TIETOTURVA- JA UHKAKARTOITUS
Jykes Kiinteistöt Oy:lle

Kirsi Kautola

Opinnäytetyö
Maaliskuu 2013

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Tekijä(t)
KAUTOLA, Kirsi

Julkaisun laji
Opinnäytetyö

Päivämäärä
07.02.2013

Sivumäärä
63

Julkaisun kieli
Suomi

Luottamuksellisuus
( ) saakka

Verkkojulkaisulupa myönnetty
(X)

Työn nimi
TIETOTURVA- JA UHKAKARTOITUS

Koulutusohjelma
Tietotekniikka

Työn ohjaaja(t)
KOTIKOSKI, Sampo, HÄKKINEN, Antti

Toimeksiantaja(t)
Jykes Kiinteistöt Oy

Tiivistelmä

Opinnäytetyössä luotiin tietoturvapolitiikka sekä tietoturva- ja uhkakartoitus sekä riskianalyysi toimeksiantajan tietojärjestelmille. Lisäksi opinnäytetyössä tehtiin Web-sivustona toteutettu yhtenäinen tallennuspaikka IT-dokumentaatiolle.

Työssä kerrotaan yrityksen tietojärjestelmistä ja palveluista sekä niiden nykytilasta, niiltä osin, joita tietoturva- ja uhkakartoitus koskettaa tässä vaiheessa. Tietoturva- ja uhkakartoitus tehtiin ohjelmisto-, laitteisto- ja tietoliikenneturvallisuuden osa-alueilta.

Tietoturva- ja uhkakartoituksen tekemiseen käytettiin apuna Vahti-dokumentteja sekä SFS-ISO/IEC 17799 ja SFS-ISO/IEC 27005 standardeja. Standardeista ja ohjeistuksista poimittiin parhaiten yrityksen tarpeisiin sopivat ohjeistukset.

Tietoturva- ja uhkakartoitus soveltuu toimeksiantajalle pohjaksi laajemman tietoturva- ja uhkakartoituksen sekä tietoturvasuunnitelman tekemiseen, joka käsittää kaikki kahdeksan tietoturvan osa-aluetta.

Web-sivustona toteutettu dokumentaatiojärjestelmä koodattiin html-kielellä ja sijoitettiin toimeksiantajan palvelimelle. Toimeksiantaja voi hyödyntää järjestelmää yhtenäisenä IT-dokumentaation tallennuspaikkana ja kerätä järjestelmään haluamansa dokumentaation.

Avainsanat (asiasanat)
Tietoturvallisuus, Uhkakartoitus, Riskianalyysi

Muut tiedot

Author(s)
KAUTOLA, Kirsi

Type of publication
Bachelor´s Thesis

Date
07.02.2013

Pages
63

Language
Finnish

Confidential

( ) Until

Permission for web publication
(x)

Title
INFORMATION SECURITY AND THREATH SURVEY

Degree Programme
Data Network Technology

Tutor(s)
KOTIKOSKI, Sampo, HÄKKINEN, Antti

Assigned by
Jykes Kiinteistöt Oy

Abstract

The purpose of this thesis was to create an information security and threat survey and information security policy for the client. During the creation of an information security and threat survey the potential risks for the client's information systems were identified and analyzed. In addition, a database for documents on information technology was created.

The thesis describes the current state of company's data systems and services. The systems are described from the point of view of software security, hardware security and data network security.

The guidelines and help for creation of information security and threat survey were collected from VAHTI documents and from the SFS standards ISO/IEC 17799 and ISO/IEC 27005. The suitable guidelines for the client were picked from the standards and document.

This information security and threat survey is suitable as the company's first plan and can be used as a base for the following more extensive plan which contains all eight sectors of information security.

The documentation system was placed in the client's server. The user interface for the system was coded with HTML-language. The client can utilize the system and collect and save the documents they want in to the system.

Keywords
Information security, Threat survey, Risk analysis

Miscellaneous

SISÄLTÖ

KUVIO

TAULUKKO

LYHENTEET

AD	Active Directory
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAPS	Ethernet Automatic Protection Switching
G.SHDSL	Single-pair high-speed digital subscriber line
OU	Organization Unit
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WSUS	Windows server update services
WLAN	Wireless Local Area Network

1 TEHTÄVÄ JA TAUSTAT

Jykes Kiinteistöt Oy:n verkko ja IT ympäristö ovat kasvaneet muutaman viime vuoden aikana merkittävästi. Omia tietoliikenneyhteyksiä ylläpidetään kahdessa eri toimipisteessä ja yrityksen asiakkaille tarjotaan, toimitilojen ja perinteisten toimitilapalveluiden lisäksi, ylläpidettyjä tietoliikenneyhteyksiä neljässä eri kiinteistössä.

Toimintaympäristön kasvu ja muutos sekä tietojärjestelmien kasvanut merkitys liiketoiminnalle loi tarpeen IT -järjestelmien keskitetystä dokumentaatiosta sekä tietoturva- ja uhkakartoituksesta, sekä tietoturvan säännöllisestä katselmoinnista ympäristön jatkuvasti kehittyessä ja muuttuessa.

Näistä tarpeista Jykes Kiinteistöt Oy käynnisti projektin tietoturva- ja uhkakartoituksen laatimiseksi ja dokumentaatiojärjestelmän suunnittelemiseksi.

Työssä kuvataan Jykes Kiinteistöt Oy:n IT -toimintaympäristö ja liiketoiminnan sille asettamat vaatimukset. Opinnäytetyössä luotiin yritykselle tietoturvapolitiikka, jonka pohjalta tehtiin tietoturva- ja uhkakartoitus.

Aiheen laajuuden vuoksi tässä työssä käsitellään tietoturvan osa-alueilta tarkemmin laitteisto-, ohjelmisto- ja tietoliikenneturvallisuutta. Muiden osa-alueiden osalta tietoturva- ja uhkakartoitusta täydennetään yrityksessä myöhemmin.

Dokumentaatiojärjestelmä suunniteltiin ja lähdettiin toteuttamaan omana osionaan, vaikkakin asiamukainen dokumentaatio on tärkeä osa tietoturvallisuutta.

2 PROJEKTIORGANISAATIO

Tietojärjestelmien toiminnasta yrityksessä vastaavat kaksi henkilöä, talouspäällikkö ja IT-koordinaattori, yhdessä alihankintana ostettavien asiantuntijapalveluiden kanssa. Käytännön ylläpito on IT-koordinaattorin vastuulla. Kiin-

teistöjen lukituksesta ja muusta fyysisestä turvallisuudesta vastaa kiinteistöpäällikkö.

Tietoturva- ja uhkakartoituksen toteuttavat pääosin talouspäällikkö ja IT-koordinaattori. Tietoturvapolitiikan hyväksyy toimitusjohtaja.

3 YRITYS – JYKES KIINTEISTÖT OY

3.1 Yleistä

Jykes Kiinteistöt Oy on perustettu 1983, ja omistajina ovat Jyväskylän kaupunki ja Laukaan sekä Muuramen kunnat. Jykes Kiinteistöt Oy on keskittynyt toimitilojen ja työpaikka-alueiden kehittämiseen ja vuokraukseen Jyväskylän seudulla. Omistuksessa yhtiöllä on noin 90 000 m^2 tuotanto-, toimisto- ja varastotiloja. Lisäksi on noin 127 000 m^2 ulkopuolisia kiinteistöjä hallinnoitavana. Vuokralaisina Jykes Kiinteistöjen tiloissa toimii noin100 yritystä. (Jykes Kiinteistöt Oy 2012. Yleisesittely.)

Henkilöstö

Jykes Kiinteistöillä työskenteli vuoden 2012 lopussa 12 henkilöä. Henkilöstö on kaksinkertaistunut viimeisen 10 vuoden aikana. Yritys on asiantuntijaorganisaatio, ja yrityksen tärkeimpiä pääomia ovat henkilöstö ja yrityksen hallinnoima tieto.

Toimintaympäristö

Asiantuntijaorganisaationa Jykes Kiinteistöt Oy:lle on suuri merkitys, että tiedon saatavuus, luotettavuus ja eheys ovat taattuja. Avainhenkilöillä on oltava pääsy tietoon luotettavasti ja turvallisesti myös toimiston ulkopuolelta sekä joustavasti eri toimipisteistä. Liikkuvan työn ja langattomien verkkojen merkitys on kasvanut huomattavasti viime vuosien aikana.

Henkilömäärän kasvu sekä toimintaympäristön muutokset, kuten sivutoimipisteiden perustaminen ja asiakkaille tarjottavat tietoliikennepalvelut, ovat tuo-

neet muutoksia myös yrityksen IT-ympäristöön. Liikkuvan työn merkitys on kasvanut, ja etäyhteydet yrityksen verkkoon ovat tulleet välttämättömiksi. Myös langattomien verkkojen merkitys on kasvanut.

Jyväskylän kaupungin tytäryhtiönä Jykes Kiinteistöille tulee kaupungin taholta ohjausta joihinkin menettelytapoihin, mm. julkinen hankintalaki koskettaa myös suurissa IT-laite- ja palveluhankinnoissa. Taloushallinnon on myös ollut mahdollista ottaa käyttöön kaupungin ylläpitämiä tietojärjestelmiä, esim. sähköinen laskujen kierto. Tämä luo yhteistyötä myös Jyväskylän kaupungin tietohallinnon ja Jykes Kiinteistöjen välille. Kaupunkikonsernin tietoturvapolitiikka koskettaa myös tytäryhtiöitä. Jykes Kiinteistöt Oy:lle luotiin kuitenkin tietoturva- ja uhkakartoitusta tehdessä myös oma tietoturvapolitiikka, joka soveltuu paremmin omaan toimintaympäristöön ja painottaa nimenomaan Jykes Kiinteistöille tärkeitä tietoturvallisuuden osa-alueita.

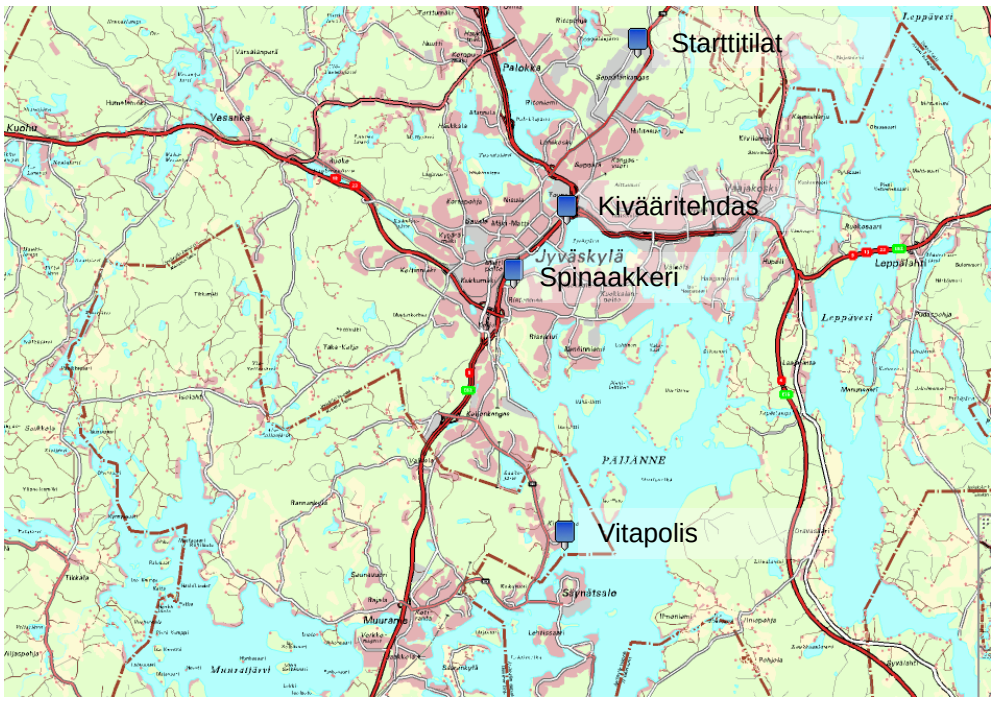
Toimitilat

Jykes Kiinteistöillä on henkilöstöä kahdessa eri toimipisteessä. Pääkonttori sijaitsee Kivääritehtaan yrityspuistossa Jyväskylän keskustan tuntumassa Tourulassa, osoitteessa Kivääritehtaankatu 8, 40100 Jyväskylä. Noin 300 m^2:n toimistossa työskentelee 11 henkilöä.

Vitapoliksen yrityspuistossa, osoitteessa Parantolantie 24, 40930 Kinkomaa, sijaitsee Jykes Kiinteistöjen etätoimipiste. Vitapoliksen toimistossa työskentelee yksi henkilö.

Sivutoimipiste Vitapolis on yhdistetty kiinteällä Site-to-Site VPN-yhteydellä pääkonttoriin.

Lisäksi Jykes kiinteistöt Oy tarjoaa vuokralaisilleen mahdollisuuden ottaa kiinteistöyhtiön ylläpitämän tietoliikenneyhteyden käyttöönsä kuukausimaksua vastaan. Palvelu on tarjolla Kivääritehtaan ja Vitapoliksen Yrityspuistojen lisäksi Mattilanniemen kaupunginosassa sijaitsevassa Spinaakkeri-nimisessä toimistorakennuksessa sekä Starttitilat nimisessä teollisuushallissa Seppälänkankaan kaupunginosassa. Tilojen maantieteellinen sijainti näkyy oheisessa kuviossa 1.



Kuvio 1.Toimipisteiden sijainti. (Jyväskylän kaupungin karttapalvelu 2012)

4 IT-YMPÄRISTÖN NYKYTILA

4.1 Yleistä

Jykes Kiinteistöillä, myöhemmin Yritys Oy, on omistuksessaan noin kolmekymmentä kiinteistöä Jyväskylän, Muuramen ja Laukaan alueella. Verkkopalveluita tarjotaan neljässä kiinteistössä, ja omaa henkilökuntaa Yritys Oy:llä on kahdessa eri kiinteistössä. Tässä työssä kuvataan ainoastaan näiden neljän kiinteistön tietojärjestelmien ja tietoverkkojen nykytilaa.

4.2 Kivääritehtaan yrityspuisto

4.2.1 Yleistä

Kivääritehtaan Yrityspuisto koostuu pääosin kahdesta eri rakennuksesta, osoitteessa Asekatu 3 sijaitsevasta henkilöstöruokalan ja toimitiloja sisältävästä rakennuksesta sekä toimistotiloja sisältävästä Kivääritehtaan päärakennuksesta. Yritys Oy:n pääkonttori sijaitsee Kivääritehtaan päärakennuksessa.

Asekatu 3:n kiinteistö on Yritys Oy:n omistuksessa. Kiinteistössä on noin 2 400 m^2, toimisto ja varastotilaa.

Sivutoimipiste Vitapolis on yhdistetty kiinteällä Site-to-Site VPN-yhteydellä pääkonttoriin, Kivääritehtaan yrityspuistoon. Mattilanniemessä sijaitseva Spinaakkeri ja Starttitilat Seppälänkankaalla ovat itsenäisiä ympäristöjä, eikä näistä toimipisteistä ole kiinteää yhteyttä Yritys Oy:n verkkoon.

4.2.2 Verkon looginen topologia

Pääkonttorin verkko ulottuu kahden eri rakennuksen alueelle. Operaattorin yhteydet tulevat Yritys Oy:n toimiston viereiseen rakennukseen. Tietoliikenneyhteys tuodaan Yritys Oy:n toimistotiloihin viereiseen rakennukseen yksimuotokuidulla.

4.2.3 Tarjottavat palvelut

Vuokranantajana Yritys Oy tarjoaa Asekatu 3:een sijoittuville yrityksille mahdollisuuden vuokrata toimitilan lisäksi kiinteistöyhtiön tarjoaman Internetyhteyden. Yhteys on toteutettu G.SHDSL 10/10 Mt Yritysliittymänä. Liittymän kapasiteetti jaetaan asiakkaiden kesken. Operaattorina toimii Elisa Oyj. Palveluun sisältyy vuokralaiselle oma VLAN-aliverkko sekä tarvittavat kiinteät ja julkiset IP-osoitteet asiakkaan tarpeiden mukaan. Lisäksi asiakas voi ottaa käyttöönsä halutessaan Wlan-yhteyden.

Kaikille Asekadun ja Kivääritehtaan vuokralaisille ja asiakkaille on lisäksi tarjolla lounasravintolassa ja sen neuvottelutiloissa sekä kaapeloitu että langaton Internet-yhteys. Lisäksi neuvottelutiloissa ovat dataprojektorit käytettävissä.

Asiakkaina on pääasiassa pieniä muutaman henkilön yrityksiä. Asiakkaita on kaikkiaan kymmenkunta.

4.2.4 Verkon ylläpito ja valvonta

Verkonvalvonta ja ylläpito on ulkoistettu alihankkijalle. Valvottavista kohteista ja vasteajoista on tehty SLA-sopimus alihankkijan kanssa. Alihankkijalla on

oma Nagiokseen perustuva verkonvalvontajärjestelmä, jota he ovat kehittäneet ja parannelleet vuosien ajan. Tiedot aktiivilaitteista haetaan SNMP-protokollan avulla.

Verkonvalvonnan hälytykset tulevat IT-koordinaattorille sähköpostiin sekä tekstiviestinä matkapuhelimeen. Viestit menevät myös alihankkijan ylläpitotiimille.

4.3 **Spinaakkeri**

4.3.1 Yleistä

Mattilanniemen Spinaakkeri-niminen kiinteistö sijaitsee osoitteessa Ahlmaninkatu 2 E, 40100 Jyväskylä. Kiinteistössä on noin 2 200 m^2 toimistotilaa, jota vuokrataan yrityksille. Ensisijainen kohderyhmä ovat pienet kasvuyritykset.

4.3.2 Tarjottavat palvelut

Vuokranantajana Yritys Oy tarjoaa Mattilanniemeen sijoittuville yrityksille mahdollisuuden vuokrata toimitilan lisäksi kiinteistöyhtiön tarjoaman Internetyhteyden. Taloon sijoittuva vuokralainen voi halutessaan ottaa Internetyhteyden käyttöönsä kuukausimaksua vastaan tai hankkia oman yhteyden ja huolehtia itse sen aktiivilaitteista ja ylläpidosta. Spinaakkerissa on 2012 vuoden lopussa reilut kymmenen asiakasta, jotka ovat ottaneet käyttöönsä tarjotun tietoliikenneyhteyden.

Yritys Oy:n hallinnoima palvelu sisältää symmetrisen G.SHDSL 10/10 Mt Yritysliittymän. Liittymän kapasiteetti jaetaan useamman asiakkaan kesken. Operaattorina toimii TNNet Oy. Sisäverkko on suojattu keskitetyllä xxxxxx kahdennetulla palomuuripalvelulla. Asiakkaan on halutessaan mahdollista ottaa myös oma palomuuri käyttöön, jolloin asiakkaan IP-osoiteavaruudesta tuleva liikenne ohjataan keskitetyn palomuuriratkaisun ohi.

Asiakkaille IP-osoitteistus tehdään yrityksen tarpeiden mukaan. Lähtökohtana asiakkaalle tehdään aliverkko privaateilla IP-osoitteilla. Tarpeen mukaan mää-

ritetään kiinteät IP-osoitteet ja myönnetään julkiset IP-osoitteet niitä vaativille palveluille.

Kaikille talon vuokralaisille on tarjolla neuvottelutilat ja niissä olevat palvelut, kuten dataprojektori ja asiakaskäyttöön tarkoitettu suojattu Wlan-yhteys.

4.3.3 Sisäverkon laitteet ja verkon looginen topologia

Kaikki sisäverkon aktiivilaitteet ovat operaattorin toimittamia ja ylläpitämiä. Yritys Oy vuokraa laitteet käyttöönsä kiinteällä kuukausiveloituksella. Operaattori huolehtii laitteiden ylläpidosta ja konfiguraatiosta. Operaattorilla on varalla mm. kytkin toimitettavaksi rikkoutuneen tilalle.

Kaikille aktiivilaitteille häiriötön virransyöttö pienien sähkökatkojen varalta on varmistettu UPS – laitteilla.

Sisäverkko on toteutettu EAPS-renkaana, joten yhden kaapelin tai kytkimen vikaantuminen ei katkaise verkkoyhteyttä. EAPS-rengasta käytetään luomaan vikasietoinen topologia konfiguroimalla ensisijainen ja toissijainen polku jokaiselle VLAN verkolle. (EAPS-rengas. 2013)

Rengas reitittää liikenteen uudelleen 50 ms:n ajassa. Katkosta ei käytännössä huomaa. Ratkaisulla on saatu tärkeää redundanttisuutta tietoliikenneyhteydelle.

Vuokraustoiminnan alkaessa kesällä 2012 kiinteistössä Internet-yhteyden nopeus on 10/10 Mt.

4.3.4 Verkonvalvonta

Operaattorilta ostettavaan palveluun kuuluu verkonvalvonta, jossa mm. seurataan verkon ja aktiivilaitteiden tilaa ja kapasiteetin riittävyyttä. Tarvittaessa kapasiteettia voidaan lisätä nostamalla yhteyden nopeutta kytkemällä lisää kuparipareja tai vaihtamalla valokuituyhteyteen.

Operaattorin kanssa on tehty SLA eli palvelutasosopimus, jossa määritellään vasteajat vikatilanteissa sekä palveluajat. Palveluajaksi on valittu arkipäivisin 8-17 ja vasteajaksi 2 tuntia.

Verkonvalvonnan hälytykset tulevat operaattorin ylläpitotiimin lisäksi IT- koordinaattorin sähköpostiin.

4.4 Starttitilat

4.4.1 Yleistä

Starttitilat-niminen kiinteistö sijaitsee osoitteessa Palokärjentie 7, 40320 Jyväskylä. Toimitila on rakennettu teolliseen tuotantoon. Tiloissa toimi kesällä 2012 kaksi eri vuokralaista, jotka ovat ottaneet käyttöönsä Yritys Oy:n tarjoaman Internet-yhteyden.

4.4.2 Tarjottavat palvelut

Vuokralaisten toiminnan luonteesta johtuen Starttitiloissa ei Internet-yhteyden tarvitse olla nopein mahdollinen, vaan 2/1 Mt:n Yritysinternet-liittymä riittää tällä hetkellä. Operaattorina toimii Elisa Oyj. Yhteys on toteutettu kuparilla.

Tiloissa ei ole neuvottelutiloja eikä tarvetta yrityksen asiakkaille tarjottavalle Wlan-verkolle, mutta yritysten omaan käyttöön Wlan-verkot on toteutettu. Kummallekin yritykselle on toteutettu oma Vlan-aliverkko privaateilla IP-osoitteilla.

Yrityksillä olisi myös Spinaakkerin tapaan mahdollisuus saada tarvittaessa julkinen tai kiinteitä IP-osoitteita, mutta tällä hetkellä niihin ei ole ollut vuokralaisilla tarvetta.

4.4.3 Sisäverkon laitteet ja verkonvalvonta

Operaattorina toimii Elisa Oyj. Operaattori huolehtii reitittimen ylläpidosta. Kytkimen, palomuurin ja Wlan-tukiaseman ylläpito ja valvonta on ulkoistettu alihankkijalle. Aktiivilaitteiden virransyöttö on turvattu UPS-laitteella.

Verkonvalvonnasta ja aktiivilaitteiden ylläpidosta huolehtii sama alihankkija kuin Asekatu 3:ssa. Verkonvalvontaan käytetään siis samaa Nagiokseen pohjautuvaa valvontaohjelmistoa.

Verkonvalvonnan hälytykset tulevat alihankkijan ylläpitotiimin lisäksi IT-koordinaattorin sähköpostiin ja tekstiviestinä matkapuhelimeen.

4.5 Vitapolis – yrityspuisto

4.5.1 Yleistä

Vitapoliksen Yrityspuisto sijaitsee Muuramessa osoitteessa Parantolantie 24, 40930 Kinkomaa. Kyseessä on entinen Kinkomaan sairaala. Päärakennuksessa toimii Yritys Oy:n sivutoimipiste, jossa työskentelee yksi henkilö.

4.5.2 Tarjottavat palvelut

Vuoden 2012 lopussa kiinteistössä ei ole vuokralaisille tarjottuja asiakasverkkoja. Kiinteistönhuollon sekä vartijan käyttöön on konfiguroitu omat Vlan-aliverkkonsa, ja kahdessa erillisessä neuvottelutilassa on tarjolla asiakkaiden käyttöön suojattu Wlan-yhteys. Yritys Oy:n sivutoimipisteessä työskentelevällä henkilöllä on myös oma Vlan-aliverkkonsa, josta on kiinteä Site-to-Site VPN-yhteys Kivääritehtaan pääkonttoriin.

Internet-yhteys on toteutettu 10/10 Mt:n valokuituyhteydellä. Operaattorina toimii Elisa Oyj.

4.5.3 Sisäverkon laitteet ja verkon looginen topologia

Vitapoliksen Yrityspuisto käsittää noin 35 hehtaaria, ja alueella on useita rakennuksia. Pelkästään päärakennuksessa on viisi kerrosta ja bruttoala on noin 16 000 m^2. Rakennus on vuodelta 1930 ja museoviraston suojelukohde. Alueen koko ja vanha rakennus aiheuttavat omat haasteensa kaapeloinnille ja sisäverkon suunnittelulle. Sisäverkosta ei mm. ole olemassa ajantasaisia kaapelointikuvia. Osa rakennuksen nousukaapeloinnista on toteutettu valokuidulla ja osa taas kuparikaapeleilla.

Verkkoyhteyksien toteuttamien haluttuihin pisteisiin vaatii tukun kuitumuuntimia ja aktiivilaitteita.

4.5.4 Verkonvalvonta

Kuten Asekatu 3:ssa ja Starttitiloissa on Vitapoliksen verkonvalvonta ja ylläpito ulkoistettu samalle alihankkijalle, ja käytössä on edelleen Nagiokseen perustuva verkonvalvontaohjelmisto. Myös tämän kohteen verkonvalvonnan hälytykset tulevat alihankkijan lisäksi IT-koordinaattorin sähköpostiin ja tekstiviestinä matkapuhelimeen.

Oman haasteensa verkon valvontaan tuovat nuo kuitumuuntimet, joita ei saada verkonvalvonnan piiriin. Reitittimen ylläpidosta huolehtii operaattori. Kytkimet, palomuuri ja langattomat tukiasemat ovat verkonvalvonnassa alihankkijalla.

4.6 Internet-yhteydet

Toimintaympäristön muuttuessa ja yrityksen kasvaessa toimipisteitä on tullut lisää. Verkkoyhteyksiä on tilattu eri operaattoreilta saatavuuden ja kilpailutuksen perusteella.

Taulukkoon 1 on koottu Yritys Oy:llä hallinnoitavana olevat Internet-yhteydet.

Taulukko 1. Internet-yhteydet

Kiinteistö	Liittymätyyppi	Nopeus	Operaattori	Määrä
Kivääritehdas	Kupari	10/10 Mt	Elisa Oyj	1
Vitapolis	Kuitu	10/10 Mt	Elisa Oyj	1
Starttitilat	Kupari	2/1 Mt	Elisa Oyj	1
Spinaakkeri	Kupari	10/10 Mt	TNNet	1
Mobiililaajakaistat	3G	vaihtelee	Elisa/Sonera	10
Laajakaistat	ADSL/Kupari	8 -24/1 Mt	Elisa/Sonera	4

Etätyöskentelyn mahdollistamiseksi yritykselle on myös hankittu avainhenkilöiden käyttöön mobiililaajakaistoja sekä ADSL-liittymiä työntekijöiden kotiin.

4.7 Yritys Oy:n tietojärjestelmät ja tietoliikenneyhteydet

4.7.1 Yleistä

Yritys Oy:llä on yksi domain eli toimialue, johon käyttäjät kirjautuvat.

Toimialue on joukko Windows-tietokoneita, joita voidaan hallita keskitetysti yhdellä tai useammalla Windows palvelimella, jota kutsutaan myös Domain Controlleriksi (DC) eli toimialueen ohjainpalvelimeksi. Ohjainpalvelin on palvelin jossa on Windows Server käyttöjärjestelmä ja Active Directory toimialuepalvelut asennettuna. (Windows Server Domain. 2013.)

DC (Domain controller) sijaitsee pääkonttorilla ja se on kahdennettu. Vanhasta tiedostopalvelimesta on tehty back up -controller, joka tuo redundanttisuutta ympäristöön.

Domain Controller (DC 1) toimii myös tiedostopalvelimena sekä taloushallinnon sovelluspalvelimena. Kaikki käyttäjät, myös etätoimipisteistä, kirjautuvat siis Kivääritehtaan toimipisteessä sijaitsevalle Domain Controllerille.

4.7.2 Toimialue ja palvelimet

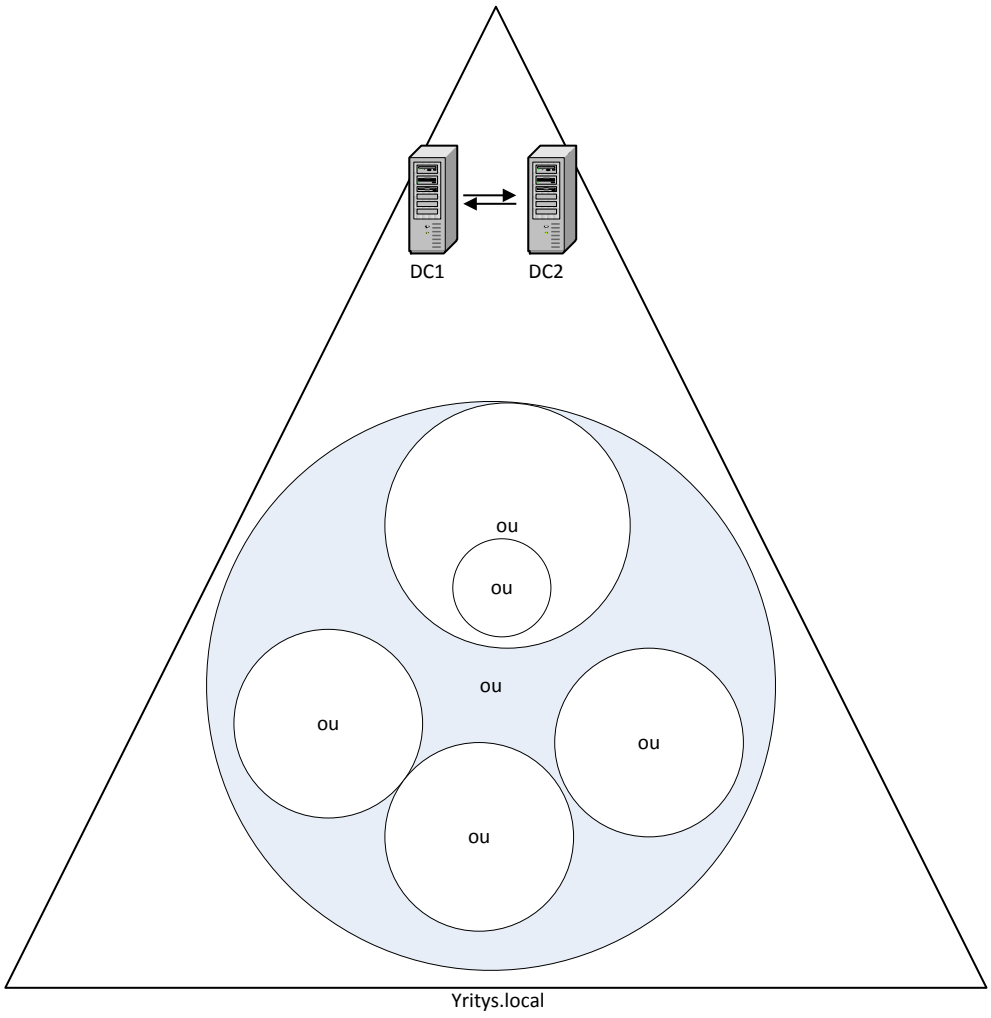
Toimialueen palvelimessa (DC1) on myös Active Directory (AD), joka on Microsoftin Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu. Se sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. AD:n kautta on mahdollista jakaa käyttäjille verkon resursseja ja sovelluksia keskitetysti. AD:n avulla voidaan myös paikallistaa, hallita ja suojata käytössä olevia verkon resursseja. (Active Directory.2013.)

Tulostuspalveluita ajetaan kummallakin palvelimella.

Yritys Oy:n toimialue sisältää erilaisia organisaatioyksiköitä eli OU:ta. Seuraavassa on listattu toimialueen organisaatioyksiköt:

- ou
    - ou
        - ou
    - ou
    - ou
    - ou

Oheisessa Kuviossa 2. on kuvattuna toimialueen looginen topologia. Kuvassa on toimialueen ohjainpalvelimet ja organisaatioyksiköt.



Kuvio 2. Yritys Oy: toimialueen looginen topologia

DC1-palvelimessa pyörivät myös DHCP- ja DNS- palvelut. Nauhavarmennusta varten samassa palvelimessa on nauha-asema, johon molempien palvelimien data ajetaan joka yö.

Nauhavarmennuksessa käytetään joka arkipäivälle maanantaista torstaille omaa nauhaa, perjantaipäiville kierrätetään kuutta eri ”perjantainauhaa”. Lisäksi aina vuoden lopussa data ajetaan vuosinauhalle, joka säilytetään seuraavan vuoden loppuun. Varmuuskopionauhat säilytetään paloturvallisessa kaapissa.

4.7.3 Etäyhteydet

Turvalliset etäyhteydet on ostettu alihankkijalta kuukausiveloitteisena palveluna. Remote VPN -yhteys otetaan käyttäjän työasemalta web-selaimella autentikoitumalla palveluun.

Autentikointipalvelin sijaitsee palveluntarjoajan konesalissa. Käyttäjät autentikoituvat palvelimelle käyttäjätunnuksellaan sekä 6-numeroisella tokenista saatavalla tunnuksella. Autentikointipalvelimelta on Site-to-Site VPN yhteys Yritys Oy:n verkkoon. 6-numeroisen tunnuksen jälkeen käyttäjä autentikoituu vielä Yritys Oy:n omalle AD-palvelimelle omalla salasanallaan.

5 TIETOTURVALLISUUS

5.1 Yleistä

Yrityksien liiketoiminta on yhä riippuvaisempi tietojärjestelmistä ja toimivista tietoliikenneyhteyksistä. Tämä korostaa tietoturvan merkitystä yrityksille. Asiantuntija organisaationa Yritys Oy:lle on suuri merkitys sillä, että tietojärjestelmät ja tieto ovat yrityksen ja sen työntekijöiden käytettävissä paikasta ja ajasta riippumatta.

Tietoturva on kilpailuetu, mikäli se on hoidettu asianmukaisesti liiketoiminnan asettamien vaatimusten mukaisesti. Kun tietoturvakulttuuria toteutetaan organisaatiossa sen liiketoimintaympäristössä, kilpailuetu realisoituu liiketoiminnan

jatkuvuuden edellytysten paranemisena. (Laaksonen, Nevasalo & Tomula 2006, 18.)

Tietoturvallisuus koostuu teknisistä ja hallinnollisista toimista, jotka suunnitellaan huolellisesti. Tehtyjen toimien vaikutuksia seurataan ja toimintaa kehitetään. Hyvän tietoturvallisuuden tason saavuttaminen ja säilyttäminen vaatii yritykseltä määrätietoista ja – muotoista toimintaa ja johtamista. (Laaksonen ym. 2006, 17.)

Yritys Oy toteuttaa tietoturvallisuutta sekä hallinnollisilla että teknisillä ratkaisuilla. Hallinnollisiin ratkaisuihin kuuluvat tietoturvapolitiikka sekä tietoturva- ja uhkakartoitus teknisiin ratkaisuihin tietojärjestelmien ja tiedon suojaamiseen hankitut ja toteutettavat ohjelmisto- ja laiteratkaisut. Yksi tärkeä tietoturvallisuuden toteuttamiskeino on myös henkilöstön kouluttaminen ja tietoturvasta tiedottaminen.

5.2 Tietoturvauhat

5.2.1 Yleistä

Kymmenen yleisintä tietoturvaongelmaa suomalaisissa yrityksissä vuonna 2011 olivat:

1. Puutteelliset salasanakäytännöt
2. Web-haavoittuvuudet
3. Käyttövaltuushallinnan ongelmat
4. Dokumentaation haasteet
5. Varmuuskopioinnin käytännöt
6. Tietoturvapäivitykset
7. Henkilökunnan tietoturvakoulutuksen puute
8. Lainsäädännön vaatimusten täyttymisen puutteet

9. Riskienhallinnan puutteet
10. Tietoturvavaatimukset järjestelmähankinnan yhteydessä. (Tietoturvaongelmat. 2012.)

Havainnot perustuvat KPMG:n vuonna 2011 tekemiin hallinnollisiin ja teknisiin tietoturva-auditointeihin. Lähdeaineistona KPMG:n raportissa on käytetty KPMG:n tietoturvatarkastusten loppuraportteja, joista valittiin 83 lähdemateriaaliksi. (Tietoturvaongelmat. 2012.)

5.2.2 Puutteelliset salasanakäytännöt

KPMG:n raportin perusteella heikot salasanat ja puutteelliset salasanakäytännöt ovat yleisin tietoturvapuute. Käyttäjät tietävät pääsääntöisesti millainen on hyvä salasana, mutta tapana on kuitenkin valita helpoin järjestelmän sallima salasana, joka on esimerkiksi tuttu toisesta järjestelmästä. Huonoja salasanoja löytyi myös ylläpitotunnuksista. (Tietoturvaongelmat. 2012.)

Ongelman korjaamiseksi raportissa ohjeistetaan vaatimaan kaikilta riittävän vahvaa salasanaa tai salasanalausetta, joka on vaihdettava 90 päivän välein. Lisäksi järjestelmien ja ohjelmien oletussalasanat tulee myös aina vaihtaa. Samaa salasanaa ei myöskään saa käyttää useassa eri järjestelmässä. Vapaa-ajan palveluihin ei tulisi käyttää työjärjestelmien salasanoja. (Tietoturvaongelmat. 2012.)

5.2.3 Web-haavoittuvuudet

Raportin mukaan vuonna 2011 julkisuudessa oli onnistuneita tietomurtoja enemmän kuin koskaan. Murtojen taustalla oli usein haavoittuvuus Internet-sivuilla. Yleisimmät haavoittuvuudet olivat SQL-injektiot (Search and Query Language) ja XSS (Cross Site Scripting). Kumpaakin haavoittuvuutta yhdistää se, ettei niitä yleensä voida paikata pelkästään tietoturvapäivityksellä. Tehokkain tapa torjua nämä hyökkäykset on tietoturvallisten kehitysmenetelmien käyttö jo sovellusta toteutettaessa. Myös käyttäjien asianmukaisella tietoturvakoulutuksella on suuri merkitys. (Tietoturvaongelmat. 2012.)

Web-haavoittuvuuksien vaikutus yrityksen liiketoimintaan riippuu Web-sovelluksen tarkoituksesta ja siinä säilytetystä tiedosta. Mikäli sivusto saa vain huonoa julkisuutta, voi yrityksen markkinaosuus jopa pienentyä. Mikäli palvelun varmuuskopiointi on myös puutteellinen, saatetaan menettää kaikki tietokannassa oleva tieto. Tieto voi myös päätyä vääriin käsiin ja sitä kautta median otsikoihin. (Tietoturvaongelmat. 2012.)

5.2.4 Käyttövaltuushallinnan ongelmat

Käyttövaltuushallinta tarkoittaa menetelmiä, jolla organisaatio hallitsee käyttöoikeuksia eri tietojärjestelmissä. Käyttövaltuudet ovat tietoturvallisesti määriteltyjä silloin, kun käyttäjällä on vain ne oikeudet, joita hän tarvitsee työtehtäviensä suorittamiseen. (Tietoturvaongelmat. 2012.)

Oikeuksien hallintaan liittyy haasteita. Käyttöoikeuksien myöntämisen tulisi olla riittävän nopea ja helppo toimenpide, jotta henkilöillä olisi varmasti riittävät oikeudet omien tehtäviensä hoitamiseen. Toisaalta prosessin tulisi olla riittävän ”jäykkä”, jotta voitaisiin varmistaa käyttäjälle pyydettyjen valtuuksien tarpeellisuus ja tarkistaa mahdolliset ristiriitaisuudet olemassa olevien oikeuksien suhteen. Yleinen käyttövaltuuksiin liittyvä ongelma on myös yhteiskäyttöisten tunnusten käyttö. Mikäli yrityksessä käytetään järjestelmään yhteiskäyttöisiä tunnuksia, on hankala varmistua siitä, kuka tunnuksen tuntevista käyttäjistä on kulloinkin operoinut tunnuksella, ja kuka tietää tunnuksen. Tämä hankaloittaa väärinkäytösten selvittämistä. Kolmas ongelma on ylläpito-oikeuksien myöntäminen liian kevein perustein. Käyttäjä voi halutessaan asentaa uusia ohjelmia koneelleen, ja samalla hän voi vahingossa asentaa myös haitallisen ohjelman tai mahdollisesti kytkeä esim. virustorjunnan pois päältä. (Tietoturvaongelmat. 2012.)

5.2.5 Dokumentaation haasteet

Yrityksen prosessit ja tietojärjestelmien kuvaukset sekä ohjeistukset tulee olla kirjallisesti dokumentoituna. Vaikka järjestelmien kuvaukset ja ohjeistukset olisivatkin dokumentoituna, ne ovat monesti useassa eri muodossa ja vaikeasti henkilöstön löydettävissä. Ajantasaiset ja helposti löydettävät dokumentit

auttavat yritystä toimimaan tehokkaammin. Samoin ajan tasalla oleva dokumentaatio helpottaa esimerkiksi vastuunjakoa. Jokainen tietää mitä häneltä odotetaan ja miten asiat tulisi hoitaa yhdenmukaisesti. (Tietoturvaongelmat. 2012.)

5.2.6 Varmuuskopioiden riittämätön testaus

Raportin mukaan toistuva havainto auditoiduissa yrityksissä oli, että varmistuksien palautusta ei testata. Testaaminen ei ole säännöllistä tai testaussuunnitelmaa ei ole laadittu. Onnistuneen Varmuuskopioinnin toteutuksen kannalta on tärkeää, että varmuuskopioiden palautusta testataan asianmukaisesti:

- Onko riittävä määrä asioita varmuuskopioinnin piirissä
- onko varmuuskopioiden palauttaminen tuotantoon mahdollista ilman versiokonflikteja? (Tietoturvaongelmat. 2012.)

Lisäksi varmuuskopioiden säilyttämiseen erillisessä palotilassa, erillään itse varmistettavasta tiedosta, on myös hyvä kiinnittää huomiota. (Tietoturvaongelmat. 2012.)

Yritys Oy:ssä varmistuksia testataan säännöllisesti. Testauksista ei kuitenkaan ole kirjattu mitään suunnitelmaa. Lisäksi, vaikka varmuuskopiot säilytetään paloturvallisessa kaapissa, sijaitsee kaappi samassa tilassa palvelinten kanssa.

5.2.7 Tietoturvapäivitykset

Tietoturvapäivitysten puute koneilta on hyökkääjälle yksi tapa päästä sisälle järjestelmään. Haavoittuvuudet ovat usein sovellustasolla sillä sovellusten päivittäminen on käyttöjärjestelmän päivittämistä vaikeampaa. Palvelimilla on yllättävän paljon myös turhia sovelluksia, eli turhia riskejä. Ohjelmien päivittäminen helpottuu, kun siitä tehdään selkeä suunnitelma. Suunnitelmasta tulisi ilmetä, kuinka usein päivityksiä tehdään, ja millä tavalla päivitykset tulee tehdä. Myös kriittisten päivitysten asentaminen päivityssyklin ulkopuolella on syytä sisällyttää päivityssuunnitelmaan. (Tietoturvaongelmat. 2012.)

5.2.8 Vähäinen tietoturvakoulutus

KPMG:n raportin mukaan henkilöstön tietoturvatietämys yrityksissä perustuu usein pienimuotoiseen perehdytykseen, jonka jälkeen tietoturvakoulutus on vähäistä. Siitä johtuen henkilöstö ei tunne uusia uhkia. Vaikka tietoturvauhkien merkitys yritysten liiketoiminnalle on kasvanut, ei henkilöstön koulutukseen panosteta kuitenkaan samalla painoarvolla. Tietoturvakoulutusta voisi järjestää vuosittain vaikka Web-kurssina. Ajankohtaisista asioista tiedottaminen voisi tapahtua esimerkiksi uutiskirjeillä. Koulutuksen merkitystä korostaa se, että monissa sähköpostihyökkäyksissä ja sosiaalisissa manipulointikeinoissa heikoin lenkki on käyttäjä, eikä teknisistä suojauskeinoista ole apua. Henkilöstön koulutus onkin kustannustehokas tietoturvan parannuskeino. (Tietoturvaongelmat. 2012.)

Yritys Oy:ssä tietoturvatiedotteita lähetetään tarpeen mukaan sähköpostitse. Uusille työntekijöille jaetaan tietoturvaohjeistus taloon tullessa. Lisäksi tarpeen mukaan järjestetään koulutuksia liittyen uusiin ohjelmiin tai tietojärjestelmiin. Vuosittaisia koulutuksia ei kuitenkaan ole järjestetty liittyen yleisesti tietoturvaan. Opinnäytetyöhön liittyvässä tietoturvapolitiikassa otetaan nyt kuitenkin kantaa henkilöstön kouluttamiseen.

5.2.9 Lakien ja asetusten vaatimuksien laiminlyönti

Tietoturvapolitiikka rakentaa pohjan tietoturvalle ja se tulee heijastaa voimassa olevaa lainsäädäntöä. Lait ja asetukset määrittelevät rajat, joiden sisällä tietoturva toimii. Tietoturvallisuuteen liittyvien lakien ja asetusten heijastuminen yritysten tietoturvaan on kuitenkin raportin mukaan vähäistä. Yritysten henkilöstö ei usein ole tietoinen voimassa olevista laeista ja asetuksista, joten organisaation tietoturvan on vaikea niitä noudattaa. Suurimmat ongelmat liittyvät yleensä henkilötietojen käsittelyyn, suojaamiseen sekä valvonta- ja suojausmekanismeihin. (Tietoturvaongelmat. 2012.)

Lainsäädäntö velvoittaa yrityksiä huolehtimaan tietoturvallisuudesta tiettyjen velvoitteiden täyttämiseksi. Velvoitteet ovat yleisluonteisia ja yrityksille itselleen on jätetty käytännön toteutus ja tietoturvallisuuden tason määrittelemi-

nen. Yritykselle on olennaista kartoittaa ne säädökset, jotka vaikuttavat tietoturvan suunnitteluun. Lainsäädännöllä pyritään luomaan tietoturvallinen yhteiskunta, jossa huomioidaan yksityiseen suoja sekä yritysten kilpailuasema. (Laaksonen ym. 2006,18.)

Yritys Oy:n tietoturvavaatimuksiin lainsäädäntö koskettaa mm. arkistolainsäädännön ja henkilötietolain osalta.

5.2.10 Riskienhallinnan vähäisyys

Tietojärjestelmien riskienhallintaa pätee sama periaate kuin liiketoiminnan riskienhallintaan. Kaikkia riskejä ei ole kustannustehokasta poistaa, mutta hallitsematon riskien realisoituminen voi pahimmillaan ajaa yrityksen konkurssiin. (Tietoturvaongelmat. 2012.)

Raportin mukaan harva yritys toteuttaa säännönmukaista riskienhallintaa tietoturvallisuuteen liittyen. Säännöllinen riskienhallinta on kiinteä osa tietoturvallisuuden hallintaa. Riskien tunnistaminen ja niiden käsittely auttaa yritystä mitoittamaan, suunnittelemaan ja kohdistamaan oikein menetelmät riskienhallintaan. (Tietoturvaongelmat. 2012.)

5.2.11 Tietoturvavaatimusten puute

KPMG:n auditointien perusteella yrityksissä tietoturva ajatellaan usein irrallisena komponenttina, joka lisätään palveluun myöhemmin. Tietoturva tulisi kuitenkin ottaa mukaan projekteihin jo järjestelmänhankinnan alusta lähtien. Usein järjestelmäkehityksessä halutaan järjestelmä toimimaan mahdollisimman nopeasti ja kun järjestelmistä löytyy myöhemmin tietoturvapuutteita, on niiden korjaaminen kallista ja aikaa vievää. (Tietoturvaongelmat. 2012.)

Yritys Oy:n suurimmat tietoturvauhkat kustannusten perusteella

Yritys Oy:n suurimmat uhat tietoturvalle, historian valossa, ovat inhimilliset virheet ja vahingot sekä laiterikot, fyysiset uhat kuten ukkosen aiheuttamat laiterikot ja sähkökatkot sekä ulkopuolelta tulevat uhkat kuten virukset ja haittaohjelmat.

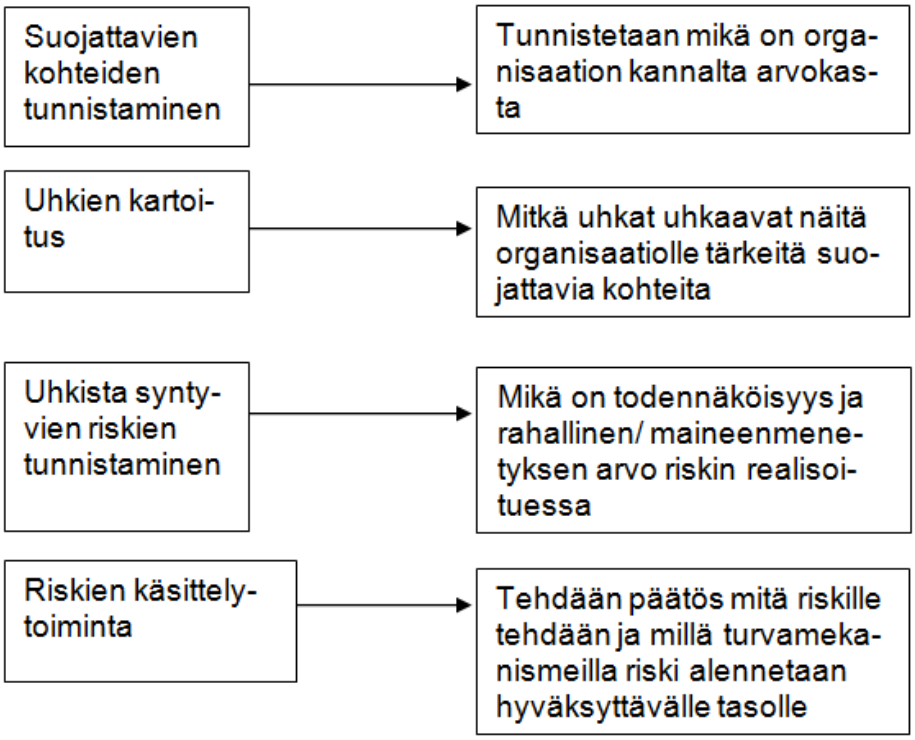
6 TIETOTURVAN SUUNNITTELU

6.1 Suunnittelun vaiheet

Yrityksen tietoturvan suunnitteluprosessissa on kolme päävaihetta:

1. Määritellään tietoturvapolitiikka
2. Määritellään tietoturvastrategia
3. Toteutetaan tietoturvasuunnitelma (Hautamäki 2011a, 4.)

Tietoturvan suunnittelun erityisvaiheet on kuvattu kuviossa 5.



Kuvio 3. Tietoturvan suunnittelun vaiheet

(Hautamäki 2011a, 5.)

Koska Yritys Oy:llä ei ollut käytettävissään aikaisempaa tietoturvapolitiikkaa tai suunnitelmaa, aloitettiin tietoturvan suunnitteluprosessi tietoturvapolitiikan laatimisella. Tietoturvastrategiaa ei tehty tähän opinnäytetyöhön liittyen, vaan siirryttiin tekemään tietoturva- ja uhkakartoitusta. Kartoitusta alettiin tehdä

siirtymällä tietoturvan suunnittelun erityisvaiheisiin, eli pohdittiin mikä on yrityksen liiketoiminnan kannalta arvokasta, eli suoritettiin suojattavien kohteiden tunnistaminen. Kun suojattavat kohteet olivat selvillä, tutkittiin mitkä ovat näitä kohteita uhkaavat uhat, eli tehtiin uhkakartoitus. Uhkakartoituksen jälkeen mietittiin millä todennäköisyydellä mikäkin uhka realisoituisi ja mikä olisi siitä syntyvän vahingon rahallinen arvo, joko suoraan laitehankintoina tai maineen menetyksenä. Eli tehtiin riskianalyysi. Suojattavien kohteiden tunnistamisen, uhkakartoituksen ja riskianalyysin jälkeen voitiin siirtyä riskien käsittelytoimintaan. Eli päätettiin mitä kyseiselle uhalle/riskille tehdään ja millä turvamekanismeilla haluttuun lopputulokseen päästään.

6.2 **Tietoturvapolitiikka**

Tietoturvapolitiikan avulla yrityksen johto määrittää päämäärät, vastuut ja toiminnalliset suuntaviivat yrityksen tietoturvallisuuden hoitamiselle. Jotta saavutettaisiin yrityksessä tietoturvallisuuskulttuuri, on tärkeää, että tietoturvallisuuden merkitys ja sen yleiset periaatteet selvitetään jokaiselle yrityksen työntekijälle. Tietoturvapolitiikka on perusta, jolle eri tietoturvasuunnitelmat ja ohjeet luodaan. (Vahti 2009, 20.)

Tietoturvan määrittelyä ohjaa yrityksen liiketoiminta ja strategia, riskianalyysi, lainsäädäntö ja säädökset. Jos organisaatio noudattaa joitain standardeja, ja erityisesti, jos se on saanut standardeihin nojaavia sertifikaatteja, tulee tietoturvapolitiikan täyttää näiden standardien vaatimukset. (Vahti 2009, 20.)

Tietoturvapolitiikan laadinta on yrityksen ylimmän johdon vastuulla. Se laaditaan kirjalliseen muotoon ja sen on tarkoitus toimia 5-10 vuoden aikavälin ohjeena tietojärjestelmien suunnittelijoille ja liiketoimintaprosessien henkilöille. (Hakala, Vainio & Vuorinen 2006, 7.)

Tietoturvapolitiikalle ei ole olemassa valmista mallia, joka sopisi automaattisesti eri yrityksien liiketoimintamalleihin. Valmiin mallin, joka ei sovellu yrityksen liiketoimintaan, noudattaminen voi vaikuttaa koko tietoturvaohjelman toimivuuteen. Johdon sitoutuminen ei ole siihen ehdotonta, eikä kaikkea sisältöä välttämättä ymmärretä. (Laaksonen ym. 2006, 148.)

Politiikka pyritään pitämään lyhyenä ja selkeänä, muutama A4 – mittainen sivu. Se tulee kirjoittaa niin yleisellä tasolla, että jokainen sen lukeva sen ymmärtää. Se ei myöskään saa sisältää sellaisia tietoja, jotka mahdollistavat hyökkäyksen tai tietomurron yrityksen järjestelmiin. Luonteeltaan tietoturvapolitiikka on julkinen ja tarkoitettu henkilökunnan lisäksi asiakkaille ja yhteistyökumppaneille.

Yritys Oy:n tietoturvapolitiikassa tuodaan esille yrityksen johdon tahtotila ja sitoutuminen tietoturvallisiin toimintatapoihin kaikessa yrityksen toiminnassa. Siinä sitoutetaan myös jokainen henkilökunnan jäsen noudattamaan yrityksen tietoturvapolitiikkaa. Yrityksen tietoturvapolitiikassa on huomioitu ja painotetaan nimenomaan liiketoiminnan kannalta tärkeitä asioita.

Tietoturvallisuuskoulutuksen ja tiedotuksen tärkeyttä korostetaan, sekä määritellään eri osa-alueille vastuuhenkilöt. Politiikassa painotetaan, että jokaisella on vastuu tietoturvan toteutumisesta. (Kts. Liite 1)

Politiikkaa tulee katselmoida säännöllisesti ja pohtia sen sisällön ajantasaisuutta. Ja mikäli muutoksille on tarvetta, päivitetään politiikka vastaamaan yrityksen nykytilaa. (Laaksonen ym. 2006, 146.)

6.3 **Tietoturvastrategia**

Tietoturvastrategiassa määritellään tietoturvatyön vastuualueet sekä organisaation tietoturvallisuudesta vastaavien roolit. Strategian tulee olla organisaation ydintoiminnan ja -tavoitteiden mukainen sekä tukea asetettujen tavoitteiden saavuttamista. Strategia ei saa muodostua yrityksen ydintoiminnasta irralliseksi. (Vahti. 2013. Sovelluskehityksen tietoturvaohje 1/2013, 33)

Tietoturvastrategian suunnittelussa on otettava huomioon, että se tukee yrityksen liiketoimintasuunnitelmaa, ydintoimintoja ja kasvusuunnitelmaa. Strategian suunnitteluun olisi hyvä osallistua henkilöitä kaikista yrityksen sidosryhmistä, kuten eri liiketoiminta-alueiden vastaavat henkilöt sekä IT-toiminnasta vastaavat henkilöt. Strategiaa suunnitellessa on otettava huomioon liiketoimin-

tariskit, jotta tietoturvatyö voidaan kohdentaa liiketoiminnan kannalta keskeisimpiin asioihin. (Vahti. 2013, 33)

Strategia dokumentissa käsitellään pitkän ja keskipitkän tähtäimen tavoitteet ja mittarit asetettujen tavoitteiden saavuttamiseksi sekä strategian hyödyt liiketoiminnalle. Lisäksi se sisältää toteuttamissuunnitelman, aikataulut, vastuuhenkilöt, tarkastuspisteet ja organisaation ylimmän johdon sitoutumiskirjeen. (Vahti. 2013, 33)

6.4 Suojattavien kohteiden tunnistaminen

Tietoturvaa suunniteltaessa organisaation täytyy ensin tunnistaa suojattavat kohteensa, eli mikä on yritykselle arvokasta. Sen jälkeen niille voidaan määrittää arvo. Kohteet tunnistetaan niin yksityiskohtaisesti kuin yritykselle on tarkoituksenmukaista. Suojattavat kohteet voidaan jakaa kahteen tyyppiin:

1. Ensisijaiset suojattavat kohteet, joita ovat esimerkiksi liiketoimintaprosessit ja liiketoiminnot sekä tieto.

2. Kaikentyyppiset ensisijaisia kohteita tukevat suojattavat kohteet, kuten laitteistot ja ohjelmistot, verkko, henkilöstö, toimipaikka ja organisaatiorakenne.(SFS-ISO/IEC 27005 2009, 66.)

Suojattavien kohteiden tunnistusta tehtäessä Yritys Oy:ssä rajattiin ensin toimintaympäristöä mistä suojattavia kohteita lähdettiin hakemaan. Toimintaympäristön ulkopuolelle jätettiin tässä työssä Yritys Oy:n omistuksessa olevat kiinteistöt joissa yrityksellä ei ole omaa henkilökuntaa tai tarjottavia tietoliikennepalveluita vuokralaisille.

Suojattavat kohteet rajattiin myös koskemaan lähinnä tietoliikenne-, laitteisto- ja ohjelmistoturvallisuuden osa-alueelta löytyviä kohteita. Fyysisen-, henkilöstö-, tietoaineisto-, käyttö- ja hallinnollisenturvallisuuden alueelta tietoturva- ja uhkakartoitusta täydennetään Yritys Oy:ssä myöhemmin.

Ensisijaisia kohteita Yritys Oy:lle ovat tieto ja liiketoimintaprosessit. Asiantuntijaorganisaatiossa tiedon luotettavuus, eheys ja saatavuus ovat tärkeässä roo-

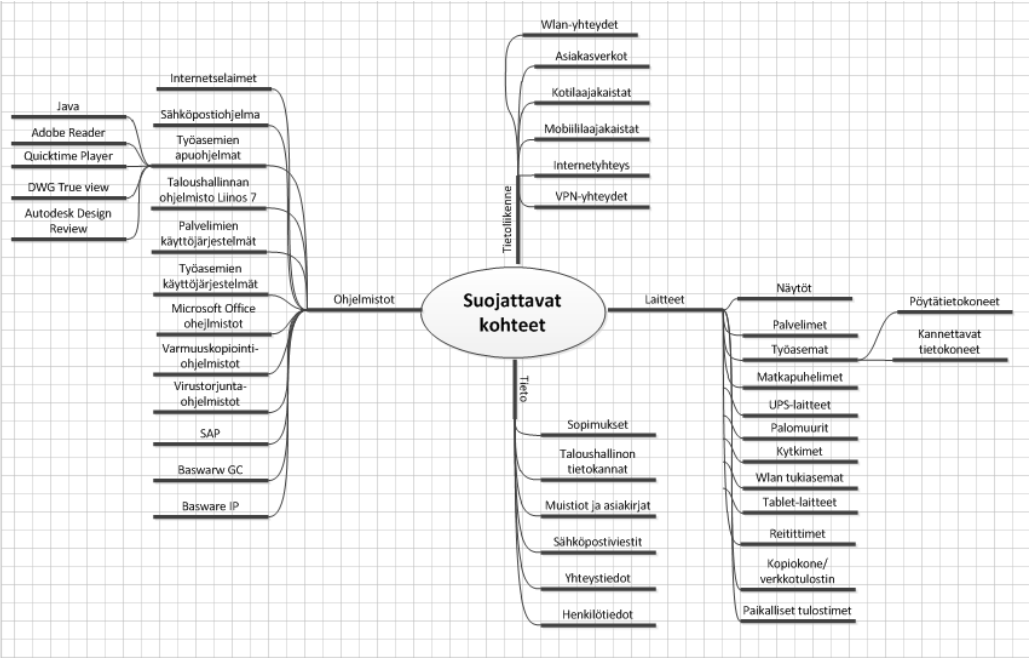
lissa. Tietoa on yrityksessä monenlaisessa muodossa, kuten henkilöstön osaamisena sekä ei dokumentoituna tietona henkilöstön tiedossa ja dokumentoituna tietona kytkimissä, palomuureissa ja työasemissa ja palvelimissa sekä tietokannoissa. Opinnäytetyötä tehdessä otettiin kantaa ainoastaan dokumentoituun tietoon ja sen saatavuuteen, eheyteen ja luotettavuuteen Tietoliikenne-, laitteisto- ja ohjelmistoturvallisuuden kannalta.

Liiketoimintaprosessien jatkuvuus vaatii korkeaa käytettävyyttä tietojärjestelmälaitteilta ja tietoliikenneyhteyksiltä sekä ohjelmistoilta.

Ensisijaisia kohteita tukevia suojattavia kohteita, joiden tietoturvallisuuteen keskityttiin, olivat tietojärjestelmälaitteistot, ohjelmistot ja verkot.

Suojattavat kohteet tulee luetteloida ja yksilöidä selkeästi sekä huolehtia luetteloiden ylläpitämisestä. Suojattaville kohteille tulee nimetä omistajat sekä määritellä vastuu riittävien turvamekanismien ylläpitämisestä. Omistaja voi kyllä delegoida turvamekanismien toteutuksen, mutta vastuu kohteiden asianmukaisesta suojauksesta säilyy kuitenkin aina kohteen omistajalla. (SFS-ISO/IEC 17799 2005, 50.)

Suojattavien kohteiden luettelointi ja dokumentointi sekä kohteille omistajien nimeäminen tehdään Yritys Oy:ssä myöhemmässä vaiheessa. Tässä vaiheessa suojattavia kohteita lähdettiin Yritys Oy:ssä tunnistamaan miellekartan avulla. Oheisessa kuviossa 6 on esimerkki miellekartasta.



Kuvio 4. Yritys Oy:n miellekartta suojattavista kohteista

Mind map eli miellekartta on diagrammi, jota käytetään visuaalisena apuvälineenä hahmottelemaan tietoa. Miellekartta luodaan usein yhden keskelle sijoitetun sanan ympärille, josta johtuneet ajatukset ja ideat kirjataan karttaan pääkategorioina ja niistä johtuneet ajatukset ja ideat taas niiden alikategorioina. (Mind map. 2012.)

Liitteessä 2 on kuvattuna miellekartta, jota käytettiin Yritys Oy:n suojattavien kohteiden tunnistamiseen.

6.5 **Uhkakartoitus**

Uhka- eli riskikartoituksessa haetaan yrityksen toimintaan liittyvät riskit ja uhkakuvat. Ensin kannattaa tehdä yleinen tietoturvariskien kartoitus, jonka avulla nähdään yleisellä tasolla mitä riskejä tietojenkäsittelyyn sisältyy. Tämän jälkeen voidaan tehdä tietojärjestelmäkohtainen riskikartoitus ja analyysi. Yleistä tietoturvariskien kartoitusta voidaan käyttää myöhemmin tarkistuslistana tietojärjestelmäkohtaista riskikartoitusta tehtäessä. (Hakala ym. 2006, 80.)

Mikäli yrityksen tietojärjestelmistä on olemassa kattava ja hyvä dokumentointi, voidaan sitä käyttää hyväksi riskien käsittelyssä ja tunnistamisessa. Mutta mikäli dokumentaatio on puutteellinen, kannattaa riskikartoitus tehdä esimerkiksi

miellekarttojen avulla. Kaikki potentiaaliset uhat saadaan parhaiten kartoitettua mikäli yrityksen eri henkilöstöryhmät osallistuvat kartoituksen tekemiseen, kuten järjestelmien käyttäjät sekä järjestelmäasiantuntijat. Riskikartoituksessa kannattaa tarkastella nykytilannetta sekä tulevaisuuden mukanaan tuomia uhkakuvia. Tiedot esiintyneistä ongelmista kannattaa ottaa lähtökohdaksi ja sen jälkeen pyritään hakemaan potentiaalisia uhkia joita ei ole vielä esiintynyt, mutta joita pidetään mahdollisina. (Hakala ym. 2006, 80–81.)

Uhkat voivat olla tahallisia, tahattomia tai ympäristöön liittyviä. Uhkat voivat realisoituessaan johtaa pahimmillaan liiketoiminnan keskeytymiseen, välttämättömien palveluiden vahingoittumiseen tai keskeytymiseen. (SFS-ISO/IEC 27005 2009, 84.)

Yritys Oy:ssä tietojärjestelmien dokumentointi oli vielä puutteellinen, joten kattavaa dokumentaatiota ei ollut käytettävissä riskikartoituksen tekemisen avuksi, vaan käytettiin hyväksi miellekarttaa, jonka avulla ensin tehtiin yleinen riskikartoitus.

Lisäksi yleistä uhkakartoitusta tehtäessä Yritys Oy:ssä käytettiin hyväksi SFS-ISO/IEC 27005 standardin liitteessä C olevaa luetteloa tyypillisistä uhkista jotka voivat vaarantaa yrityksen tietoturvallisuuden. Luettelosta poimittiin laitteisto-, ohjelmisto- ja tietoverkkoturvallisuuteen vaikuttavia mahdollisia uhkia.

Taulukossa uhkan aiheuttajat on jaoteltu standardissa tahallisiin (D), tahattomiin (A) tai ympäristöön liittyviin (E).

Taulukko 2. Uhkakartoitustaulukko (SFS-ISO/IEC 27005 liite C)

Tyyppi	**Uhka**	**Aiheuttaja**
Fyysinen vaurio	- Tuli	A, D, E
	- Vesivahinko	A, D, E
	- Laitteiston tai tietovälineiden tuhoutuminen	A, D, E

Lunnonilmiöt	- Ukkonen	E
Välttämättömien palvelujen menettäminen	- Virransyötän katkeaminen - Tietoliikennelaiteiden häiriö	A, D A, D
Säteilyn aiheuttamat häiriöt	- Lämpösäteily	A, D, E
Tiedon vaarantuminen	- Salakuuntelu - Tietoväline- tai asiakirjavarkaudet - Laitteistovarkaudet - Kierrätettyjen tai käytöstä poistettujen tietovälineiden talteenotto - Epäluotettavista lähteistä saatu aineisto - Laitteiston peukaloiminen - Ohjelmiston peukaloiminen	D D D D A, D D A, D
Tekniset häiriöt	- Laiterikko - Laitteen toimintahäiriö - Ohjelmiston toimintahäiriö - Tietojärjestelmän ylläpidettävyyden pettäminen	A A A A, D
Luvattomat toimet	- Laitteiston luvaton käyttö - Ohjelmiston vilpillinen kopiointi - Väärennetyn tai kopioidun ohjel-	D D

	miston käyttö - Aineiston turmeltuminen - Aineiston luvaton käsittely	A, D D D
Toimintojen vaarantuminen	- Käyttövirhe - Oikeuksien väärinkäyttö - Oikeuksien väärentäminen	A A, D D

Lisäksi Yritys Oy:ssä käytettiin vielä SFS-ISO/IEC 27005 standardin liitteessä D olevaa luetteloa eri turvallisuusalueiden haavoittuvuuksista ja uhkista jotka, voivat hyväksi käyttää näitä haavoittuvuuksia. Turvallisuusalueista tarkasteltiin tässäkin laitteisto-, ohjelmisto- ja tietoverkkoalueita. Taulukosta poimittiin todennäköiset haavoittuvuudet joihin tulee kiinnittää huomiota ja tehdä riskianalyysi.

Taulukko 3 Luettelo turvallisuusalueiden haavoittuvuuksista (SFS-ISO/IEC 27005 liite D)

Tyyppi	**Esimerkki haavoittuvuudesta**	**Esimerkki uhkasta**
Laitteisto	Tallennusvälineiden riittämätön ylläpito ja virheellinen asennus Altistuminen kosteudelle, pölylle ja likaantumiselle Altistuminen jännitevaihteluille Suojaamaton varasto	Tietojärjestelmän ylläpidettävyyden pettäminen Laitteiston tai tietovälineiden pettäminen Virransyötön katkeaminen Tietoväline ja asiakirja

		varkaudet
	Huolimaton käytöstä poistaminen	Tietoväline- tai asiakirjavarkaudet
	Altistuminen lämpötilavaihteluille	Sääilmiöt
Ohjelmisto	Ohjelmistotestaus toteuttamatta tai riittämätöntä	Oikeuksien väärinkäyttö
	Ohjelmiston tunnetut viat	Oikeuksien väärinkäyttö
	Ei kirjauduta ulos poistuessa työasemalta	Oikeuksien väärinkäyttö
	Tallennusvälineiden hävittäminen tai uusiokäyttö ilman kunnollista tietojen pyyhkimistä	Oikeuksien väärinkäyttö
	Tunnistus- ja todennusmekanismien, kuten käyttäjän todentamisen, puute	Oikeuksien väärentäminen
	Huono salasana hallinto	Oikeuksien väärentäminen
	Tarpeettomien palvelujen aktivointi	Aineiston luvaton käyttö
	Ohjelmistojen valvomaton lataaminen	Ohjelmiston peukaloiminen
	Varmuuskopioiden puute	Ohjelmiston peukaloiminen
	Fyysisen suojauksen puute raken-	

	nuksen ovissa ja ikkunoissa	Tietoväline- tai asiakirjavarkaudet
Verkko	Suojaamattomat viestintälinjat	Salakuuntelu
	Suojaamaton arkaluontoinen tietoliikenne	Salakuuntelu
	Yhden pisteen vikaantuminen	Tietoliikennelaitteiden häiriö
	Turvaton verkkoarkkitehtuuri	Etävakoilu
	Suojaamattomat julkiset verkkoyhteydet	Laitteiston luvaton käyttö
	Riittämätön verkonhallinta	Tietojärjestelmän kyllääntyminen

Kun miellekartta yleistä uhkakartoitusta varten oli saatu valmiiksi, hyödynnettiin sitä tietojärjestelmäkohtaisien uhkakartoituksien tekemiseen. Tietojärjestelmäkohtaisilla uhkakartoituksilla tarkoitetaan tässä ohjelmistoihin, laitteisiin ja tietoliikenteeseen kohdistuvien uhkien kartoitusta. (Kts. liitteet 3-6).

Käytettäessä uhkaluetteloita ja aikaisemmin tehtyjä uhka-arviointeja tulee muistaa, että uhkat vaihtelevat ja muuttuvat jatkuvasti, varsinkin mikäli liiketoimintaympäristössä tai tietojärjestelmäympäristössä tapahtuu muutoksia. (SFS-ISO/IEC 27005 2009, 28.)

Riskien arviointi

Kun suojattavat kohteet on tunnistettu ja luetteloitu sekä uhkakartoitus on tehty, arvioidaan seuraukset joita eheyden, luottamuksellisuuden ja käytettävyyden menettämisellä olisi suojattaville kohteille sekä uhkien realisoitumistodennäköisyys. (SFS-ISO/IEC 27005 2009, 32.)

Uhkan toteutumisen seurauksia voivat olla esim. laitteistolle tai ohjelmalle aiheutuneen vian tutkimiseen ja korjaamiseen kulunut aika, menetetty työaika, mahdollisesti menetetty liiketoiminta mahdollisuus, vahingon korjaamisen aiheuttamat rahalliset menetykset ja yrityksen imagolle ja maineelle aiheutuneet vahingot. (SFS-ISO/IEC 27005 2009, 32.)

Yritys Oy:ssä uhkien realisoitumistodennäköisyyttä arvioitiin aikaisempien vikatilanteiden ja tapahtumien perusteella sekä tarkastelemalla liiketoimintaympäristöä ja toimitilojen sijaintia ja kuntoa. Toteutuneen riskin seurauksien vakavuutta arvioitiin lähinnä menetetyn työajan ja aiheutuneiden välittömien kustannusten perusteella sekä mahdollisia vaikutuksia yrityksen imagolle. Uhkien realisoitumistodennäköisyyttä sekä seurauksien vakavuutta kuvaavat numerot kirjattiin riskienhallintataulukkoon.

6.6 **Riskianalyysi**

Riskianalyysi voidaan jakaa kahteen eri vaiheeseen: riskikartoitukseen ja riskien arviointiin. Riski- tai uhkakartoituksessa toimintaan liittyvät uhkat kartoitetaan, kuten aiemmin on esimerkiksi kuvattu. Riskien arvioinnissa puolestaan löydettyjen riskien ja uhkien vaikutusta yrityksen toimintaan arvioidaan. (Hakala ym. 2006, 80.)

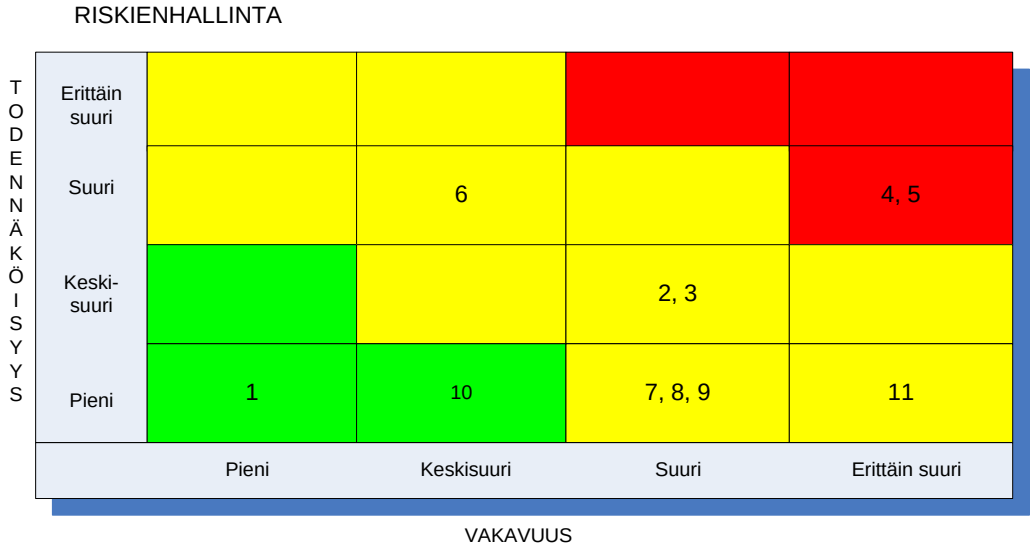
Vahinkojen vakavuutta ja niiden todennäköisyyttä arvioidaan yhtä aikaa. Mitä suurempaa vahinkoa uhka voi yritykselle aiheuttaa, ja mitä todennäköisempi uhka on, sitä enemmän riskiin on varauduttava. (Hakala ym. 2006, 81.)

Vahinkojen vakavuuden ja todennäköisyyden arvioinnissa käytetään yleensä kaaviota, jonka pystyakselille sijoitetaan vahingon vaikutusta yrityksen liiketoiminnalle kuvaava arvo ja vaaka-akselille sijoitetaan vahingon todennäköisyyttä kuvaava arvo. Asteikko voi olla yksinkertainen joko sanallisiin kuvauksiin perustuva tai numeerisilla arvoilla varustettu taulukko. (Hakala ym. 2006, 82.)

Kuviossa 7 on esimerkki riskienhallintataulukosta, johon on sijoitetaan luetteloidut uhat niiden vakavuuden ja todennäköisyyden perusteella. Numerot tau-

lukon sisällä merkkaavat kyseisen uhkan numeroa erillisessä luettelossa, johon uhkat on kerätty. Taulukkoon voidaan merkitä eri väreillä suojaustoimenpiteiden kiireellisyys. Esim. punaisella värillä merkitään ne riskit joilta tulee suojautua välittömästi. Keltaisella ne riskit joilta tulee suojautua sovitun aikataulun mukaisesti, ja vihreällä värillä ne riskit, jotka tietoisesti hyväksytään.

Kun Yritys Oy:ssä oli saatu uhkat luetteloitua ja kerättyä riskienhallintataulukkoon, voitiin tarkastella mitkä uhkat sijoittuivat punaiselle alueelle ja mitkä keltaiselle. Tämän jälkeen tarkistettiin mikä oli uhkilta suojautumisen vaativien toimenpiteiden tila. Mikäli toimenpidettä ei ollut vielä toteutettu lainkaan tai se oli puutteellinen, voitiin aikatauluttaa korjaava toimenpide. Yritys Oy:ssä kerättiin taulukkoon uhkat omiin sarakkeisiinsa sekä arvo niiden realisoitumistodennäköisyydelle ja uhkan vakavuudelle. Lisäksi kirjattiin omiin sarakkeisiinsa uhkalta suojaava tai sitä pienentävä toimenpide sekä toimenpiteen tila yrityksessä. Huomio sarakkeeseen kirjattiin mahdollinen puute suojauksessa ja aikataulu puutteen korjaamiseen.



Kuvio 5. Riskienhallintataulukko (Hautamäki 2011a, 36)

6.7 **Riskienkäsittelytoiminta**

Tietojenkäsittelyyn kuten liiketoimintaankin kuuluu riskejä. Tietojenkäsittelyn riskit ovat osa liiketoimintariskejä, ja niitä tulisi käsitellä kuten muitakin yritystoimintaan liittyviä riskejä. Riskejä ei voi kokonaan poistaa mutta niiden toden-

näköisyyttä ja vaikutuksia voidaan pienentää. Riskeihin voidaan varautua tai päättää tietoisesti olla varautumatta joihinkin riskeihin. (Hakala ym. 2006, 90.)

Riskienhallintaan kuuluu hyväksyttävien riskien kriteerien luominen. Eli millä perusteille jokin tietojenkäsittelyyn liittyvä riski hyväksytään sellaisenaan, ilman, että sen vaikutuksia tai todennäköisyyttä yritetään pienentää jollain tietoturvatoimenpiteellä. Tämä, kuten yleisten liiketoimintariskien hallinta, ovat yritysjohdon tehtäviä. Johto vastaa myös hyväksyttävien tietoturvallisuusriskien arviointikriteerien määrittelystä. (Hakala ym. 2006, 90.)

Yritys voi myös hallita riskejä siirtämällä niitä yrityksen ulkopuolelle, esimerkiksi ulkoistamalla tietojenkäsittelytoimintoja ulkopuoliselle palveluntuottajalle. Ulkoistettu riski tulee kuitenkin hallita, eli palvelluntuottajan toimintaa on valvottava ja varmistuttava sen riittävästä tietoturvallisuustasosta. (Hakala ym. 2006, 90.)

Riskeiltä, joita ei haluta tietoisesti ottaa, tai joita ei voida siirtää ulkopuoliselle palveluntuottajalle, suojaudutaan tai niiden realisoitumiseen varaudutaan. Suojautumistoimenpiteet voivat olla teknisiä tai hallinnollisia. Kaikilta riskeiltä ei voida suojautua riittävästi, tällöin yritys voi turvata toiminnan jatkuvuutta vakuutuksilla. (Hakala ym. 2006, 90.)

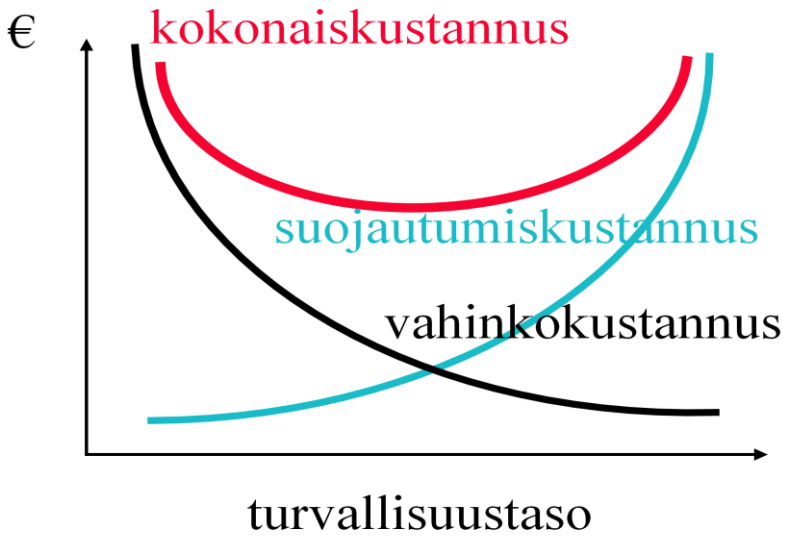
Tietoturvaratkaisuilla pyritään siis pienentämään riskin todennäköisyyttä tai sen vaikutuksia yrityksen liiketoimintaan. Tietoturvasuunnittelija pyrkii löytämään kustannustehokkaan keinon riskin pienentämiseksi. Yleensä yhdistellään useampaa hallinnollista ja teknistä suojautumiskeinoa. Suojautumiskeinoilla pyritään laskemaan riskin vaikutukset, sen realisoituessa, hyväksyttävälle tasolle. Suojautumiseen käytettävien kustannuksien on oltava pienemmät kuin riskin realisoituessa liiketoiminalle aiheuttamat taloudelliset menetykset. (Hakala ym. 2006, 91.)

Yritys Oy on ulkoistanut joitakin IT-palveluita palveluntuottajalle. Esimerkiksi verkonvalvonta ja etäyhteyspalvelut on ulkoistettuja. Ulkoistettujen palveluiden riskejä pyritään pienentämään tehdyillä palvelusopimuksilla, joissa määritellään saatavuudet ja vasteajat kyseisille palveluille. Lisäksi palveluiden toimi-

vuutta valvotaan Yritys Oy:n sisältä jatkavasti. Palveluntuottaja kanssa on myös säännölliset palaverit puolivuosittain, joissa palvelujen toimivuutta tarkastellaan.

Kustannusten arviointi

Kun uhkien vakavuus ja todennäköisyys on selvitetty, on syytä myös tarkastella uhkasta koituvaa kustannusta sen realisoituessa ja verrata sitä tietoturvatoimenpiteiden kustannuksiin, jotka syntyvät uhkaa torjuttaessa. Vahinkokustannusten ja suojautumiskustannusten välille on löydettävä optimi. (Hautamäki 2011b, 6)



Kuvio 6. Kustannusten vertailu (Hautamäki 2011b, 6.)

Yksittäistä riskiä vastaan voidaan suojautua yleensä monella eri tavalla, ja yksi suojautumiskeino saattaa suojata useammalta eri uhkalta, ja toinen vaikuttaa vain tiettyyn uhkaan. Kaikkia tietoturvan suunnittelun yhteydessä esiin tulleita keinoja ei yleensä kannata ottaa käyttöön vaan valita kustannuksiltaan ja hyödyltään sopivin. (Hakala ym. 2006, 94.)

Täysin ilmaisia suojautumiskeinoja ei yleensä ole. Suojautumiskeinon kustannuksen on oltava pienemmät kuin uhkan realisoituessaan aiheuttamat kustannukset. Eli suojaustoimenpiteestä aiheutuvia kustannuksia on aina verrattava tiedon arvoon. (Hakala ym. 2006, 94.)

Kuviossa 8 on havainnollistettu kuinka turvallisuustasoa nostetaan panostamalla suojautumiskeinoihin. Samalla vahinkojen kustannukset pienenevät ja vastaavasti suojautumiskustannukset nousevat.

Suojaustoimenpiteistä muodostuvat kustannukset muodostuvat välittömistä kustannuksista ja välillisistä kustannuksista. Välittömät kustannukset ovat suoraan itse suojausratkaisuun liittyvät kustannukset, kuten lisenssit ja hankintakustannukset. Välillisiä kustannuksia ovat puolestaan ratkaisun käyttöön liittyviä kustannuksia, kuten koulutus ja työajanmenetys. (Hakala ym. 2006, 95.)

Suojaustoimenpiteiden kustannusten arvioinnissa kannattaa kustannukset laskea pidemmällä aikavälillä esim. kumulatiivisesti viidelle vuodelle. Joissakin tapauksissa hankintakustannukset tai välittömät kustannukset saattavat olla pienet mutta välilliset eli käyttökustannukset suuret. Tietoteknisten ratkaisujen käyttöikä ei kuitenkaan ole yleensä kovin pitkä, joten sekin kannattaa huomioida kumulatiivisia kustannuksia tietylle aikavälille laskettaessa. (Hakala ym. 2006, 96.)

7 TIETOTURVASUUNNITELMA

7.1 Yleistä

Tietoturvasuunnitelma sisältää konkreettisesti ne käytännöt, työmenetelmät ja tekniset ratkaisut, joilla haluttuun tietoturvallisuuden tasoon pyritään. Tietoturvasuunnitelma laaditaan 2-5 vuoden aikavälille ja sen reunaehtoina toimii yritykselle laadittu tietoturvapolitiikka. Organisaatiossa käyttöön otettavat uudet teknologia ja toimintaprosessit vaativat kuitenkin tietoturvasuunnitelman jatkuvaa päivittäistä. Toisin kuin tietoturvapolitiikka, tietoturvasuunnitelma ei ole julkinen dokumentti, sillä siinä kuvataan yksityiskohtaisemmin käytettyjä menetelmiä ja teknisiä ratkaisuja. Tietoturvasuunnitelma voi olla osa yrityksen omaa tai standardiin perustuvaa laatukäsikirjaa, mikäli yrityksellä on sellainen käytössään. (Hakala ym. 2006, 9.)

Yritys Oy:n tietoturvaa tarkasteltiin ohjelmisto-, laitteisto- ja tietoliikenneturvallisuuden osalta. Uhkakartoituksessa löytyneiden riskien vakavuus ja todennäköisyys arvioitiin. Suojaavien toimenpiteiden nykytila myös tarkistettiin ja tarvittaville toimenpiteille määriteltiin aikataulu. Tietoturva- ja uhkakartoituksesta saatiin hyvä kehys, jota yrityksessä voidaan hyödyntää kenties myöhemmässä vaiheessa tehtävässä tietoturvasuunnitelmassa.

Koska tietoturvasuunnitelmat ja uhkakartoitukset ovat jatkuvasti kehittyviä dokumentteja, korjataan yleensä ensimmäisellä iteraatiokierroksella löytyneitä uhkia, jonka jälkeen tilannetta tarkastellaan uudelleen.

Tietoturvallisuuden mittaaminen liittyy tietoturvallisuuden seurantaan ja valvontaan. Tietoturvan mittaaminen voidaan antaa tietyn tahon vastuulle, kun taas seuranta ja valvonta voidaan nähdä koko organisaation tehtävänä. (Laaksonen ym. 2006, 267)

Tietoturvallisuuden mittaamisen tarkoituksena on tuottaa informaatiota, joka auttaa suojaustoimenpiteiden suunnittelussa, priorisoinnissa ja investointipäätösten tekemisessä sekä tietoturvallisuuden johtamisessa. Tietoturvallisuuden mittaamisella pyritään mm. saamaan vertailuaineistoa tietoturvallisuuden kehittämiseksi, kouluttamaan henkilökuntaa, vakuuttamaan sidosryhmät ja kohdistamaan korjaavat toimenpiteet oikein. (Laaksonen ym. 2006, 268–269)

Tietoturvallisuus koostuu kahdeksasta eri osa-alueesta, joita ovat hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöstö-, tietoliikenne-, ohjelmisto-, laitteisto-, tietoaineisto- ja käyttöturvallisuus. Kutakin osa-aluetta on kuvattu tarkemmin seuraavissa alaotsikoissa.

7.2 **Hallinnollinen turvallisuus**

Tietoturvallisuuden kehittäminen ja johtaminen ovatkin hallinnollisen turvallisuuden pyrkimys. Organisaation tietohallinto vastaa yleensä tästä osa-alueesta. Siihen kuuluvat niin yhteydenpito ulkopuolisiin viranomaisiin kuin yhteydenpito oman organisaation sisäisiin turvallisuudesta vastaaviin elimiin. (Hakala ym. 2006, 10.)

Tärkeänä osana on arvioida eri palvelusopimusten, lisensointien ja lainsäädännön vaikutuksia yrityksen tietoturvakäytäntöihin. (Hakala ym. 2006, 11.)

Yritys Oy:ssä hallinnollisen tietoturvallisuuden kehittämistä ei otettu laajemmin kuin tietoturvapolitiikan osalta tämän opinnäytetyön piiriin.

7.3 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstön toimista aiheutuvien ja henkilöstöön kohdistuvien tietoturvauhkien hallintaa. Tietojenkäsittely tulee suojata henkilöstön aiheuttamilta tahallisilta ja tahattomilta virheiltä ja vahingoilta. (Laaksonen ym. 2006, 138)

Organisaation tietojärjestelmien ja tietojen käyttöoikeuksien rajaaminen ja sekä vastuiden määrittäminen kuuluu henkilöstöturvallisuuden osa-alueeseen. Henkilöstö tulee myös kouluttaa käyttämään tietojärjestelmiä, jolla taataan käyttäjien toimintakyky. Henkilöstöhallinto on vastuussa yleensä henkilöstöturvallisuudesta yhdessä tietohallinnon kanssa. (Hakala ym. 2006, 11.)

Uusien työntekijöiden palkkaamiseen liittyvät taustatarkistusten tekeminen ovat osa henkilöstöturvallisuutta. Taustatarkistusten avulla voidaan vähentää uuden henkilön palkkaamiseen tai yhteistyökumppanin valintaan liittyviä riskejä. (Laaksonen ym. 2006, 139)

Tässä opinnäytetyössä ei käsitelty henkilöturvallisuuteen liittyviä asioita Yritys Oy:n osalta.

7.4 Fyysinen turvallisuus

Rakennusten ja niiden eri tilojen suojaaminen erilaisilta uhkilta kuten ilkivallalta, murroilta, vesi- ja palovahingoilta ja sähkö- ja lämmitysjärjestelmien toimintahäiriöiltä on osa fyysistä turvallisuutta. Fyysisen turvallisuuden ylläpito on suurilta osin kiinteistönhoidon ja vartioinnin ammattilaisten vastuulla. Tietohallinnon on kuitenkin hyvä osallistua tietojenkäsittelytilojen, kuten palvelintilojen fyysisen suojauksen ylläpitoon. (Hakala ym. 2006, 11.)

Tässä työssä ei käsitelty fyysiseen turvallisuuteen liittyviä asioita laajemmin Yritys Oy:n osalta.

7.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuteen kuuluu tietoliikenneratkaisujen kuten lähi- ja laaja-verkkoyhteyksien turvallisuudesta huolehtiminen. Tällä pyritään turvaamaan tietoliikenteessä kulkevan tiedon eheys, luotettavuus ja saatavuus. (Hakala ym. 2006, 12.)

Tietoverkkojen toiminta ja eri verkkojärjestelmät, joilla verkkoyhteyksiä toteutetaan, tulee suunnitella ja toteuttaa hyvää tietojenkäsittelytapaa noudattaen. Valitun verkkoarkkitehtuurin tulee tukea menetelmiä, joilla voidaan suojautua eri uhkia vastaan. (Vahti 2009, 51.)

Tietoliikenneturvallisuuteen kuuluu mm. tietoliikennelaitteiden asennus, luettelointi ja ylläpito. Lisäksi monitoroidaan muutoksia sekä seurataan määritettyjä lokeja tapahtumista. Olennainen osa on myös pääsyn valvonta ja verkon hallinta, liikenteen salaus, varayhteydet ja verkko-ohjelmistojen testaus ja hyväksyntä. Epänormaalien tietoturvatilanteiden tutkiminen ja dokumentoiminen kuuluvat osaltaan myös tietoliikenneturvallisuuteen. (Vahti 2009, 51.)

Yritys Oy:n lähiverkon tietoturvallisuus

Yritys Oy:ssä tarkasteltiin tietoliikenneturvallisuutta tekemällä uhkakartoitus miellekartan avulla. Kts. liite 6. Löytyneille uhkille tehtiin riskianalyysi ja sen perusteella riskien käsittelytoiminta ja päätettiin tarvittavat toimenpiteet.

Lisäksi Yritys Oy:n lähiverkon tilaa tarkasteltiin Vahti Sisäverkko-ohje-dokumentista löytyvän tarkistuslistan avulla. Ohjeistuksesta poimittiin yritykselle soveltuvat ja sitä koskettavat ohjeet ja tarkistuslistat. Ohjeesta käytettiin hyväksi tarkistuslistat verkon rakenteelle, yhteistyölle muiden toimijoiden kanssa, kaapeloinnille, langattomalle lähiverkolle, verkon aktiivilaitteille, sisäverkon päätelaitteille, sisäverkon palveluille, tunnistautumiselle ja verkon hallinnalle/valvonnalle.

Verkon rakenne

Vahti Sisäverkko-ohje dokumentista poimittiin seuraavia ohjeita ja toimenpiteitä, joiden tilaa tarkasteltiin Yritys Oy:ssä.

- Verkolla on nimettävä omistaja, joka voi tehdä päätöksiä verkon suhteen. Verkon ylläpito on usein delegoitu vastuuhenkilöille tai ulkopuolisille organisaatioille. Verkon omistaja on kuitenkin organisaation sisältä, mutta ylläpitäjä voi olla ulkoistettu.

- Verkosta tulee olla ajantasainen dokumentaatio, josta löytyvät ainakin seuraavat tiedot: Fyysinen arkkitehtuurikuva, joka kuvaa verkon fyysisen rakenteen eli kaapeloinnit ja verkon aktiivilaitteet. Erityisesti liitäntäpisteet ulkoisiin verkkoihin tulee olla selkeästi merkitty. Looginen arkkitehtuurikuva, joka kuvaa verkon loogisen rakenteen eli eri verkkoalueet ja mahdolliset virtuaaliverkot (VLAN). Verkon laitelista, jossa on määritelty vähintään kunkin laitteen osoitetiedot (MAC, IP), omistaja, fyysinen sijainti sekä käyttötarkoitus.

- Liikennettä sisä- ja ulkoverkon välillä rajoitetaan teknisesti siten, että vain tarpeellinen liikenne päästetään läpi. Rajoitus suoritetaan teknisesti esim. palomuurin avulla. Etäkäyttöyhteyksiä voidaan avata sisäverkkoon kontrolloidusti, tiettyihin rajoitettuihin palveluihin. Etäkäyttöyhteydet salataan.

- Verkot jaetaan käyttötarkoituksensa mukaan loogisesti erillisiin aliverkkoihin, esim. sisäiseksi, ylläpito- (hallinta-/valvonta-), asiakas-, ja vierailijaverkoksi.

- Sallitut yhteydet ulkoverkosta on dokumentoitu ja hyväksytetty organisaation tietoturvallisuudesta vastaavalla henkilöllä.

- Verkkoliitännät yleisölle avoimissa tiloissa on suojattu siten, että organisaation sisäverkkoon on pääsy ainoastaan sallituilla osapuolilla.

- Kriittiset verkon komponentit on kahdennettu.

- Suorat, ulkoverkosta sisäverkkoon otetut yhteydet on estetty.
- Verkon rakenne on suunniteltu kestämään nykyinen ja arvioitu tuleva liikennemäärä. (Vahti 2011, 20 - 38.)

Yritys Oy:ssä tarkistuslistasta suurin osa oli kunnossa. Verkon dokumentoinnissa on kuitenkin vielä puutteita. Myös verkon komponenttien redundanttisuudessa on parantamisen varaa.

Yhteistyö muiden toimijoiden kanssa

Dokumentista poimittiin seuraavat kolmannen osapuolen kanssa toimiessa huomioon otettavat asiat, jotka koskevat Yritys Oy:tä ja niiden tila tarkastetiin:

- Keskeisille verkon laitteille, liitännöille ja palveluille on palvelusopimuksin (SLA) tai muuten ylläpitojärjestelyin taattava kohteen kriittisyyttä vastaava ylläpitotaso.
- Palveluntarjoajan kanssa on sovittu henkilöt, jotka on kiinnitetty organisaation käyttöön ainakin normaaliolojen häiriötilanteiden aikana.
- Yhteistyökumppanin kanssa järjestetään säännöllisiä seurantapalavereja
- Mikäli yhteistyökumppanilla on pääsy salassa pidettävään tietoon, määritellään sopimukseen henkilöstön tarvittavat turvallisuusselvitykset. (Vahti 2011, 50.)

Yritys Oy:ssä kolmannen osapuolen kanssa olivat tarkistuslistan asiat kunnossa.

Kaapelointi

Kaapeloinnin osalta tarkasteltiin seuraavat tarkistuslistan asiat:

- Kaapelit kulkevat kytkeytymistä ja fyysisiä vaurioita ehkäisevissä rakenteissa.

- Jakamot, ristikytkentäpaikat ja verkon aktiivilaitteet sisältävät telineet sijaitsevat lukituissa tiloissa, joihin on pääsy vain valtuutetuilla henkilöillä.

- Kaapelointi on dokumentoitu ja näkösuojaan jäävät kaapelit on nimiöity dokumentteja vastaavasti molemmista päistään.

- Käyttämättömät liitäntäpisteet on irrotettu aktiivilaitteesta tai ao. laitteen portit estävät oletuksena uusien asemien vapaan liittämisen sisäverkkoon. (Vahti 2011, 53.)

Kaapeloinnin osalta ainoa löydetty ongelma liittyi dokumentointiin. Kaikkien kiinteistöjen kaapeloinnista ei ole olemassa ajantasaista dokumentaatiota, eikä kaapeleiden ja ristikytkentäpaneeleiden nimiöinti ole yhdenmukainen ja riittävä.

Langaton lähiverkko

Yritys Oy:ssä tarkasteltiin langattoman lähiverkon tietoturvallisuutta. Langattomalla lahiverkolla (WLAN, Wireless LAN) tarkoitetaan IEEE 802.11-standardeihin perustuvia verkkoja, joita kutsutaan myös Wi-Fi-verkoiksi (Wireless Fidelity). WLAN verkkojen haasteina voidaan pitää niiden kuuluvuutta rakennuksen ulkopuolelle, kuulumattomuutta rakennuksen sisällä, käyttäjien tai tunkeutujien mahdollisesti asentamia luvattomia tukiasemia, (rogue access point) sekä tunnettuja ongelmia liikenteen salauksessa. Samalla taajuusalueella olevat toimivat muut radiolähteet, kuten mikroaaltouuni, Bluetooth-laitteet sekä toiset WLAN verkot häiritsevät myös liikennettä. (Vahti 2011, 55.)

WLAN verkko voidaan saada toimintakyvyttömäksi samoilla kanavilla toimivilla tehokkailla lähettimillä tai suunta-antenneilla. WLAN verkkojen salaus salaa vain datan, mutta ei hallintaliikennettä eikä laitteiden fyysisiäosoitteita eli MAC-osoitteita. Yksittäinen laite voidaan pakottaa pois verkosta väärentämällä hallintaviestejä. Laitteiden MAC-osoitteet saadaan selville liikennettä tarkkailemalla, ja siten myös mahdollisesti henkilön paikallaolo ja sijainti. (Vahti 2011, 55.)

Yritys Oy:n kannalta oleelliset kohdat tarkistuslistasta olivat seuraavat:

- Vierailijaverkko: Langaton vierailijaverkko on toteutettava siten, että se on fyysisesti tai loogisesti eriytetty sisäverkosta ja siitä on vain yhteys Internetiin.

- Sisäverkkoon liitetty WLAN-verkko: WLANin liikenne tulee olla vahvasti salattu.

- Sisäverkkoon liitetty WLAN-verkko: WLANissa on käyttäjille vahva tunnistusmenettely.

- Vierailijaverkko: WLANissa on käyttäjille vahva tunnistusmenettely. (Vahti 2011, 55.)

Verkon aktiivilaitteet

Verkon aktiivilaitteiden osalta Yritys Oy:ssä tarkasteltiin seuraavat tarkistuslistan asiat:

- Verkolle on tehty riskianalyysi ja tämän tuloksena keskeiset verkkolaitteet, niiden komponentit (esim. virtalähde) ja yhteydet on tarvittaessa kahdennettu.

- Keskeisillä laitteilla on UPS ja kaikki verkon laitteet palautuvat virtakatkon jälkeen normaalitoimintaan.

- Verkkolaitteissa on vaihdettu tunnistukseen liittyvät toimittajien oletusparametrit.

- Tarpeettomat palvelut, ohjelmat ja protokollat on poistettu verkon aktiivilaitteista käytöstä.

- Verkkolaitteiden asetukset on tallennettu ja varmuuskopioitu mahdollista laitteen vaihtoa ja asetusten palauttamista varten.

- Laiteiden lokitiedot kerätään keskitetysti ja niitä seurataan säännöllisesti. (Vahti 2011, 61- 62.)

Sisäverkon päätelaitteet

- Kullakin päätelaitteella on yksilöity tunnus. Identtiset laitekokoonpanot erotetaan em. tunnuksen perusteella.
- Käyttäjille on laadittu lyhyet, selkeät ohjeet päätelaitteiden turvallisesta verkkokäytöstä - kullekin päätelaitetyypille omansa.
- Mobiililaiteiden loppukäyttäjiä on ohjeistettu niiden turvalliseen käyttöön.
- Työasemissa on käytössä työasemakohtainen palomuuri.
- Kannettavien työasemien kiintolevyt on salattu (Vahti 2011, 68 - 69)

Sisäverkon palvelut

- Sovellusten tietoturvapäivitykset pidetään ajan tasalla.
- Kriittisten infrapalveluiden, eli osoite-, reititys- ja nimipalvelun toimivuus on varmistettu tarkoituksen mukaisella palvelutasolla ja varautumisen tasolla
- Vastaanotetut ja lähetettävät sähköpostit skannataan virusten, haittaohjelmien ja roskapostien varalta.
- Resurssien jako (esim. kiintolevy, tulostin) on rajattu palvelinlaitteille. Työasemien resurssien jako on estetty. (Vahti 2011, 73)

Tunnistautuminen

- Käyttäjän tunnistamisessa käytetään henkilökohtaisia tunnuksia. Tämä koskee myös ylläpitotunnuksia.
- Etäyhteyksien muodostamiseen ei käytetä pelkkää käyttäjätunnus-/ salasanaparia.
- Kaikki käyttäjät ja päätelaitteet ovat hallittujen tunnistautumisratkaisujen piirissä.

- Käytettäessä käyttäjätunnus-/salasanaparia, luodaan salasanapolitiikka, joka koskee kaikkia palveluita ja käyttäjiä.

- Kaikkien verkkotuotteiden ja muiden valmisohjelmistojen oletustunnusten salasanat on vaihdettu oletusarvosta tai oletustunnus on poistettu.

- Organisaatio on määritellyt käyttäjänhallintaprosessin, jotta voidaan varmistua, että käyttöoikeudet vastaavat kulloistakin tehtävää. (Vahti 2011, 79 - 80)

Verkon hallinta/valvonta

Verkon valvontaa ja hallintaa koskien tarkistuslistasta poimittiin seuraavat kohdat:

- Verkon hallinnan yhteydessä jokaisesta muutoksesta otetaan varmuuskopio.

- Etukäteen on määritelty, mitä asioita verkossa valvotaan.

- Ulkoistettaessa verkon hallinta, määritellään hyvin tarkasti se, miten ja mitä toimenpiteitä ulkoistuskumppani tekee, miten ja millä toimenpiteillä valvontaa ja hallintaa tehdään. Säilytetään itsellä riittävä perusosaaminen verkoista, jotta voidaan ostaa siihen liittyviä palveluita

- Verkkolaitteiden ohjelmistot päivitetään valmistajan suositusten mukaisesti.

- Verkon hallintaan ja valvontaan on määritelty selkeät vastuuhenkilöt

- Käytetyt hallinta- ja valvontaprosessit on dokumentoitu.

- Verkkolaitteiden kuormitustilannetta valvotaan.

- Käyttäjät koulutetaan ilmoittamaan havaituista puutteista, ongelmista ja niiden epäilyistä esimiehelle, tietoturvavastaavalle tai verkon vastuuhenkilölle (Vahti 2011, 79 - 80)

Yritys Oy:ssä verkon valvonta- ja hallinta on ulkoistettu kolmannelle osapuolelle. Yrityksen oma IT-henkilöstö valvoo kuitenkin alihankkijan toimintaa.

IT-koordinaattori vastaa verkon dokumentaatiosta. Tavoitteena on saada Kivääritehtaan, Mattilanniemen, Starttitilojen ja Vitapoliksen verkkojen fyysiset ja loogiset topologiat dokumentoitua seuraavan kahden vuoden aikana. Kattavat topologia kuvat pienentävät vianselvitykseen kuluvaa aikaa. Tavoitteen saavuttamista voidaan mitata vertaamalla verkon vianselvittelystä aiheutuneita kustannuksia, aiempiin kustannuksiin ennen dokumentaation tekemistä.

Verkon aktiivilaitteiden varmuuskopioinnista ja ylläpidosta vastaa kolmasosapuoli eli yhteistyökumppani. IT-koordinaattori valvoo alihankkijan toimintaa. Alihankkijan kanssa pidetään säännöllisesti palaveri, jossa tarkastellaan ylläpitosopimusten toimivuutta ja täyttymistä.

Verkon aktiivilaitteiden sähkönsyöttö tulee varmistaa UPS-laitteilla. Laitteiden hankinnasta ja asennuksesta vastaa IT-koordinaattori. UPS-laitteilla pyritään ehkäisemään esimerkiksi ukkosesta johtuvien virransyöttö häiriöiden aiheuttamia verkkokatkoja. Toimenpiteen vaikutuksia voidaan mitata laskemalla verkkokatkojen lukumäärä tietyllä aikavälillä ja vertaamalla sitä edeltäviin lukemiin.

Sisäverkon päätelaitteiden ja mobiililaitteiden turvallisesta käytöstä laaditaan käyttäjille ohjeistus. Ohjeistuksen laatii IT-koordinaattori. Ohjeen hyväksyy talouspäällikkö.

7.6 **Ohjelmistoturvallisuus**

Ohjelmistojen testaus on tärkeä osa ohjelmistoturvallisuutta. Siinä varmistetaan että ohjelmistot soveltuvat suunniteltuun käyttötarkoitukseen, toimivat virheettömästi ja ovat yhteensopivia muiden käytettävien ohjelmien kanssa. Lisäksi ohjelmistoturvallisuuteen kuuluvat ohjelmistoversioiden ja lisenssien hallinta. (Hakala ym. 2006, 11.)

Ohjelmien asetukset käyttöönoton yhteydessä ovat myös osa ohjelmistoturvallisuutta. Sekä käyttöjärjestelmäasetukset, että työasemaohjelmistojen kuten

sähköposti ja tekstinkäsittelyohjelmistojen asetukset, tulee käyttöönoton yhteydessä asettaa yrityksen tietoturvakäytäntöjen mukaisiksi. Ohjelmisto päivityksistä on myös huolehdittava. (Hautamäki 2011b, 23.)

Yritys Oy:n ohjelmistoturvallisuus

Yritys Oy:n tietoturva- ja uhkakartoitusta tehdessä ja ohjelmistoturvallisuutta tarkastellessa tehtiin ohjelmistoihin liittyvä uhkakartoitus käyttämällä mielekarttaa. Kts.liite 5. Lisäksi käytettiin Vahti ohjeistusta käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvien toimien osalta. Ohjeen mukaan tulee tarkastella ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi. Ohjeesta poimittiin Yritys Oy:n toimintaan sopivat seuraavat kohdat:

- Tarkistetaan että, ohjelmistojen dokumentointi on kattavaa: vaatimukset, määrittelyt, tuotevertailut, testisuunnitelmat, testiraportit, asennukset, jne.
- Valitut ratkaisut, tuotteet ja palvelut ovat keskenään yhteensopivia.
- Ohjelmistolisenssit ovat ajan tasalla ja hallinnassa.
- Ohjelmistojen hankinta, kehitys, käyttöönotto ja ylläpito jne. on tietoturvallisuuden huomioiva prosessi.
- Kaikissa asennuksissa huomioidaan tietoturvallisuus. Oletusarvoiset asennukset ymmärretään turvattomiksi.
- Ylläpito on suunniteltua ja dokumentoitua.
- Ohjelmistojen vaatimat käyttäjätiedot ja pääsyoikeudet säilytetään ja hallitaan huolellisesti ja turvallisesti. Käyttäjien todennuksen tietoturvataso valitaan suojattavien tietojen turvaluokituksen perusteella.
- Ohjelmistoille on saatavilla riittävät tuki- ja päivityspalvelut.

- Ylläpitäjät ja käyttäjät saavat riittävän koulutuksen ohjelmiston hallintaan ja käyttöön. Sovellushankintaan ja -kehitykseen osallistujille on järjestetty riittävä tietoturvakoulutus

- Ohjelmistojen käsittelemät tiedot ja ohjelmiston käyttöasetukset varmistetaan säännöllisesti ja varmistusten oikeellisuus testataan.

- Haittaohjelmien torjumisesta on huolehdittu. (Ohjelmistoturvallisuus. 2013.)

Ohjelmistopäivityksistä huolehditaan Yritys Oy:ssä säännöllisesti. Lisäksi käyttöjärjestelmien ja Windows työasemaohjelmistojen päivittäminen tapahtuu automaattisesti palvelimelta WSUS:n kautta. Käyttäjillä ei myöskään ole oikeuksia asentaa ohjelmia tai tehdä ohjelmien asetuksiin muutoksia. Työasemilla on asennettuna mm. palomuuri-, varmuuskopiointi ja virustorjuntaohjelmistot.

Suuria ohjelmistohankintoja tai kehitystyötä ei ole tiedossa noin kahden vuoden kuluessa. Työasemien käyttöjärjestelmät ja työasemaohjelmistot on päivitetty uuteen versioon vuoden 2012 aikana. Myös palvelinlaitteisto käyttöjärjestelmineen on hankittu 2011, joten senkään uusiminen ei ole ajankohtainen. Yritys Oy:llä ei ole myöskään käytössään mitään erityisohjelmistoja / toiminnan ohjausjärjestelmiä. Yritys Oy:llä ei myöskään ole ohjelmistokehitystä.

Virustorjunta- ja varmuuskopiointiohjelistojen lisenssit on päivitetty muutamaksi vuodeksi eteenpäin, joten näiden ohjelmistojen uusiminen ei ole edessä pariin vuoteen. Varmuuskopioinnin ja virustorjunnan toiminnan seurannasta ja testauksesta vastaa IT-koordinaattori.

Mahdollisten uusien työasemaohjelmistojen hankinnasta päättää talouspäällikkö. Asennuksesta, ylläpidon dokumentoinnista ja ylläpidosta huolehtii IT-koordinaattori. Uusien palvelinohjelmistojen asennuksesta huolehtii palveluntarjoaja yhdessä IT-koordinaattorin kanssa. Automaattisilla ohjelmistopäivityksillä, ja käyttäjien oikeuksien rajoittamisella ohjelmien asentamisessa pyritään ehkäisemään mahdollisia ohjelmistojen vikatilanteita ja tietoturvauhkia. Ohjelmistolisenssien hallinnoinnista, dokumentoinnista ja ajantasaisuudesta vastaa IT-koordinaattori.

Ohjelmistoturvallisuutta voidaan Yritys Oy:ssä mitata esimerkiksi seuraamalla ohjelmistojen vikatilanteiden lukumäärää ja niistä syntyneitä kustannuksia tiettynä ajanjaksona. Ohjelmistoturvallisuudella pyritään minimoimaan ohjelmistojen vikatilanteet ja niistä aiheutuvat välilliset ja välittömät kustannukset. Koska aikaisempaa tietoturvasuunnitelmaa eikä mittaustuloksia ole, ei ensimmäisenä vuonna saada vielä uusien tietoturvatoimien vaikutuksia näkyviin, vaan saadaan pohja, johon verrata seuraavan mittausjakson tuloksia ja mahdollisten uusien tietoturvatoimien vaikutuksia.

7.7 **Laitteistoturvallisuus**

Laitteistoturvallisuuteen kuuluu tietokoneiden, oheislaitteiden ja muiden tietojärjestelmiin kuuluvien laitteiden mitoitus, testaus, huolto ja varautuminen laitteiden vanhenemiseen ja särkymiseen ja sitä kautta niiden korjaamiseen tai vaihtamiseen. Lisäksi laitteistoturvallisuuteen kuuluu laitteiden käytöstä aiheutuvien vaaratekijöiden arvioiminen ja minimoiminen. Tällaisia vaaratekijöitä voivat olla esimerkiksi sähköiskut ja muut loukkaantumisvaarat. (Hakala ym. 2006, 12.)

Yritys Oy:n laitteistoturvallisuus

Yritys Oy:n tietoturva- ja uhkakartoitusta tehdessä laitteistoturvallisuutta tarkastellessa tehtiin laitteisiin liittyvä uhkakartoitus käyttämällä miellekarttaa. Kts.liite 4. Lisäksi käytettiin ISO/IEC 17799 standardin ohjeistusta laiteturvallisuudesta.

Laitteistot tulisi sijoittaa siten, että ympäristövaarojen ja luvattoman tunkeutumisen riskejä vähennetään. Standardista poimittiin seuraavat toteuttamisohjeet:

- Laitteistot tulisi sijoittaa siten, että pääsy työskentelyalueille minimoidaan
- Arkaluonteista tietoa käsittelevät tietojenkäsittelypalvelut tulisi sijoittaa ja niiden näkyvyyttä rajoittaa vähentämään riskiä, että luvattomat henki-

löt näkevät tietoa käytön aikana, ja varastotilat tulisi suojata luvatonta pääsyä vastaan

- Tietojenkäsittelypalvelujen läheisyydessä syömisestä, juomisesta ja tupakoimisesta tulisi laatia ohjeet

- Sellaisia ympäristöolosuhteita, kuten lämpötilaa ja kosteutta, jotka voivat vaikuttaa haitallisesti tietojenkäsittelylaitteistojen toimintaan, tulisi tarkkailla. (SFS-ISO/IEC 17799 2009, 74.)

Laitteistot tulisi suojata sähkökatkoilta ja muilta peruspalveluiden aiheuttamilta häiriöiltä.

- Organisaation kannalta kriittisiä toimintoja ylläpitävien laitteistojen tueksi suositellaan katkotonta tehonsyöttöä (UPS) varmistamaan toiminnan suunnitelmanmukainen alasajo tai jatkuminen. (SFS-ISO/IEC 17799 2009, 76.)

Laitteistoja tulisi huoltaa asianmukaisesti käytettävyyden ja eheyden ylläpitämiseksi.

- Laitteistoja tulisi huoltaa toimittajan suosittelemin aikavälein ja tämän määräyksiä noudattaen

- kaikista epäillyistä ja sattuneista vioista sekä ehkäisevistä ja korjaavista toimenpiteistä tulisi pitää kirjaa

- kun laitteistolle on suunniteltu tehtäväksi huolto, tulisi toteuttaa asianmukaiset turvamekanismit ottaen huomioon, tekeekö huollon paikan päällä oleva henkilöstö vai organisaation ulkopuolinen taho, ja tarvittaessa arkaluonteiset tiedot tulisi poistaa laitteistosta tai huoltohenkilöstö tulisi hyväksyä. (SFS-ISO/IEC 17799 2009, 76-78.)

Toimitilojen ulkopuolelle vietyjen laitteiden turvallisuus:

- Toimitilojen ulkopuolelle vietyjä laitteita ja tietovälineitä ei saisi jättää valvomatta julkisille paikoille, kannettavat tietokoneet tulisi matkustaessa kuljettaa käsimatkatavarana ja naamioida jos mahdollista

- Toimitilojen ulkopuolella käytettävä laitteisto tulisi kattaa riittävällä vakuutusturvalla. (SFS-ISO/IEC 17799 2009, 78.)

Laitteistojen turvallinen käytöstä poistaminen ja kierrättäminen:

- Arkaluonteista tietoa sisältävät laitteet tulisi tuhota fyysisesti tai tieto tulisi tuhota, poistaa tai toteuttaa päällekirjoitus käyttäen tekniikoita, jotka tekevät alkuperäisen tiedon palauttamisen mahdottomaksi, tavanomaisen tiedon poiston tai välineen formatoimisen sijasta. (SFS-ISO/IEC 17799 2009, 78.)

Yritys Oy:ssä laitteistot on vakuutettu. Vakuutuksista vastaa talouspäällikkö.

Päätelaitteet on vakioitu, jotta ylläpito olisi tehokkaampaa. Laitteiden hankinnasta päättää talouspäällikkö ja hankinnasta vastaa IT-koordinaattori.

Laitteiden tuhoamisesta ja kierrättämisestä tulee laatia ohjeistus. Ohjeen laatimisesta ja laitteiden kierrättämisestä ja tuhoamisesta vastaa IT-koordinaattori. Ohjeistuksen hyväksyy talouspäällikkö.

Tietojenkäsittelylaitteiden sijoittamisesta ja niiden läheisyydessä syömisestä ja juomisesta laaditaan ohjeistus. Ohjeistuksen laatimisesta vastaa IT-koordinaattori. Ohjeistuksen hyväksyy talouspäällikkö.

Yritys Oy:ssä ei ole seuraavaan vuoteen tai kahteen tulossa suurempia laitehankintoja. Päätelaitteita, kuten kannettavia tietokoneita ja matkapuhelimia hankitaan tarpeen mukaan.

7.8 **Tietoaineistoturvallisuus**

Tietojen säilyttäminen, varmistaminen, palauttaminen ja tuhoaminen sekä niihin liittyvät toimet kuuluvat tietoaineistoturvallisuuteen. Tietoaineistoihin kuulu-

vat sekä manuaalisen tietojenkäsittelyn asiakirjat, että automaattisen tietojenkäsittelyn tulosteet. (Hakala ym. 2006, 12.)

Tiedoille merkitään omistaja, joka vastaa tiedon luokituksesta, jakelusta ja käytöstä sekä määrittelee tietoturvavaatimukset. (Tietoaineistoturvallisuus. 2013.)

Luokittelussa voidaan käyttää esimerkiksi merkintöjä, yleinen, luottamuksellinen ja salainen. Nämä merkinnät määräävät osaltaan kuinka tiedot tulee käsitellä niiden elinkaaren aikana. Elinkaareen kuuluu esim. tallentaminen, välittäminen, arkistointi ja tuhoaminen.

Tässä työssä ei käsitelty tietoaineistoturvallisuuteen liittyviä asioita laajemmin Yritys Oy:n osalta.

7.9 **Käyttöturvallisuus**

Käyttöturvallisuuteen kuuluvat tietojärjestelmien ja verkkojen sisäänkirjautumisten valvonta, käyttäjien tunnistaminen ja todentaminen sekä käyttöoikeus määrittelyt. Käyttöoikeus määrittelyissä käytetään yleensä vähimmän valtuutuksen periaatetta, eli käyttäjälle annetaan vain oikeudet niihin verkon resursseihin mitkä hän tarvitsee. Lisäksi tietojärjestelmissä käytettävien salasanojen laatu on yksi tärkeä osa käyttöturvallisuutta. (Hautamäki 2011b, 24.)

Tässä työssä ei käsitelty käyttöturvallisuuteen liittyviä asioita laajemmin Yritys Oy:n osalta.

8 JATKUVUUSSUUNNITELMA

Jatkuvuussuunnitelman tarkoitus on turvata liiketoimintaprosessien toiminta sekä normaali- että häiriötilanteissa ja häiriötilanteiden jälkeen. Jatkuvuussuunnitelmaa tehdessä kannattaa huomioida myös normaalitoiminnan aikana tietojärjestelmille tehtävät erilaiset säännölliset huoltotoimenpiteet, joilla on merkittävä vaikutus toiminnan jatkuvuutta ajatellen. (Laaksonen ym. 2006, 227.)

Yritys Oy:llä jatkuvuussuunnitelmaa ei vielä ole, vaan se tehdään tietoturvasuunnitelman yhteydessä.

9 TOIPUMISSUUNNITELMA

Toipumissuunnitelman tarkoituksena on mahdollistaa yrityksen liiketoimintaprosessien mahdollisimman nopea toipuminen häiriötilanteista. Toipumissuunnitelma on jatkuvuussuunnitelman osa, joka sisältää ohjeet kuinka katastrofista toivutaan ja palataan mahdollisimman nopeasti normaali toiminnantilaan. Se sisältää määritelmät varajärjestelmille tärkeille tietojärjestelmille, vastuut ja toimet kuinka valmiudet luodaan. Lisäksi siitä löytyy ohjeet kuinka poikkeustilanteissa toimitaan. (Laaksonen ym. 2006, 227.)

Yritys Oy:llä ei toipumissuunnitelmaa vielä ole, vaan se tehdään tietoturvasuunnitelman yhteydessä.

10 HENKILÖSTÖN TIETOTURVAOHJEISTUS

Tietoturvaohjeiden tarkoitus on estää ongelmien syntyminen. Ohjeita tarvitaan yrityksen tietojärjestelmien jokapäiväiseen käyttöön, kuten tiedon käsittelyyn, Internetin ja sähköpostin käyttöön, vierailujen järjestämiseen, laitteiden ja järjestelmien käyttöön sekä toiminnan kuvaukseen väärinkäyttötilanteissa. Ongelmatilanteiden ja poikkeusolosuhteiden varalle on oltava myös ohjeet. Tietoturvaohjeistus luodaankin usein rinnan teknisen tietoturvan rakentamisen kanssa. (Laaksonen ym. 2006, 146.)

Tavallisesti tietoturvaoheistus koostuu yksittäisistä tiettyyn tarkoitukseen laaditusta ohjeista. Ohjeiden pohjalla tulee kuitenkin olla selkeä kuva siitä miksi ohjeita laaditaan. Hyvä tietoturvaohje vastaa myös kysymykseen, miksi jokin ohje on laadittu.

Yritys Oy:llä on henkilöstön tietoturvaohjeistus tehty muutama vuosi sitten. Tämän jälkeen on hankittu uusia ohjelmia sekä tietojärjestelmiä. Tietoturvaohjeistuksen päivitys tehdään Yritys Oy:ssä myöhemmässä vaiheessa.

11 IT-DOKUMENTAATIO

11.1 Yleistä

Tietoturvallisuutta edistämään ja ylläpitämään tarvitaan riittävän yksityiskohtainen dokumentointi, joka noudattaa yrityksessä sovittua rakennetta. Hyvä dokumentointi helpottaa tietojärjestelmien teknistä ylläpitoa tietojenkäsittelyä ja tietohallintoa. Usein dokumentointi laiminlyödään vedoten ajanpuutteeseen. Puutteellisen dokumentoinnin aiheuttama selvitystyö vie kuitenkin usein moninkertaisen ajan verrattuna varsinaisen dokumentin tekemiseen. (Hakala ym. 2006, 32.)

11.2 Mitä dokumentoidaan?

Tietoverkosta tulee löytyä ajantasainen dokumentaatio, josta löytyvät ainakin fyysinen arkkitehtuurikuva, joka kuvaa verkon fyysisen rakenteen eli kaapeloinnit ja verkon aktiivilaitteet. Lisäksi liitäntäpisteet ulkoisiin verkkoihin tulee olla selkeästi merkitty. Dokumentaatiosta tulee löytyä myös looginen arkkitehtuurikuva, joka kuvaa verkon loogisen rakenteen eli eri verkkoalueet ja mahdolliset virtuaaliverkot (VLAN). Myös verkon laitelista dokumentoidaan, jossa on määritelty vähintään kunkin laitteen osoitetiedot (MAC, IP), omistaja, fyysinen sijainti sekä käyttötarkoitus. (Vahti 2011, 20.)

Kaikki tietojärjestelmät, laitteet ja ohjelmistot tulee inventoida, ja kirjata niistä vähintään seuraavat tiedot:

- Omistaja / käyttäjä
- tekniset ominaisuudet, kuten prosessoriteho, muistin ja levytilan määrä
- IP-osoite
- fyysinen sijainti
- käyttötarkoitus. (Laaksonen ym. 2006, 223)

Ohjelmista kirjataan niiden omistaja ja käyttäjät sekä ohjelmistoversiot. (Laaksonen ym. 2006, 223)

11.3 **Dokumentaation nykytila yrityksessä**

Yksi Yritys Oy:ssä tietoturvaan vaikuttava tekijä oli yhtenäisen dokumentaation puute koskien tietoverkkoja, ohjelmistoja, laitteita ja sopimuksia. Osa tiedoista oli IT-tukihenkilön työaseman paikallisella kovalevyllä, osa palvelimen jaetulla verkkolevyllä ja osa oli dokumentoimatta kokonaan.

Tässä opinnäytetyössä keskityttiin luomaan ohjelmistojen, laitteiden, tietoverkkojen ja sopimuksien osalta yhtenäinen paikka näille dokumenteille.

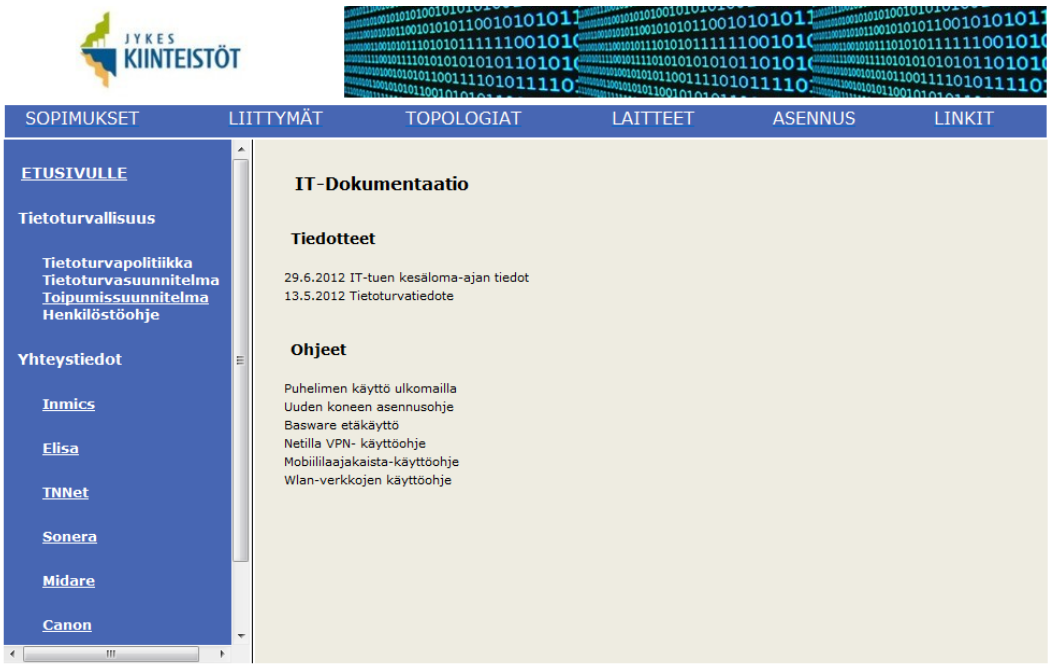
11.4 **Dokumentaatiojärjestelmä**

Dokumentaatio tullaan sijoittamaan Web-sivustona Yritys Oy:n tiedostopalvelimelle. Käyttöoikeus kyseisiin tiedostoihin tullaan rajaamaan IT-tuelle ja talouspäällikölle, sekä laitteisto-, tietoverkko- ja ohjelmistodokumentaation osalta myös alihankkijalle, joka toimittaa järjestelmäasiantuntijapalveluita yritykselle.

Web-sivusto toteutettiin HTML-koodilla. Sivusto toimii käyttöliittymänä eri dokumenteille. Jotta varsinaisia dokumentteja olisi kaikkien käyttäjien helppo päivittää, ovat ne Excel, Word, tai Visio tiedostoja, joihin käyttöliittymä sisältää linkit. Sopimukset ovat skannattuja Pdf-tiedostoja.

Järjestelmän alle tullaan siirtämään eri paikoissa hajallaan oleva dokumentaatio. Puuttuvaa dokumentaatiota lisätään matkan varrella.

Kuviossa 9 on kuvakaappaus dokumentaatiojärjestelmän pääsivusta.



Kuvio 7. IT-dokumentaatiojärjestelmä

12 POHDINTA

Työn tarkoituksena oli tehdä Yritys Oy:lle tietoturva- ja uhkakartoitus ja luoda yhtenäinen dokumentaatiojärjestelmä. Tietoturva- ja uhkakartoitusta lähdettiin tekemään tyhjästä. Yrityksellä ei ollut aikaisempia kartoituksia eikä tietoturvapolitiikkaa. Ensimmäiseksi tehtiin tietoturvapolitiikka. Politiikan luominen sujui suhteellisen helposti yhteistyössä yritysjohdon kanssa. Tietoturvapolitiikka onnistui mielestäni hyvin kuvaamaan yrityksen päämääriä tietoturvan suhteen.

Aiheen laajuuden vuoksi tietoturva- ja uhkakartoitus rajattiin tässä työssä koskemaan lopulta kolmea tietoturvallisuuden osa-aluetta, ohjelmisto-, laitteisto- ja tietoliikenneturvallisuutta. Työstä syntyi mielestäni hyvä alku ja kehys laajemmalle tietoturva- ja uhkakartoitukselle joka käsittää loputkin tietoturvallisuuden osa-alueista. Työtä voidaan jatkossa hyödyntää Yritys Oy:ssä tietoturvasuunnitelman tekemiseen. Työn edetessä ymmärsin konkreettisesti, että tietoturva- ja uhkakartoitus ei tule koskaan olemaan valmis dokumentti vaan sitä iteroidaan jatkuvasti. Tietojärjestelmiä hankitaan uusia ja uusia uhkia kehittyy jatkuvasti ja niitä vastaan tulee löytää suojautumiskeinot.

Itse olen työskennellyt Yritys Oy:ssä viimeiset kymmenen vuotta, joten yrityksen tuntemus ja tietojärjestelmien muuttuminen ja kehittyminen vuosien aikana on hyvin tiedossani. Yritys Oy:n tietojärjestelmien nykytilasta tiedon kerääminen oli melko helppoa. Vaikkakin dokumentaation puuttuminen tai hajanaisuus vaikeutti työtä.

Aineistoa tietoturvallisuudesta on saatavilla valtavasti, ja käytettävien lähteiden rajaaminen olikin ongelmallista. Lopulta päädyin lähteisiin ja standardeihin, jotka olivat mielestäni sopivia pienehkölle yritykselle ja sen liiketoimintaympäristöön. Tarkistuslistoista ja standardeista poimittiin edelleen Yritys Oy:lle sopivat osat. Standardit täydensivät hyvin toisiaan ja Vahti dokumentit olivat hyvä lähde. Näistä lähteistä keräämällä ja yhdistelemällä tietoa, sain riittävästi teoriatietoa ja ohjeistuksia tietoturva- ja uhkakartoituksen tekemiseen. Pitkäaikainen työskentely yrityksessä ja sen tietojärjestelmien tuntemus auttoivat käytettävän materiaalin valinnassa.

Työn edetessä oma tietämykseni tietoturvasta kasvoi. Ymmärsin myös kuinka tärkeää ajantasainen ja kattava dokumentaatio on kaikille tietojenkäsittelyn osa-alueille. Tietoturvan kerroksellisuuden merkitys tuli myös selkeästi esille. Materiaaleja tutkiessani huomasin, ettei voi luottaa vain yhteen suojausmenetelmään tai tasoon vaan tietoturvaa tulee rakentaa kerroksittain. Mikäli yksi taso pettää, on muita suojausmenetelmiä kuitenkin vielä olemassa.

Yksi työn tavoite oli yhtenäisen dokumentaatiojärjestelmän tekeminen Yritys Oy:lle. Dokumentaatiojärjestelmä toteutettiin Web-sivustona, joka sijoitetaan Yritys Oy:n palvelimelle. Dokumentaatiolle on nyt yhtenäinen paikka. Suurin työ sen osalta tulee olemaan dokumentoitavan tiedon kerääminen järjestelmään, mutta sen tekeminen jatkuu tämän opinnäytetyön jälkeen. Ongelmana dokumentaation suhteen oli jo työtä tehdessä se, että esimerkiksi kaapeloinnista ei kaikissa kiinteistöissä ole olemassa ajantasaisia kuvia. Kaapelointien ajantasaisen dokumentaation saaminen voi joistakin kiinteistöistä olla mahdotonta, jo kustannusten vuoksi.

Kaikin puolin tämä on ollut hyvin opettavainen projekti. Työn edetessä olen arvioinut uudelleen omia työmenetelmiäni tietoturvallisuuden kannalta, ja

huomannut kehittämisen aihetta erityisesti dokumentoinnin suhteen. Myös Henkilöstön ohjeistamisen ja kouluttamisen tärkeys tietoturvan suhteen on korostunut.

LÄHTEET

Active Directory.2013. Viitattu 13.2.2013. http://technet.microsoft.com/en-us/library/cc780036(WS.10).aspx#w2k3tr_ad_over_qbjd

EAPS-rengas, 2013. Viitattu 3.2.2013. http://en.wikipedia.org/wiki/Ethernet_Automatic_Protection_Switching

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo Finland Oy.

Hautamäki, J. 2011a. Tietoturva ja palveluiden hallinta -kurssi, tietoturvasuunnittelu, kurssimateriaali.

Hautamäki, J. 2011b. Tietoturva ja palveluiden hallinta -kurssi, yleistä tietoturvasta, kurssimateriaali.

Jyväskylän kaupungin karttapalvelu, 2012. Viitattu 15.8.2012. http://kartta.jkl.fi

Tietoturvaongelmat. 2012. Viitattu 13.2.2013, http://www.kpmg.com/FI/fi/Ajankohtaista/Uutisia-ja-julkaisuja/Neuvontapalvelut/Documents/KPMG-Tietoturvaraportti-2012.pdf

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

Mind map, 2012. Viitattu 7.10.2012. http://en.wikipedia.org/wiki/Mind_map.

Ohjelmistoturvallisuus, 2013. Viitattu 3.2.2013. https://www.vahtiohje.fi/web/guest/225

SFS-ISO/IEC 17799. 2005. Suomen Standardisoimisliitto, standardi.

SFS-ISO/IEC 27005. 2009. Suomen Standardisoimisliitto, standardi.

Tietoaineistoturvallisuus. 2013. Viitattu 3.2.2013. https://www.vahtiohje.fi/web/guest/226

Vahti. 2013. Sovelluskehityksen tietoturvaohje 1/2013

Vahti. 2009. The Government Information Security Management Board. 5/2009. Effective information security.

Vahti. 2011 Sisäverkko-ohje 3/2011

Windows Server Domain, 2013. Viitattu 13.2.2013. http://technet.microsoft.com/en-us/library/cc786438(WS.10).aspx

LIITTEET

Liite 1 Jykes Kiinteistöt Oy Tietoturvapolitiikka

Jykes Kiinteistöt Oy

Tietoturvapolitiikka

Versio 1.2
8.8.2012

SISÄLLYSLUETTELO

JOHDANTO

Jykes Kiinteistöt Oy:n liiketoiminta on riippuvainen toimivista tietojärjestelmistä ja tietoliikenneyhteyksistä. Tietojen saatavuus, eheys ja luottamuksellisuus ovat ensiarvoisen tärkeitä. Siksi Jykes Kiinteistöjen tietoturvapolitiikassa määritellään ne päämäärät, toimet ja vastuut, joilla liiketoiminnan jatkuvuus ja katkosten minimointi pyritään turvaamaan kaikissa olosuhteissa.

Jykes Kiinteistöt Oy:n tietoturvapolitiikassa määritellään lisäksi tietoturvallisuuteen liittyvä tiedottaminen ja kouluttaminen sekä ongelmatilanteiden käsittely.

Tietoturvapolitiikan lisäksi Jykes kiinteistöillä on tietoturvaohjeet henkilöstölle sekä tietoturvasuunnitelma, joissa kuvataan tarkemmin ne käytänteet ja tekniset menetelmät, joilla tietoturvaa pyritään ylläpitämään.

TIETOTURVAN PÄÄMÄÄRÄT

Jykes Kiinteistö Oy:n tietoturvan päämäärillä tarkoitetaan yrityksen hallussa olevien tietojen, järjestelmien ja palvelujen suojaamista yrityksen omien toimenpiteiden avulla. Tietoturvan tarkoituksena on varmistaa tietojärjestelmien kyky tukea liiketoimintaa sekä minimoida tietoturvaan liittyvien, ei toivottavien tapahtumien, liiketoiminnalle aiheuttamat vahingot ja keskeytykset.

Tavoitteena on hyvän tiedonhallintatavan toteuttaminen kaikissa Jykes Kiinteistöjen toiminnoissa, henkilöstön tietoturvaosaamisen ylläpitäminen ja kehittäminen sekä sitouttaminen tietoturvalliseen toimintaan ja tietoturvaohjeisiin.

Tietoturvallisuuden painopistealueet ovat järjestelmien käytettävyys, toimivat tietoliikenneyhteydet, tiedon eheys ja käytettävyys, luotettava käyttäjän tunnistus, käyttöoikeushallinta, tietoturvakoulutuksen järjestäminen ja ohjeistus sekä ulkopuolisten hyökkäyksien torjunta, roskapostin suodattaminen ja haittaohjelmien torjunta.

Tietoturvaperiaatteet perustuvat tietoturvan viiteen osatekijään:

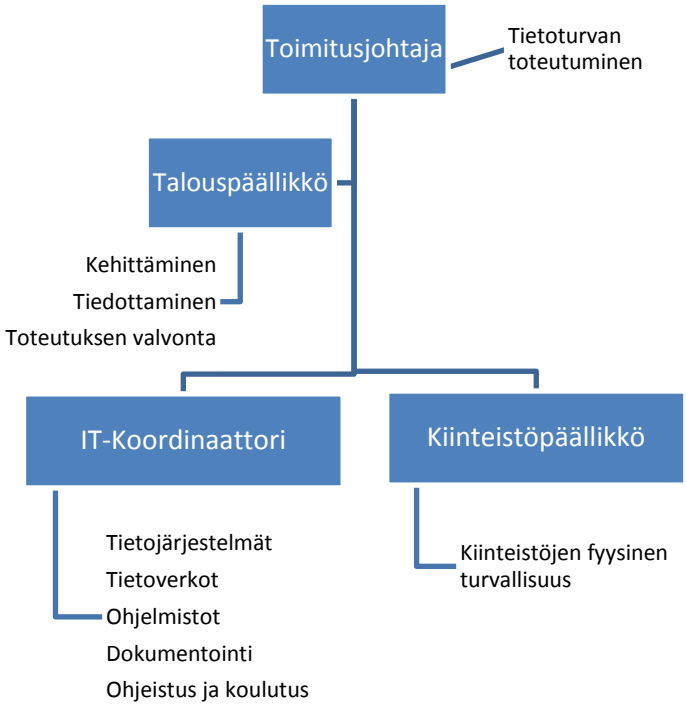
- **Luottamuksellisuus** eli yrityksen hallussa olevan tiedon ja arkaluontoisen informaation suojaaminen luvattomalta käytöltä, paljastumiselta ja salakuuntelulta
- **Eheys** eli tiedon oikeellisuuden, täydellisyyden ja muuttumattomuuden suojaaminen
- **Käytettävyys** eli tiedon ja tärkeiden palveluiden käytettävyyden varmistaminen. Käytettävyyden perusajatuksena on, että tiedot ovat oikeita ja ajantasaisia, ja ne ovat niiden käytettävissä, joilla on niihin oikeudet.
- **Kiistämättömyys** eli tietojärjestelmät kykenevät tunnistamaan ja tallentamaan luotettavasti järjestelmää käyttävän henkilön tiedot.
- **Pääsynvalvonta** eli ne menetelmät, joilla rajoitetaan tietojärjestelmien ja tietoliikenneyhteyksien käyttöä.

VASTUUT JA ORGANISOINTI

Jokainen Jykes Kiinteistöt Oy:n työntekijä vastaa osaltaan tietoturvan toteuttamisesta ja ylläpitämisestä sekä tietoturvaohjeiden noudattamisesta. Jokaisen vastuulla on noudattaa mm. seuraavia sääntöjä:

- Jykes Kiinteistöjen luottamuksellisia tietoja ei saa luovuttaa ulkopuolisille
- Jykes Kiinteistöjen tietojenkäsittelylaitteita tai salasanoja ei saa luovuttaa ulkopuolisille
- Jykes Kiinteistöjen tietojärjestelmistä ei saa luovuttaa tietoja ulkopuolisille
- Jokainen huolehtii osaltaan fyysisestä turvallisuudesta, mm. ovien lukitseminen
- Jokainen noudattaa tietoturvaohjetta ja huolellisuutta tietojen ja postien käsittelyssä.

Jykes Kiinteistöt Oy:n tietoturvan ylläpitoon on perustettu tietoturvaorganisaatio. Tietoturvaorganisaation tehtävä on kehittää ja ylläpitää Jykes kiinteistöt Oy:n tietoturvaa sekä huolehtia tietoturvaan liittyvästä tiedottamista ja koulutuksesta henkilöstölle. Tietoturvaorganisaatio koostuu seuraavista henkilöistä



Edelleen jokainen Jykes Kiinteistöt Oy:n palveluksessa oleva henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietoturvan vastuuhenkilölle.

TOTEUTTAMISKEINOT

Jykes Kiinteistöt Oy:ssä Tietoturvaa toteutetaan huolehtimalla:

- Hallinnollisesta turvallisuudesta, jolla tarkoitetaan Jykes Kiinteistöjen tietoturvapolitiikan ja turvallisuuden toteuttamiseksi laadittuja ohjeistoja.
- Fyysisestä turvallisuudesta, jolla tarkoitetaan rakenteellista turvallisuutta kuten ovien lukituksia ja tilojen valvontaa ja turvallisuutta.

- Henkilöstöturvallisuudesta, jolla tarkoitetaan henkilöstön liikkumiseen, matkustamiseen ja tunnistamiseen liittyviä seikkoja. Sekä henkilöstön yksityisyyden suojaan ja kouluttamiseen liittyviä seikkoja.

- Tietoaineistoturvallisuudesta, jolla tarkoitetaan Jykes Kiinteistöjen hallussa olevien tietojen käsittelysääntöjä koko niiden elinkaaren ajan, tallentamisesta tuhoamiseen.

- Käyttöturvallisuudesta, jolla tarkoitetaan järjestelmien käyttöön oikeuttavien tunnuksien hallintaa ja käyttäjien todentamista eri menetelmillä.

- Laitteistoturvallisuudesta, jolla tarkoitetaan laitteiden huoltoa, hallintaa ja dokumentointia.

- Ohjelmistoturvallisuudesta, jossa määritellään mitkä ohjelmat ovat sallittuja sekä niiden ylläpitoa ja varmuuskopiointia.

- Tietoliikenneturvallisuus, jolla tarkoitetaan lähi- ja laajaverkkoyhteyksien sekä muiden viestintäjärjestelmien turvallisuutta.

Verkon ja tietojärjestelmien tilaa valvotaan siihen tarkoitetuilla järjestelmillä. Palomuuri ja virustorjunta ratkaisut sekä ohjelmistot pidetään ajan tasalla. Tarkemmat tekniset menetelmät ja käytänteet edellä mainittuihin tietoturvan toteuttamiskeinoihin löytyvät Jykes Kiinteistöt Oy:n tietoturvasuunnitelmasta.

Tietoturvaa koskevan politiikan sekä siihen kohdistuvat muutokset hyväksyy yrityksen johto. Tietoturvaohjeet ja niitä koskevat muutokset hyväksyy tietoturvan vastuuhenkilö.

TIEDOTTAMINEN JA KOULUTUS

Jykes Kiinteistöt ylläpitää ja kehittää koko henkilöstön tietämystä ja osaamista tietoturvasta tiedottamalla ja kouluttamalla. Tietoturvan ylläpitoon ja kehittämiseen osallistuu koko henkilöstö.

Tietoturvallisuuden koulutuksesta ja tiedottamisesta vastaa tietoturvan työryhmä ja vastuuhenkilö.

SEURANTA JA ONGELMATILANTEET

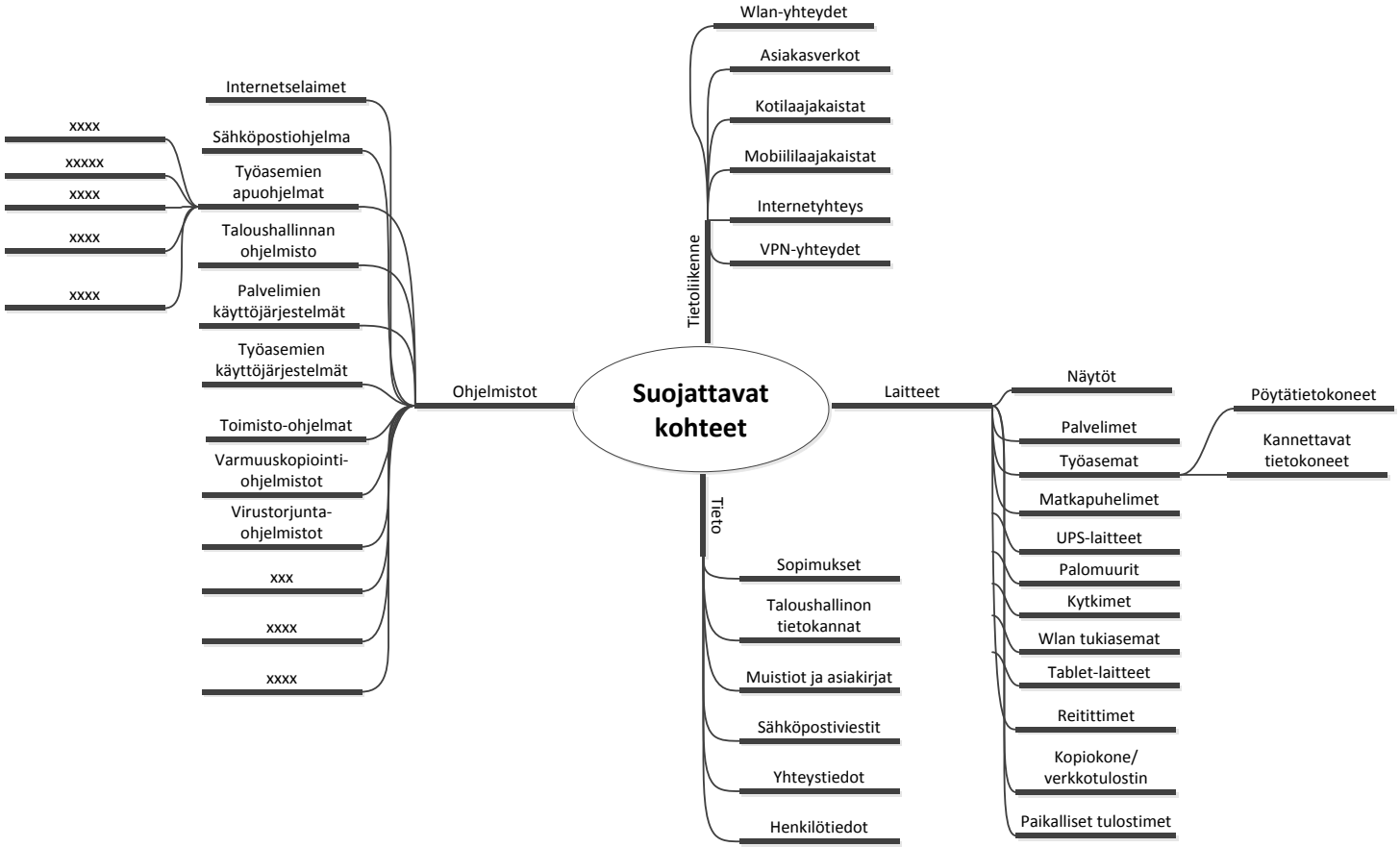
Tietoturva on osa Jykes Kiinteistöt Oy:n riskienhallintaa. Jykes Kiinteistöt seuraa tietoturvaan liittyvää alan kehitystä sekä hyödyntää uutta tietoa toiminnan kehittämiseksi.

Tietoturvan toteutuminen edellyttää tehokasta valvontaa ja ohjausta. Tietoturvaan liittyvästä valvonnasta vastaa yrityksen johto yhteistyössä tietoturvan vastuuhenkilön kanssa.

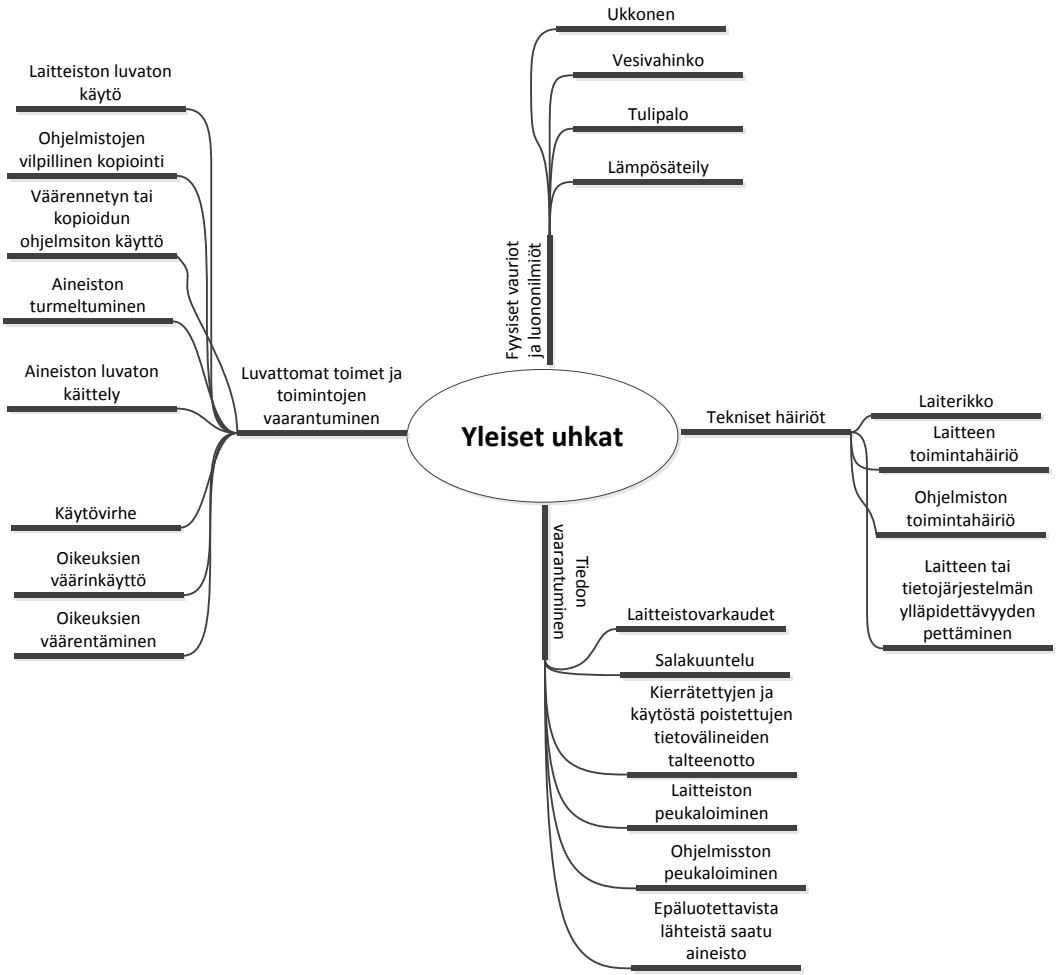
Jokainen Jykes Kiinteistöjen työntekijä on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietoturvan vastuuhenkilölle.

Kaikki tietoturvaan liittyvät väärinkäytökset ja epäkohdat raportoidaan tietoturvasta vastaavalle henkilölle. Yrityksen johto käsittelee tietoturvarikkomukset tapauskohtaisesti.

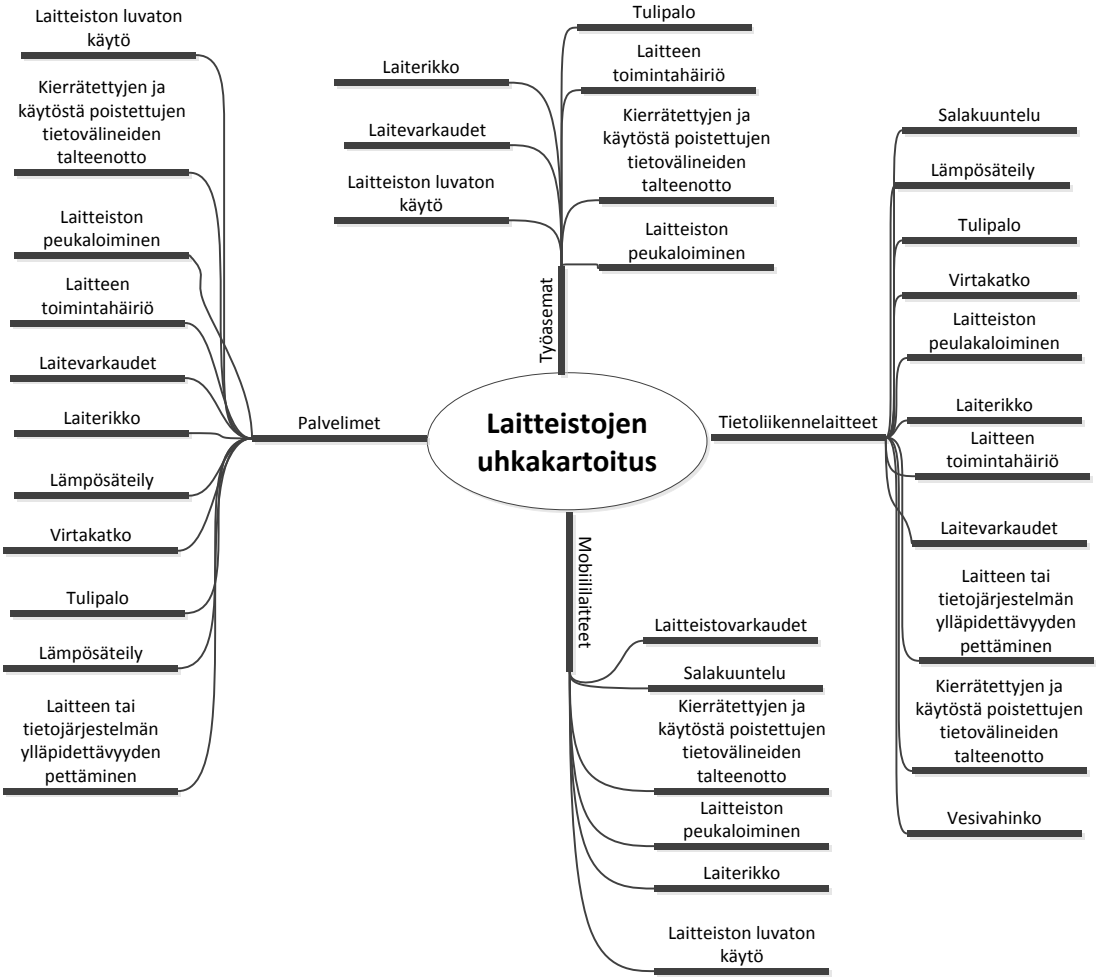
Liite 2 Miellekartta - Suojattavien kohteiden tunnistaminen


Suojattavat kohteet
Ohjelmistot
Internetselaimet
Sähköpostiohjelma
Työasemien apuohjelmat
xxxx
xxxxx
xxxx
xxxx
xxxx
Taloushallinnan ohjelmisto
Palvelimien käyttöjärjestelmät
Työasemien käyttöjärjestelmät
Toimisto-ohjelmat
Varmuuskopiointi-ohjelmistot
Virustorjunta-ohjelmistot
xxx
xxxx
xxxx
Tietoliikenne
Wlan-yhteydet
Asiakasverkot
Kotilaajakaistat
Mobiililaajakaistat
Internetyhteys
VPN-yhteydet
Tieto
Sopimukset
Taloushallinon tietokannat
Muistiot ja asiakirjat
Sähköpostiviestit
Yhteystiedot
Henkilötiedot
Laitteet
Näytöt
Palvelimet
Työasemat
Pöytätietokoneet
Kannettavat tietokoneet
Matkapuhelimet
UPS-laitteet
Palomuurit
Kytkimet
Wlan tukiasemat
Tablet-laitteet
Reitittimet
Kopiokone/ verkkotulostin
Paikalliset tulostimet

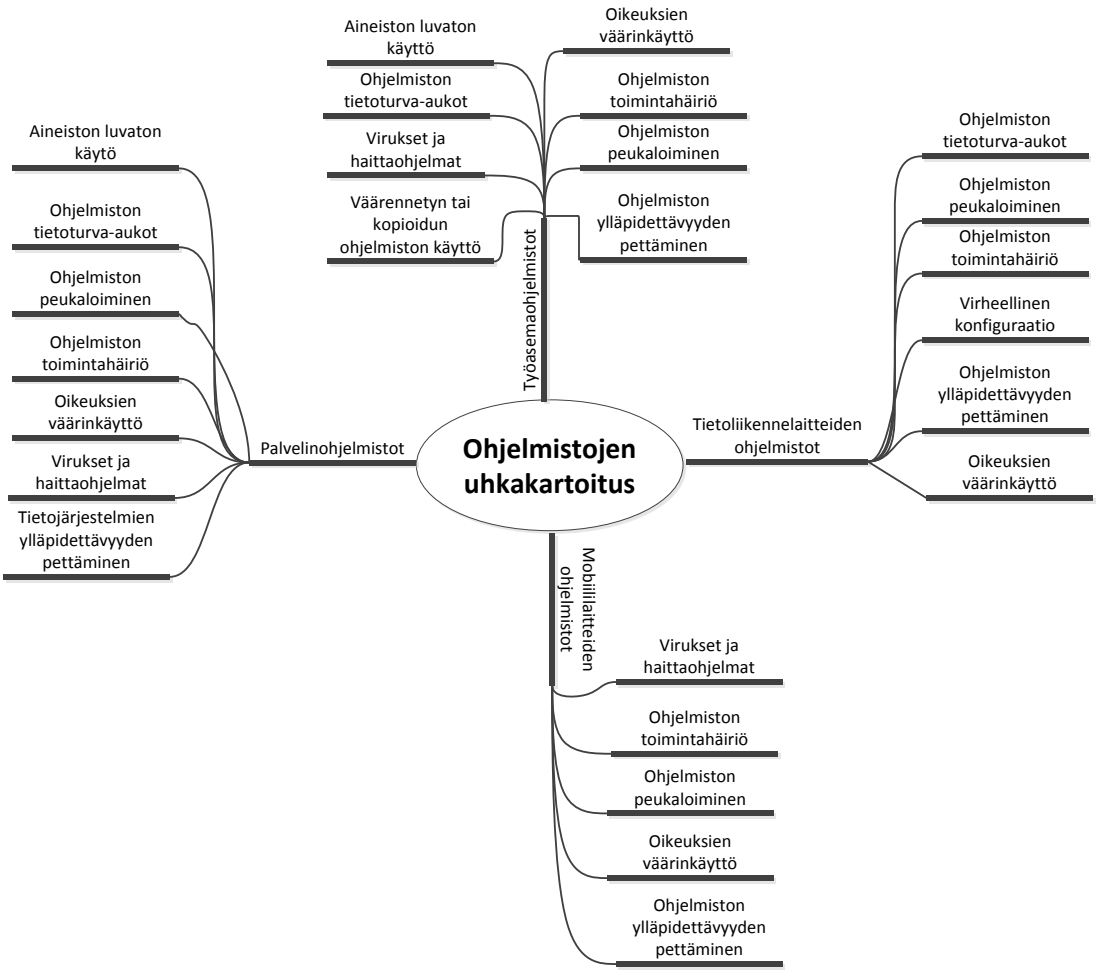
Liite 3 Miellekartta - yleiset uhkat



Liite 4 Miellekartta - laitteistojen uhkakartoitus



Liite 5 Miellekartta - Ohjelmistojen uhkakartoitus



Liite 6 Miellekartta - Tietoliikenneturvallisuuden uhkakartoitus