen tekeminen on haasteellinen tehtävä. Kartoitusta suunniteltaessa tulee ottaa huomioon erilaisia tekijöitä mm. millainen toimintaympäristö tutkittavassa kohteessa on sekä millaiset ovat liiketoiminnalliset motiivit kartoitukselle, että millaista osaamista kartoitus vaatii. Kartoituksen tekeminen vaatii osaamista kaikista tietoturvan osa-alueista. Ammatillisesti projekti on ollut hyvin antoisa, uutta tietoa on ollut mahdollista ammentaa koko prosessin ajan.

Lähteet

HAAGA-HELIA ammattikorkeakoulu 2005. Anne Valsta, Seppo Salo. Projektisuunnitelma.
Luettavissa: http://myy.haaga-helia.fi/~valan/ict05%20projekti%20ohje%20projektisuunnitelma.pdf
Luettu 10.10.2012

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

Järvinen, P. 2002. Tietoturva ja yksityisyys. Docendo. Jyväskylä.

Järvinen, P. 2010. Yksityisyys, turvaa digitaalinen kotirauhasi. Docendo. Jyväskylä.

Kairab,S. 2005. A practical guide to security assessments. Auerbach Publications. Boca Raton

Krutz & Vines 2003. Tietoturvasertifikaatti – CISSP. IT Press. Helsinki.

Laaksonen ym. 2006. Yrityksen tietoturvakäsikirja – ohjeistus, toteutus ja lainsäädäntö. Edita. Helsinki.

Raggad, B. 2010. Information security management – Consepts and practice.CRC Press. Boca Raton.

Ruohonen, M. 2002. Tietoturva. Docendo. Porvoo.

Suomen Standardoimisliitto SFS 2006. ISO/IEC 17799:fi -standardi. Helsinki.

Suomen Standardoimisliitto SFS 2006. ISO/IEC 27001:fi -standardi. Helsinki.

Tietosuojavaltuutetun toimisto 2010. Sanastoa.

Luettavissa: http://www.tietosuoja.fi/27247.htm.

Luettu 16.2.2012

Valtiovarainministeriö 2006. Tietoturvallisuuden arviointi valtionhallinnossa (VAHTI 8/2006)
Luettavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf
Luettu 16.2.2012

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia. (VAHTI 3/2007)

Luettavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=8c85fe8f-aa4c-4e67-9236-2fee696498a9&groupId=10128&groupId=10229

Luettu: 15.9.2012

Valtiovarainministeriö 2011. Tietoturvatasot, organisaation arviointi-taulukko

Luettavissa:

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20101215Tietot/name.jsp

Luettu: 5.10.2012

Valtiovarainministeriö 2008. Tietoturvatasot käsikirja

Luettavissa:

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/02_TTT-kaesikirja-20081029.pdf

Luettu: 1.9.2012

Valtiovarainministeriö 2008. tietoturvatasot käsikirja Liite 1

Luettavissa:

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/03_TTT-kaesikirja-Liite1-org-kypsyys-20081030.pdf

Luettu: 1.9.2012

Valtiovarainministeriö 2008. tietoturvatasot käsikirja Liite 2

Luettavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/04_TTT-kaesikirja-Liite2-IT-kypsyys-20081030.pdf
Luettu:1.9.2012

Valtiovarainministeriö 2009. Vahti-ohjeet ohjelmisto ja ohjelmistokehityksen turvallisuus
Luettavissa: https://www.vahtiohje.fi/web/guest/ohjelmisto-ja-ohjelmistokehityksen-turvallisuus
Luettu 21.11.2012

Valtiovarainministeriö 2010. VAHTI-ohje 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta Liite 5
Luettavissa: https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta
Luettu 1.10.2012

Valtiovarainministeriö 2003. Valtionhallinnon tietoturvakäsitteistö
Luettavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf
Luettu 16.2.2012

Viestintävirasto 2004. Suositus määräyksen Viestintävirasto 47B/2004M soveltamisesta teleyrityksen tietoturvasta.
Luettavissa:
http://ficora.fi/attachments/suomi_R_Y/1156442754964/Files/CurrentFile/SMS47B.pdf
Luettu: 16.2.2012

Viestintävirasto 2009. Tietoturva ja -suoja.
Luettavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html
Luettu 16.2.2012

Liitteet

Liite 1. Tietoturvallisuuden perustason vaatimukset

Johtajuudelle asetettavat vaatimukset

- Yrityksellä on tiedossa toimintaansa koskeva lainsäädäntö ja niistä tiedottaminen on organisoitu ja vastuutettu
- Yritys on tunnistanut ydintoimintonsa ja –prosessinsa.
- Yrityksellä on kirjallinen johdon hyväksymä tietoturvapolitiikka.
- Yritykseen on nimetty tietoturvavastaava ja hänellä on aikaa tietoturvavastuidensa suorittamiseen.
- Yrityksen johto ja tietoturvallisuudesta vastuussa olevat keskustelevat säännöllisesti.
- Yrityksellä on säännöllisesti kokoontuva tietoturva-asioita käsittelevä työryhmä.
- Yritys on tunnistanut sidosryhmät joille se on tietoturvasta vastuussa.
- Yrityksen johto on organisoinut ja vastuuttanut sidosryhmiin vaikuttavien tietoturva-asioiden raportoinnin sekä tietoturvapoikkeamista tiedottamisen.
- Tietoturvapoikkeamien käsittely on organisoitu ja vastuutettu.
- Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.

Toiminnan suunnittelulle asetettavat vaatimukset

- Yritys on tunnistanut erilliset tietojenkäsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät sekä toiminnot.
- Yritys on tunnistanut tietoturvallisuuden osalta kunkin toimintaympäristön erityisvaatimukset ja tavoitteet.
- Yritys on tunnistanut ydintoimintojen ja –prosessien tietoturvallisuuden kannalta suojattavat kohteet ja luokitellut ne vaadittavan tietoturva tason mukaisesti.
- Tietoturvatavoitteita on liitetty ydintoimintojen sekä –prosessien tavoitteisiin.
- Yrityksessä tehdään säännöllisesti tietoturva riskien arviointia.
- Yritys parantaa tietoturvallisuuttaan riskien arvionnista saatujen tulosten perusteella, liian suurten riskien osalta johdon päättämillä toimenpiteillä.

- Yrityksellä on tiedossa, millaisissa toiminta verkostoissa se on mukanasekä mitä alihankkijoita ja yhteistyökumppaneita sen tietojen kanssa toimii missäkin roolissa.
- Yrityksellä on jatkuvuussuunnitelma tai –suunnitelmia.

Henkilöstölle asettavat vaatimukset

- Yritys järjestää säännöllisesti tietoturvakoulutusta henkilöstölle.
- Tietoturva-asiat otetaan esille perehdyttäessä.
- Tietoturvaohjeiden ja –käytänteiden muutoksista tiedotetaan kaikille yrityksessä toimiville.
- Yritys seuraa tietoturva sääntöjen noudattamista.
- Suomen erityisvaateena on että työntekijöiden tekninen valvonta on käsitelty YT-menettelyn mukaisesti (Laki yksityisyyden suojasta työelämässä, 21§).
- Yritys on vastuuttanut toteuttavaksi valitut tietoturva toimenpiteet ja –prosessit.
- Yritys on tunnistanut tietoturvallisuuden avainroolit ja niille on nimetty varahenkilö tai –henkilöt.
- Yrityksen henkilöstö tietää kenelle tietoturvapoikkeamista ja –tapauksista ja niiden uhkista tulee raportoida.

Kumppanuuksille ja resurssien hallinnalle asetettavat vaatimukset

- Yritys on vastuuttanut ja organisoinut kumppanuus ja hankintatoiminnan.
- Yritys laatii kirjallisen sopimuksen kumppanin kanssa, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu.
- Yritys on organisoinut ja vastuuttanut tietoturvallisuuden valvonnan sekä poikkeamien kirjaamisen yhteistyön kohteena olevaan kohteeseen liittyen.
- Kumppanille tiedotetaan välittömästi havaituista kumppania koskevista tietoturvapoikkeamista ja poikkeaman korjaustoimet aloitetaan sovitusti.

Toiminnan prosesseille asetettavat vaatimukset

- Tietoaineiston käsittely yrityksessä on määritelty.
- Asiakirjoista käy ilmi kuka sen on tehnyt, milloin ja mikä on sen hyväksymisen tila.
- Asiakirjat tuhotaan niin, että niiden luottamuksellisuus ja tietosuoja on varmistettu.
- Yrityksen työntekijät tietävät miten tietoaineisto käsitellään.
- Yrityksellä on luettelot sen omistamista ja käyttämistä fyysisistä tai virtuaalisista laitteista, palveluista, tietojärjestelmistä, ohjelmistoista ja lisensseistä.
- Yritys on vastuuttanut laitteiden, rekisterien ja tietojärjestelmien omistajuuden ja päivityksen.
- Tietoturvallisuuden auditointeja ja arviointeja tehdään säännöllisesti.
- Arvioinnit ja auditoinnit ovat suunniteltuja ja johdon hyväksymiä.
- Auditoinneista ja arvioinneista raportoidaan kohteen tai toiminnon omistajalle.
- Arvioinneista ja auditoinneista pidetään kirjaa ja parannustoimenpiteiden toteutumista seurataan.

Tietojärjestelmien hallinnan vaatimukset

Raportointi tietoturvavastaavalle

- Vakavat tietoturvapoikkeamat raportoidaan tietoturvavastaavalle välittömästi.
- Tietoturvallisuuden tilasta raportointi on vastuutettu ja organisoitu.

Tietojenkäsittely-ympäristöjen käyttöönotto ja poisto

- Tietoturvavaatimukset otetaan huomioon poistettaessa tietojärjestelmiä tai työasemia käytöstä.
- Yritys on vastuuttanut tietojärjestelmien ja työasemien käytöstä poistamisen ja käyttöönoton.

Tietojenkäsittely-ympäristöjen päivitys ja muutoshallinta

- Tietoturvapäivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on laitteiden ja tietojärjestelmien osalta vastuutettu ja organisoitu.
- Yrityksessä seurataan laitteiden ja tietojärjestelmien muutostarvetta, muutospäätösten teko ja toteutus on vastuutettu ja organisoitu.
- Yritys on määrittänyt periaatteet siitä millaiset päivitykset ja muutokset asennetaan välittömästi ja millaisiin muutoksiin tai pävityksiin käytetään riskitason huomioivaa tarveharkintaa.

Turva-alueiden muodostus ja niiden välinen suodatus

- Yritys on tunnistanut ja eriyttänyt tietoverkon eri suojaustasoa vaativat osat. Verkkojen välisen suojaustason ollessa erisuuruinen, verkkojen välistä liikennettä rajoitetaan ja suodatetaan.
- Yritys on vastuuttanut ja organisoinut palomurien ja muiden tietoliikennelaitteiden sääntöjen lisäämisen, muuttamisen ja poistamisen.
- Yrityksessä on etäkäyttöperiaatteet.
- Palomuurien ja muiden tietoliikennelaiteiden suodatussäännöt on dokumentoitu.

Pääsynvalvonta

- Yrityksen palomuurit ja muut tietoliikennelaitteet noudattavat sisäänpäin tulevan liikenteen osalta ”kaikki liikenne on kielletty ellei erikseen sallittu” periaatetta.
- Yrityksestä julkiseen verkkoon lähtevää liikennettä suodatetaan.
- Yrityksessä estetään huonolaatuisten salasanojen käyttöä.

Käyttäjien ja käyttövaltuuksien hallinta

- Yrityksessä on laadittu periaatteet siitä, kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmien sisältämien tietojen käyttöön tarvitaan ja että, niitä noudatetaan.

- Yritys pitää lokia tietojärjestelmiin kirjautumisesta niin, että onnistuneet ja epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin. Yksittäisen käyttäjän kirjautumiset järjestelmiin tulee voida yhdistää hänen henkilöllisyyteensä sekä selvittää luotettavasti.
- Yrityksessä on laadittu käyttövaltuuksien hallintaperiaatteet. Periaatteen mukaisesti myönnettävien tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on vastuutettu ja organisoitu.
- Käyttövaltuudet ja tunnukset ovat henkilö- ja roolikohtaisia.
- Käyttövaltuuksien tulee perustua palvelusuhteeseen tai muuhun kirjalliseen sopimukseen. Perusteen päätyttyä, järjestelmien käyttö estetään ilman tarpeetonta viivytystä.
- Käyttövaltuudet yksittäisen käyttäjän kohdalta tulee voida selvittää.
- Uuden henkilön yritykseen tulee ensimmäinen tunnistus tehdä virallisesta kuvallisesta henkilöllisyystodistuksesta. Uuden käyttäjän rekisteröityessä sähköiseen palveluun tulee rekisteröitymisen osalta käyttää samantasoista todennusmenetelmää.

Haittaohjelmasuodatus

- Yrityksessä on käytössä työasemakohtainen haittaohjelmasuodatus, sekä kaikkia sähköpostin sekä www-liikenteen sisääntulo ja ulosmeno pisteitä suodatetaan haittaohjelmilta.
- Haittaohjelmakuvaukset päivittyvät automaattisesti ja säännöllisesti.

Fyysisen ympäristön suojaus

- Yritys on tunnistanut omien tilojen tarvitseman suojausluokan ja eriyttänyt eri suojausluokkaa vaativat osat rajoittamalla kulkua niiden välillä.
- Pääsyä IT-laite tiloihin valvotaan ja yrityksessä on sovittu henkilö- tai roolitasolla, kenellä on tiloihin pääsyoikeus.

Varmuuskopiointi

- Yritys on vastuuttanut ja organisoinut varmuuskopioiden ottamisen.

- Yritys on tunnistanut varmuuskopionnin kannalta tärkeimmät suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti.
- Varmuuskopioiden palauttaminen on suunniteltu ja testattu.

Tietoturvapoikkeamat

- Yritys on laatinut toipumisstrategian ja -suunnitelman tärkeimpien omien järjestelmien häiriöille. Yrityksen johdon tulee hyväksyä tärkeysjärjestys.
- Yritys on vastuuttanut ja organisoinut tietojärjestelmien häiriöiden selvittämisen ja niistä toipumisen.

(Valtiovarainministeriö VAHTI-ohje 2/2010 liite 5, 2010, 96-125.)

Liite 2. Tietoturvallisuuden nykytilan kartoituksen kysymykset

Yritys on tunnistanut ydintoimintonsa ja –prosessinsa sekä organisoinut ja vastuuttanut ne?

- Kyllä
- Ei

kunkin avaintoiminnon ja –prosessin kannalta suojattavat kohteet on tunnistettu ja luokiteltu vaadittavan tietoturvatason mukaisesti?

- Kyllä
- Ei

Avaintoimintojen tai –prosessien tavoitteisiin on liitetty myös tietoturvatavoitteita?

- Kyllä
- Ei

Yrityksellä on kirjallinen johdon hyväksymä tietoturvapolitiikka?

- Kyllä
- Ei

yritykseen on nimetty tietoturvavastaava ?

- Kyllä
- Ei

Yrityksessä pidetään kirjaa vakavista tietoturvapoikkeamista?

- Kyllä
- Ei

Erilliset tietojenkäsittelyn toimintaympäristöt ja niihin kuuluvat järjestelmät ja toiminnot on tunnistettu ja luetteloitu?

- Kyllä

Onko yrityksellä käytössä tietoturvariskien arvioinnin menetelmä?

- Kyllä
- Ei

Yrityksessä tehdään tietoturvariskien arviointia?

- Kyllä
- Ei

Yrityksellä on jatkuvuussuunnitelma?

- Kyllä
- Ei

Henkilöstölle järjestetään tietoturvakoulutusta?

- Kyllä
- Ei

Yritys on luetteloinut omistamansa fyysiset ja virtuaaliset laiteensa, palvelunsa, ohjelmistonsa sekä lisenssinsä?

- Kyllä
- Ei

Laitteiston ja tietojärjestelmien omistajuus on vastuutettu ja organisoitu?
Omistaja on henkilö jolla on valta tehdä laitteistoon muutoksia kuten päättää käytöstä poistosta.

- Kyllä
- Ei

Tietojärjestelmien ja työasemien käyttöönottoasennuksessa ja käytöstä poistamisessa otetaan huomioon järjestelmien tietosisällön tietoturvavaatimukset?

- Kyllä
- Ei

Palomuurien tai muiden suodatuslaitteiden suodatussäännöt on dokumentoitu?

- Kyllä
- Ei

Yrityksessä on vastuutettu palomuurien ja muiden suodatuslaitteiden sääntöjen lisääminen, muuttaminen ja poistaminen?

- Kyllä
- Ei

Yrityksellä on etäkäyttöperiaatteet?

- Kyllä
- Ei

Yritys on määritellyt kuinka vahvaa tunnistautumista järjestelmien sisältämien tietojen käyttö vaatii?

- Kyllä
- Ei

Yrityksessä estetään huonolaatuisten salasanojen käyttöä?

- Kyllä
- Ei

yrityksessä suodatetaan haittaohjelmia sekä työasematasolla että kaikissa sähköposti ja WWW–liikenteen sisääntulo- ja ulosmenopisteissä?

- Kyllä
- Ei

Haittaohjelmakuvaukset päivittyvät automaattisesti ja säännöllisesti?

- Kyllä
- Ei

Yrityksessä on vastuutettu ja organisoitu varmuuskopioiden ottaminen?

- Kyllä
- Ei

Yrityksessä on tunnistettu varmuuskopioinnin kannalta olennaiset suojattavat kohteet ja niistä otetaan varmuuskopioita suunnitelman mukaisesti?

- Kyllä
- Ei

Liite 3. Liiketoimintaprosessien arvioinnin kysymykset

- Miten prosessia tukeva teknologia on suojattu?
- Kenellä on käyttöoikeudet prosessia tukevaan teknologiaan ja miten käyttöoikeuksia valvotaan?
- Onko käyttäjätunnusten luonnille ohjeistusta?
- Kuka on vastuussa prosessia tukevan teknologian ylläpidosta?
- Jos prosessia tukeva teknologia ei ole käytettävissä, eikä prosessia voida toteuttaa, millaiset ovat vaikutukset tuloihin ja imagoon?
- Mikä on hyväksyttävä toiminnon keskeytysaika?
- Onko olemassa manuaalisia toimenpiteitä jotka voidaan tehdä jos teknologia ei ole käytettävissä?
- Miten pitkään manuaalisia toimenpiteitä voidaan tehdä?
- Millaista kriittistä tietoa prosessin tuloksena syntyy ja missä sitä säilytetään?
- Onko fyysinen kovalevy jolla kriittinen tieto sijaitsee salattu l. kryptattu?
- Mikä tietoturvassa tällä hetkellä huolestuttavat?
- Onko liiketoimintaan tiedossa muutoksia?
- Millaisia tietoturvatapahtumia teillä on aikaisemmin ilmennyt?

Liite 4. Yritys X:n tietoturvakartoitus (Salattu).

Liite 5. Loppuraportti

Taustaa

Tietoturvallisuus suojaa tietoa, joka on yritysten tärkeimpiä voimavaroja. Tiedon suojaaminen on edellytys menestyvän liiketoiminnan harjoittamiseen. Projektin päämääränä oli oppia mitä on tietoturva sekä miten yrityksen tietoturvaa kartoitetaan ja kehitetään. Valitsin tietoturvallisuuden opinnäytetyön aihepiiriksi, koska aihe on ajankohtainen ja halusin kehittää ammatillista osaamistani tietoturvallisuudesta.

Saavutetut tulokset

Projektisuunnitelmassa määriteltiin projektille seuraavat tehtävät ja tavoitteet:

- tutkia tietoturvaa perehtyen kirjallisuuteen
- tutkia kohdeyrityksen tietoturvan nykytilaa
- tehdä kohdeyritykselle tietoturvakartoitus.
- laatia havaituista puutteista korjausehdotukset
- laatia nykytilan kartoitus raportti
- laatia riskianalyysi
- tarpeen mukaan laatia ohjeistusta tietoturvan parantamiseksi.

Projektin tehtävät ja tavoitteet saatiin tutkimustyöllä täytettyä. Projekti on ollut opettavainen ja mielenkiintoinen. Uutta tietoa on ollut mahdollista ammentaa koko projektin ajan.

Opinnäytetyöprosessi on opettanut projektin hallintaa ja ollut aika-ajoin haastavaa aikataulujen suhteen. Lähteiden etsiminen on ollut välillä varsin haasteellista ja siihen kuluu paljon aikaa. Tekstin tuottaminen ilman inspiraatiota ei ole minulta onnistunut, välillä on kulunut päiviäkin ilman että olen saanut mitään järkevää kirjattua ylös. Sitten kun inspiraatio iskee, tekstiä on parhaimmillaan virrannut ulos tuntien ajan yhteen soittoon. Projekti on ollut opettavainen, olen oppinut itsestäni työskentelijänä sekä itse projektin teosta että itse aiheesta.

Prosessi, työn eteneminen

Työ aloitettiin perehtymällä tietoturvallisuutta koskevaan kirjallisuuteen. Kirjallisuutta oli valtavasti saatavilla, hyvien lähteiden etsiminen otti oman aikansa. Tietoturvakartoituksen tekoon tarvittavan tiedon valtava määrä hämmästytti ja pelotti aluksi, mutta oppimiskokemukset auttoivat uskomaan siihen että teoriatausta saadaan kirjattua ylös. Allekirjoittaneen loukkaantumisen vuoksi projekti piti keskeyttää. Projektia jatkettiin heti kun se oli mahdollista, laatimalla aikataulut uusiksi.

Samaan aikaan teoriataustan kirjoittamisen kanssa aloitettiin kohdeyrityksen tietoturvan kartoitus. Yrityksen toimipisteessä käytiin haastattelemassa yrityksen henkilöstöä yleisistä toimintatavoista. Yrityksen johdolle tehtiin kyselytutkimus, jolla kartoitettiin tietoturvan nykytila. Nykytilan kartoituksen jälkeen annettiin suosituksia tilanteen parantamiseksi. Yrityksen ydinprosessit ja niihin kohdistuvat uhkat kartoitettiin haastattelun avulla. Haastattelujen ja suositusten valmistelu ja tekeminen olivat varsin mukavaa työtä. Työn viimeistelyyn ja puhtaaksikirjoittamiseen olen joutunut käyttämän paljon aikaa.

Kustannukset

Projektille varattiin 50€ työn kansittamisen kuluihin.

Resurssien käyttö

Projektisuunnitelman mukaan projektin työmäärä on 407 tuntia. Laskujeni mukaan tähän mennessä tehtyjä työtunteja on yhteensä 463. Työn tuntiseuranta löytyy liitteestä1.

Ehdotukset jatkotoimenpiteiksi

Kohdeyritys voi jatkaa tietoturvakartoitusta Kairabin mallin mukaan.

Liite 1. Projektin tehtävät, työmäärät ja ajoitus toteutuneet tunnit

		lopputulos	aloituskriteeri		Vko	3	4	5	6	7	8	9	10	11	12	13	34	35	35	37	38
1	**Projektin käynnistäminen**	**Hyväksytty projektisuunnitelma**		**tuntia**	**12**																
1.1	Projektisuunnitelman viimeistely					8															
1.2	Aloituskokouksen valmistelu					1															
1.3	Aloituskokous						1														
1.4	Pöytäkirjan laatiminen						1														
1.5	Kick-Off ja sen valmistelu					1															
2	**Projektin seuranta ja ohjaus**	**Hallittu projekti**	**Projekti on käynnistetty**	**tuntia**	**12**																
2.2	Edistymisraportin laatiminen												1								1
2.3	Ohjauskokouksen valmistelu												1								1
2.4	Ohjauskokous												1								1
2.5	Pöytäkirjan laatiminen													1							1
3	**Teoreettinen tutkimus**	**Teoria valmiina**	**Projekti on käynnistetty**	**tuntia**	**235**																
3.1	Teorian tutkimus							30	30	30	30	30					15	15	15		
3.2	Dokumenttien tekoa																			15	15
4	**Empiirinen tutkimus**	**Valmis työ**	**Teoreettinen tutkimus on valmis**	**tuntia**																	
4.1	Kyselytutkimus	Valmis tutkimus																			
4.2	Toimitilojen ja työmenetelmien tarkastus	Tarkastusraportti																			
4.3	Riskianalyysi	Riskianalyysi																			
4.4	Ohjeistus	Ohjeet																			
4.5	Työn viimeistely	Valmis työ																			
				yhteensä	**259**																

Liite 1. Projektin tehtävät, työmäärät ja ajoitus toteutuneet tunnit

		lopputulos	aloituskriteeri		Vko	39	40	41	42	43	44	45	46	47	48	49	50
1	**Projektin käynnistäminen**	**Hyväksytty projektisuunnitelma**		**tuntia**													
1.1	Projektisuunnitelman viimeistely																
1.2	Aloituskokouksen valmistelu																
1.3	Aloituskokous																
1.4	Pöytäkirjan laatiminen																
1.5	Kick-Off ja sen valmistelu																
2	**Projektin seuranta ja ohjaus**	**Hallittu projekti**	**Projekti on käynnistetty**	**tuntia**	**4**												
2.2	Edistymisraportin laatiminen					1											
2.3	Ohjauskokouksen valmistelu					1											
2.4	Ohjauskokous					1											
2.5	Pöytäkirjan laatiminen					1											
3	**Teoreettinen tutkimus**	**Teoria valmiina**	**Projekti on käynnistetty**	**tuntia**	**40**												
3.1	Teorian tutkimus						**20**	**20**									
3.2	Dokumenttien tekoa																
4	**Empiirinen tutkimus**	**Valmis työ**	**Teoreettinen tutkimus on valmis**	**tuntia**	**160**												
4.1	Kyselytutkimus	Valmis tutkimus					20	20									
4.2	Toimitilojen ja työmenetelmien tarkastus	Tarkastusraportti							20	20							
4.3	Riskianalyysi	Riskianalyysi									20	20					
4.4	Ohjeistus	Ohjeet											10				
4.5	Työn viimeistely	Valmis työ											10	20			
				yhteensä	**463**												