OULUN SEUDUN
AMMATTIKORKEAKOULU

Rauno Karvonen

TIETOTURVASUUNNITELMA

TIETOTURVASUUNNITELMA

Rauno Karvonen

Opinnäytetyö

Kevät 2013

Tietotekniikan koulutusohjelma

Oulun seudun ammattikorkeakoulu

ALKULAUSE

Tämä opinnäytetyö on tehty Oulun seudun ammattikorkeakoulussa, Raahen tekniikan ja talouden kampuksella 2012 helmikuun ja 2013 huhtikuun välisen aikana. Toimeksiantajana toimi Miilukangas Oy.

Ohjaavana opettajana toimi Lea Hannila. Työelämäohjaajana Miilukangas konsernista toimivat tietohallintopäällikkö Jari Kangasharju ja johtaja Jussi Miilukangas.

Kiitos Lea Hannilalle työn ohjauksesta sekä neuvoista. Kiitos Jari Kangasharjulle ja Jussi Miilukankaalle sekä muulle Miilukangas Oy:n henkilökunnalle opinnäytetyön aiheesta sekä työn edistämisestä.

Raahessa 30.4.2013

Karvonen Rauno

TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu
Tietotekniikan koulutusohjelma, Tietoturvatekniikka

Tekijä(t): Rauno Karvonen
Opinnäytetyön nimi: Tietoturvasuunnitelma
Työn ohjaaja(t): Lea Hannila
Työn valmistumislukukausi ja -vuosi: kevät 2013 Sivumäärä: 37+5 liitettä

Opinnäytetyön tavoitteena oli tehdä tietoturvapolitiikka ja tietoturvasuunnitelma Miilukangas Oy:lle. Koska yritys toimii maailmanlaajuisesti, on tietojen turvaamisesta tullut yhä tärkeämpää. Toinen tärkeä asia on, että yrityksellä ei ollut tätä asiakirjaa toimintakäsikirjan yhteydessä, joten he eivät voineet todentaa yhteistyökumppaneille ja kolmansille osapuolille sitä, että heidän toimintansa ovat ajan tasalla tietoriskien ja tietoturvallisuuden osa-alueella.

Opinnäytetyössä oli tarkoitus käydä kaikki tietoturvan osa-alueet läpi. Työssä kartoitettiin Miilukangas Oy:n senhetkisiä tietoturvatoimia ja mahdollisia puutteita. Puuteiden löytämiseksi käytettiin apuna syksyllä 2011 tehtyä tietoriskikartoitusta. Havaittujen puutteiden korjaamiseksi esitettiin tarvittavia korjaustoimenpiteitä.

Tietoturvapolitiikassa käsitellään tietoturvallisuutta yleisellä tasolla. Tietoturvasuunnitelmassa noudatetaan tietoturvapolitiikan linjauksia ja kuvataan yksityiskohtaisesti tietoturvaratkaisut ja kehittämisen tarpeet. Opinnäytetyölle asetetut tavoitteet täytettiin siinä laajuudessa kuin suunniteltiin. Miilukangas Oy sai tietoturvapolitiikan ja tietoturvasuunnitelman. Tämän opinnäytetyön tuloksena syntyneet dokumentit antavat Miilukangas Oy:lle hyvän työkalun ylläpitää ja kehittää tietoturvallisuuttaan. Tietoturvasuunnitelma ja tietoturvapolitiikka on syytä tarkistaa määräajoin ja tehdä muutoksia tarvittaessa.

Asiasanat:
tietoturvasuunnitelma, pienet ja keskisuuret yritykset, tietoturva, tietoturvapolitiikka

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology

Author:Rauno Karvonen
Title of thesis: Information security plan
Supervisor: Lea Hannila
Term and year of completion: spring 2013 Number of pages: 37+5 appendix

The aim of this Bachelor's thesis was to create an information security plan and an information security policy to Miilukangas Oy. For the company operating worldwide, the security information is increasingly important. In addition to this, the company did not previously have this kind of documentation to prove their partners in cooperation and the third party that their action is up-to-date in relation to data security and information security.

In this thesis it was meant to look through all the fields of information security. To find Miilukangas Oy's potential shortages in information security, I executed an information security risk survey in 2011. The observed findings of that study were presented as demand for repairs and they gave me the basis to this thesis.

The information security policy deals with the information security commonly. The information security plan follows the information security policy and it describes a full account of the information security solution and it informs the needs of development. The target of this thesis was fulfilled. Miilukangas Oy got the security policy and the information security plan. These documents give a useful tool to maintain their information security. The information security plan and information policy should be periodically inspected and updated when needed.

Keywords: information security, small and medium-size enterprises, information security plan, data security risk

SISÄLLYS

1 JOHDANTO

1.1 Yrityksen historia

Vuonna 1967 Anja ja Erkki Miilukangas perustivat Saloisten Putkiliike Miilukangas & kumpp., joka toimi alkuaikoina LVI-alalla. Vähitellen toiminta laajeni pieniin teräsrakenteisiin ja talonrakennushakualalle. 1970–luvun lopulla yritys rakensi oman konepajan. Vuonna 1983 yritysmuoto muutettiin ja nimi vaihtui Miilukangas Ky:ksi. (Miilukangas Ky kotisivu, hakupäivä 24.4.2012.)

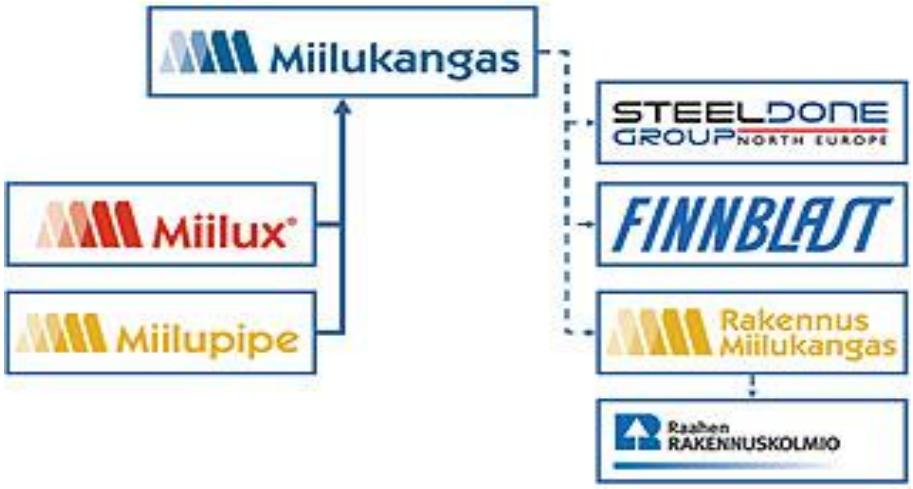
Tässä vaiheessa toiminta oli konepaja-, asennus- ja rakennustyötä. Vuonna 1987 yritys osti Kone Oy:n konepajatilat Raahesta. Putkipinnoitustehtaan toiminta käynnistettiin Pattijoella vuonna 1993 ja karkaisulaitos aloitti toimintansa Raahessa vuonna 2000. Tänään perheyrityksen tilauskonepaja toimintaa harjoittaa konsernin emoyhtiö Miilukangas Oy, kulutusteräsliiketoimintaa Miilux Oy ja virtausputkiliiketoimintaa sekä sopimusvalmistusta Miilupipe Oy. Vuonna 2011 konsernin liikevaihto oli noin 32 milj. euroa ja tase noin 25 milj. euroa. Henkilöstöä näissä yhtiöissä on n. 180. Vuonna 2013 yrityksen yritysmuoto muuttui osakeyhtiöksi, joka on nyt Miilukangas Oy. Saman vuoden maaliskuussa yrityksen konepajaliiketoiminta hajautettiin kahdeksi itsenäiseksi osakeyhtiöksi, jotka ovat Miilumachine Oy ja Miiluweld Oy. Miilumachine Oy harjoittaa koneistus- ja asennusliiketoimintaa ja Miiluweld Oy hitsaus- ja osanvalmistusliiketoimintaa. (Miilukangas Ky kotisivu, hakupäivä 24.4.2012.)

Tänä päivänä Miilukangas Oy on yksi merkittävimmistä työllistäjistä Raahen talousalueella. Miilukankaan laaja toiminta näkyy monella tapaa Raahessa ja sen ympäristökunnissa. Historian saatossa Miilukangas Ky on rakentanut useita näkyviä kohteita, kuten esimerkiksi Pattijoen vesitorni, Kauneuskanavan 2. silta, Pyhäjoen seurakuntatalo (pääurakoitsija) sekä monet muut kunnallisen puolen rakennushankkeet ja peruskorjaukset.

1.2 Miilukangas konserni

Miilukangas Oy on konserni, jossa tilauskonepajatoimintaa harjoittaa konsernin emoyhtiö Miilukangas Oy (kuva 1). Yhtiö on Suomen suurimpia tilauskonepajoja. Siltanostureiden suurin nostokorkeus on 10 metriä ja nostokyky 100 tonnia. Asiakkaina on suomalaisia ja kansainvälisiä teollisuus-

yrityksiä, insinööritoimistoja, teollisuuden palveluyrityksiä sekä kone- ja laitevalmistajia. Yritys toteuttaa valmistuksen asiakkaan piirustusten mukaisesti. Tarvittaessa käytetään suunnittelussa yhteistyökumppaneita. (Miilukangas Ky kotisivu, hakupäivä 24.4.2012.)



KUVA 1. Konsernikaavio (Miilukangas Ky kotisivu, hakupäivä 24.4.2012.)

Miilukangas Oy on osakkaana Rakennus Miilukangas Oy:ssä, suihkupuhallusteknologiaan erikoistuneessa revonlahtisessa yrityksessä Finnblast Oy:ssä ja konepajojen vientiyhtiössä, Oy Steel-Done Group Ltd:ssä. Miilukangas Oy:n konserni ja osakkuusyhtiöt työllistävät suoraan noin 270 työntekijää ja yhtiöiden yhteinen liikevaihto on n. 50 miljoonaa euroa. (Miilukangas Ky kotisivu, hakupäivä 24.4.2012.)

Miilux Kulutusteräskeskus palvelee metalli-, kaivos- ja kiviteollisuuden sekä maanrakentamisen ja koneenrakennuksen yrityksiä Suomessa ja ulkomailla. Vahvuuksia ovat asiakaslähtöinen toimintatapa, korkealaatuiset tuotteet, nopeat ja varmat toimitukset oman varaston ansiosta sekä ammattitaitoinen henkilökunta. Tuotantotilat sijaitsevat Raahessa, hyvien meri- ja maantieyhteyksien päässä. Yritys kasvaa voimakkaasti ja kehittää jatkuvasti toimintaa vastaamaan asiakkaiden tarpeita nyt ja tulevaisuudessa. (Miilux Oy kotisivu, hakupäivä 7.4.2013.)

Miilupipe Oy:n liiketoiminta on runkovesijohtoputkien sisäpuolista betonointia, putkilinjojen osien valmistusta sekä tilauskonepajatoimintaa. Toimitukset suuntautuvat Norjaan, Ruotsiin ja Suomeen. (Miilupipe Oy kotisivu, hakupäivä 7.4.2013.)

1.3 Konsernin tuotteita

Konepajan vahvaa aluetta ovat vaativat koneistukset ja teräsrakennetyöt sekä suuret ja painavat rakenteet. Yritys pintakäsittelee kaikki tuotteet nykyaikaisessa pintakäsittelylaitoksessa. Yritys tekee tuotteet asiakkaan tarpeiden mukaisesti kokoonpantuihin ja asennusvalmiisiin kokonaisuuksiin, jotka koeajetaan tarvittaessa konepajalla. (Miilukangas Ky kotisivu, hakupäivä 24.4.2012.)

Miiluxin päätuotantoa on erilaiset kulutusteräsosat ja komponentit maanrakennusalalla, kuten kauhakuormaajan huulilevyt, kuorma-autojen lavojen pohjalevyt ym. missä tarvitaan hyvää kulutuskestävyyttä. Miilux Protection -suojausteräkset ovat laadukkaita suomalaisia suojausteräksiä vaativiin käyttökohteisiin. Miilux Protection -suojausteräkset on testattu muun muassa PM2000-, EN1522-, Stanag 4569- ja MIL-A-46100D-normien mukaan. (Miilux Oy suojausteräkset, hakupäivä 7.4.2013.)

Putkien pinnoitus ja osien valmistus perustuu yhteistyösopimukseen, jossa Rautaruukki Oyj hoitaa markkinoinnin, myynnin ja Miilupipe Oy tuotteiden valmistuksen. Yritys pinnoittaa Ruukki Metals kierresaumaputkia sisäpuolisella ruiskubetonoinnilla. Yritys valmistaa käyrät, t-osat yms. siten, että asiakas saa kaikki putkilinjaansa tarvitsemansa osat mahdollisimman pitkälle jalostettuna. (Miilupipe Oy toiminta-ajatus, hakupäivä 24.4.2012.)

1.4 Miilukankaan laatutyö

Miilukankaan vahvan kasvun taustalla on dynaamisen ja osaavan henkilöstön koulutus sekä määrätietoinen pyrkimys vahvaksi osaajaksi omalla toimialallaan. Toimiessaan kansainvälisillä ja kotimaisilla runsaasti kilpailutetuilla markkinoilla yritys on joutunut kehittämään omia vahvuuksiaan. Miilukankaan eräs kilpailukeino näillä markkinoilla on vahva laatutyö, joka perustuu sertifioituun toimintajärjestelmään. Toimintajärjestelmään kuuluvat laatujärjestelmä ISO 9001, ympäristöjärjestelmä ISO 14001 ja turvallisuusjärjestelmä OHSAS 18001. Nämä ansaitut sertifikaatit helpottavat yrityksen toimintaa erityisesti kansainvälisillä markkinoilla. Raahen seutukuntaan mahdollisesti rakennettava ydinvoimala ja jatkuvasti kasvava kaivostoiminta pakottavat yritystä kehittämään omaa toimintaansa. Eräs laatutyön tärkeimmistä piirteistä on jatkuva kehittyminen jokaisella osa-alueella. Näistä yksi osa-alue on tietoturvallisuus ja siihen liittyvät riskit. Tietoturvallisuus on noussut yhä tärkeämmäksi kehittämisen kohteeksi yrityksessä, joka kilpailee vaativilla markkinoilla. Tietoturvaohjelmalla ja laatujärjestelmällä on monia yhtymäkohtia, laadusta vastaa koko organisaatio ja niillä pyritään vähentämään henkilöistä, toimintatavoista, koneista ja laitteista aiheutuvia virheitä tai poikkeamia. (Laaksonen, Nevasalo & Tomula 2006, 112.)

1.5 Tietoriskikartoitus

Tein Miilukangas konserniin tietojärjestelmien tietoriskikartoituksen syksyllä 2011. Tietoriskikartoituksessa ilmenneiden tietoriskien johdosta yrityksen johto ja IT-palvelut katsoivat tarpeelliseksi tehdä yritykselle tietoturvapolitiikan ja tietoturvasuunnitelman sekä mahdolliset muutokset laatukäsikirjaan. Tietoturvalla tai tietoturvallisuudella tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista tarkoituksenmukaisella tavalla. Kartoituksessa käytiin läpi koko konsernin kaikki organisaatiotasot ylemmästä johdosta työntekijöihin. Tällä keinolla saatiin kokonaiskuva yhtiön työntekijöiden ja johdon tietoturvallisuudesta sekä mahdollisista tietoriskeistä.

2 MÄÄRITELMÄ

Tämän opinnäytetyön tarkoituksena on luoda Miilukangas konsernille tietoturvapolitiikka ja tietoturvasuunnitelma. Näiden lisäksi yrityksen toimintakäsikirjaan joudutaan tekemään muutoksia ja lisäyksiä. Tietoturvapolitiikan ja tietoturvasuunnitelman luomisessa tutustutaan yrityksen IT-palveluihin, tietojärjestelmiin ja toimintaan.

Tässä työssä on suurena apuna ollut syksyllä 2011 tekemäni tietoriskikartoitus. Tietoriskikartoituksessa ilmenneiden puutteiden ja haluttujen kehittämistoimien pohjalta voidaan laatia tietoturvasuunnitelma, kuitenkin rakentaen tietoturvallisuutta kokonaisuutena. Tietoturvasuunnitelmassa kerrotaan kuinka puutteet korjataan sekä käytössä olevat hyvät käytänteet ja menettelyohjeet, jotka kirjataan myös tietoturvapolitiikkaan. Koska yrityksellä on toimintakäsikirja, jonka mukaan tuotanto ja koko organisaatio toimii, niin on hyvä, että tietoturvatyön tuomat muutokset kirjataan myös toimintakäsikirjaan.

2.1 Tietoturvapolitiikka

Osana tätä opinnäytetyötä on laatia Miilukangas konsernille tietoturvapolitiikka, esitellä ja hyväksyttää se yritysjohdolla ja julkaista se. Tietoturvapolitiikka on Miilukankaan johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot yrityksessä. Tietoturvapolitiikassa luodaan toimintatavat ja kehykset, joiden puitteissa yritys tekee tietoturvatyötä. Tietoturvapolitiikassa tuodaan esille tavoitteet, roolit ja vastuut, tietoturvallisuuskoulutus, tietojenkäsittelyn suojaaminen ja seuraukset tietoturvapolitiikan laiminlyönneistä. (Laaksonen, ym. 2006, 147.) Tietoturvapolitiikka on jatkuva tahtotila, jota on tarkoituksenmukaista päivittää ja tarkastaa määräajoin.

Tavoitteilla määritellään, mitä asioita ja tietoja tulisi turvata. Rooleissa ja vastuissa määritellään tahot, jotka vastaavat asetetuista tavoitteista ja toimista niiden saavuttamiseksi sekä siitä, ketä kaikkia tietoturvan toteuttaminen koskee. Toteutuksella määritellään ne keinot, joilla saavutetaan asetetut tavoitteet ja päämäärät sekä tietoturvallisuustyön ylläpito ja kehittäminen. Tietoturvapolitiikassa määritellään, kuinka toimitaan ongelmatilanteissa ja kenelle ilmoitetaan tietoturvallisuuspuutteista. Tietoturvapolitiikassa on myös määritelty ne toimet, joita tarvitaan, kun rikotaan tietoturvallisuutta.

2.2 Tietoturvasuunnitelma

Tietoturvasuunnitelma rakennetaan tietoturvapolitiikassa määritettyjen tavoitteiden, vastuiden ja toteutuskeinojen pohjalta. Tietoturvasuunnitelmassa käydään yksityiskohtaisesti läpi tietoturvapolitiikan määrittämät tavoitteet ja päämäärät sekä esitetään ne keinot, joilla voidaan ylläpitää ja turvallisuudessa, joka käy ilmi hyvin tietoriskikartoituksesta. Tietoriskikartoituksessa havaittuja riskejä ja puutteita lähdetään korjaamaan tietoturvasuunnitelmalla. Tietoturvasuunnitelmassa käsitellään ainoastaan tietoturva-asioita ja se on tarkoitettu IT-palveluiden käyttöön.

2.3 Toimintakäsikirja

Yrityksen toimintakäsikirjan muutoksia tehdään sen mukaan, kun niitä on tarpeellista tehdä. Toimintakäsikirjan muutokset on tarkoituksenmukaista toteuttaa yhdellä kertaa sitten, kun on selvinnyt, mitä muutoksia täytyy tehdä. Tietoturvapolitiikan ja tietoturvasuunnitelman tuomat muutokset ja lisäykset toimintakäsikirjaan tehdään yhdessä yrityksen laatupäällikön kanssa. Nämä laatutyöhön tulevat muutokset koskevat koko yritystä ja ovat helposti siirrettävissä myös tytäryhtiöihin.

3 TOIMINTAYMPÄRISTÖ

Miilukangas konserni koostuu useasta yrityksestä. Yrityksen tilat sijaitsevat useassa pisteessä Raahen kaupungin alueella. Päätoimipiste sijaitsee Ruonankatu 1:ssä. Toimitilojen moninaisuus on haaste tietojärjestelmille, koska rakennus on osittain rakennettu ennen sotia 1917. Yrityksen toimitiloja on laajennettu vuosien saatossa monta kertaa. Viimeisin laajennus on tehty 2011. Kokonaispinta-ala on noin 25 000 m².

3.1 Organisaation johtaminen ja sidosryhmät

Yritystä johtaa toimitusjohtaja kolmen johtoryhmän jäsenen kanssa. Johtoryhmä on tietoinen tietoriskeistä, mutta ei ole perehtynyt niiden yksityiskohtiin. Yrityksen johto on sitoutunut parantamaan omaa toimintaansa tietoturvallisuuden osalta.

Nykyaikaisen yrityksen tietotekniikan tarpeet ovat aivan eri mittakaavassa kuin 10 vuotta sitten. Henkilöstöllä on suuri merkitys työn tekemisessä tietokoneilla ja tietojärjestelmillä. Nämä alati kehittyvät sovellukset ja vaatimukset työntekijöiden tarpeissa tulee ottaa huomioon mietittäessä yrityksen toimintaa ja henkilöstön koulutusta ja ohjeistusta. Henkilöstölle ei ole järjestetty koulutusta nykyaikaisen yrityksen tietojärjestelmien turvalliseen ja riskittömään käyttöön. Työntekijöitä ei ole ohjeistettu, kuinka paljon he voivat puhua työaikanaan tekemästään työstä, eikä työntekijöiltä vaadita salassapitovelvollisuutta. Yrityksellä ei ole määritelty tarkasti tietoturvaperiaatteita, joiden mukaan työntekijöiden tulisi toimia.

Uusia työtekijöitä palkattaessa heidän taustansa selvitetään siinä laajuudessa kuin on tarpeellista. Tämä menettely on yleisessä käytössä yritysmaailmassa. Näin pystytään karsimaan osa mahdollisesti tulevista tietoriskeistä. Työntekijöitä perehdytettäessä heille ei kerrota tietoturvaan liittyvistä asioista. Esimiehillä on tieto siitä, milloin työntekijän työsuhde päättyy yrityksessä ja milloin hän luovuttaa varusteensa, mutta työntekijältä ei kerätä pois hänen saamiaan työ- ja tallennusvälineitä eikä tietomateriaaleja. Työsuhteen päättymiselle ei ole luotu menettelytapoja tietoturvallisuuden kannalta. Riitaisten työsuhteiden purkamisiin yrityksessä ei ole erikseen luotu ohjetta.

Yrityksen käyttäjätunnukset ovat jaettu kahteen ryhmään: henkilökohtaisiin tunnuksiin ja ryhmätunnuksiin. Henkilökohtaisia tunnuksia käyttävät pääsääntöisesti toimihenkilöt, jolloin he kirjautuvat

omana itsenään järjestelmään. Toisinaan tulee tilanteita, että jotkin sovellukset ovat käytössä vain erikseen nimetyillä henkilöillä, josta seuraa ongelmia varsinkin lomien aikaan. Ryhmätunnuksien käyttäjät kirjautuvat järjestelmään ryhmätunnuksilla, joilla käynnistetään tuotannon ohjaussovellus. Jokaisella työntekijällä ei ole omaa käyttäjätunnusta eikä salasanaa. Nykyinen salasanan muodostaminen on monien mielestä tullut riittämättömäksi.

Yrityksen sidosryhmiä ovat suuret metalliteollisuuden asiakkaat, tavarantoimittajat ja kunnat, ja näiden lisäksi on erilaisia palveluntarjoajia. Yrityksellä on myös monia muita sidosryhmiä eikä vain tuotteisiin liittyviä asiakkaita. Palveluntarjoajat ovat vakiintuneita toimittajia yritykselle. Uusien toimittajien kanssa ei ole selviä pelisääntöjä. Palveluita tarjoavia yrityksiä on paljon, joista muutamia alla:

- PPO tietoliikenne- ja tietojärjestelmäpalvelut
- Logica tuotannonohjausjärjestelmä
- Jydacom taloushallinto (Rakennuskolmio)
- Arrow kunnossapito-ohjelma
- Rescom tilausten tiedot Miilux
- Datakolmio Miilux tuotantosovellus
- Raahen turvallisuusvartiointi vartiointi ja kulunvalvonta.

Yrityksen liiketoimintastrategiassa on määritelty ns. TOPTEN-yritykset, jossa asiakkaat on luokiteltu tärkeisiin asiakkaisiin. Heidän kanssaan on luotu yhteistyökuviot liike- ja yhteistyötoiminnassa. Yritysten valinnassa ei ole painoarvo ollut tietoriskien hallinnan menettelyissä tai tietoriskikäytännöissä. Yrityksen oma tietoturvapolitiikan puuttuminen näkyy myös sidosryhmäasioita käsitellessä. Sidosryhmien tietoturvapolitiikkaa ei ole kyselty eikä heidän toimintaansa tietoriskien osalta. Eri liikekumppanien tietoturvallisuustoimintaa ei ole tarkasteltu. Kaikkien palveluntarjoajien ja yhteistyökumppanien kanssa ei ole sovittu yhteisistä käytännöistä, kuten esimerkiksi turvakäytännöistä, toimintaperiaatteista häiriötilanteissa tai toimenpiteistä, kun yhteistyö päättyy. Näistä sidosryhmistä monesti jäävät nuo edellä luetellut toimenpiteet huomioimatta. Kaikkien osapuolien kanssa ei ole sovittu tietoturvaperiaatteista.

3.2 Toimitilat

Miilukangas konsernin kiinteistöjä on eri puolella Raahen kaupunkia kaikkiaan viidessä toimipisteessä. Näiden lisäksi yrityksellä on virkistys- ja koulutuskeskus Fantissa sekä rakennuskohteita erinäinen määrä.

Kiinteistössä on osittainen kulunvalvonta, sillä toimihenkilöillä on vain kulunvalvontakortit ja samoin Miiluxin kaikilla työntekijöillä. Kulunvalvontakortilla pääsee yrityksen niihin tiloihin, joihin kulkukortin omistajalla on pääsyoikeus. Muilla työntekijöillä ei ole kulunvalvontakortteja.

Yrityksen kaikkia tehdaskiinteistöjä vartioi yöaikaan Raahen turvallisuusvartiointi. Yrityksen kiinteistöissä on kattava kameravalvonta. Valvontakamerajärjestelmä kattaa kaikkien kiinteistöiden yleiset piha-alueet ja yleiset sisätilat. Turvakameroiden tallenteita voidaan tutkia noin kolme viikkoa taaksepäin. Yrityksen kaikissa toimistorakennuksissa on varashälytysjärjestelmä, joka on päällä öiseen aikaan. Järjestelmä hälyttää ainoastaan näistä tiloista vartiointiliikkeeseen.

Avaintenhallinta on järjestetty asianmukaisesti kuten kulkukortitkin. Avaimia annetaan ainoastaan niille henkilöille, jotka niitä tarvitsevat työssään. Kulkuoikeuksien myöntämiselle tulisi olla nimetty henkilö, jolle tämä kuuluu.

Asiakkaiden palvelutilat ja neuvotteluhuoneet on sijoitettu valvottuihin tiloihin. Neuvottelutilat on äänieristetty ja osittain näköeristetty. Yrityksen tuotantotilat ovat myös ”asiakastiloja” ja näissä asia ei ole hoidettu yhtä hyvin kuin esimerkiksi neuvottelutiloissa. Yrityksen asiakkaitten töihin liittyvät piirustukset ovat työpisteessä ja työnjohtotiloissa. Yrityksessä on muuten hyvin hoidettu asiakirjojen hallinta, joka ei kuitenkaan toimi silloin, kun ollaan hallin puolella. Piirustukset ja työhön liittyvät työohjeet ovat myös esillä, jolloin kuka tahansa ulkopuolinen voi nähdä piirustukset ja työohjeet.

3.3 Tietojärjestelmät ja ohjelmistot

Kaikki nämä toimipisteet ovat samassa verkossa, mutta omissa VLANeissa (liite 1). Yrityksen verkko on jaettu kahteen siirtotekniikkaan, Ethernet- ja WLAN-verkkoon. Miilukankaalla on myös paljon erilaisia palvelinsovelluksia (liite 2). Turvakameratallenninpalvelin on tällä hetkellä yrityksen omissa tiloissa.

Miilukankaan ethernet-verkko on rakennettu toimintavarmuutta silmällä pitäen. Verkossa on käytetty kahta eri verkkotopologiaa. Verkkotopologialla tarkoitetaan tietokoneverkon tapaa, jolla verkon laitteet ovat liitetty toisiinsa. Monimuotokuituverkko toimii rengastopologian mukaan ja nämä kuiturenkaat ovat tähtitopologian mukaan yhteydessä toisiinsa. Monimuotokuituverkot on uusittu osittain kesällä 2011, jolloin päivitettiin kaikki kytkimet vastaamaan nykypäivän tietoliikennetarpeita. Samassa yhteydessä yritykseen asennettiin Ciscon WLAN-verkko. WLAN-verkossa on yhteensä 17 accesspointia eli liityntäpistettä, jotka kattavat koko tehdasalueen (liite 3). WLAN-verkkoa käytetään tuotannon ohjauksen sovelluksiin. Tietokoneita yrityksessä on kaikkiaan noin 150, tuotannossa on noin 40 kappaletta ja loput ovat henkilökohtaisia työkoneita. Näiden lisäksi on paljon älypuhelimia myynti- ja johtohenkilöstön käytössä.

Yrityksen tärkeät palvelin- ja varmuuskopiointitoimet on siirretty Pohjanmaan Puhelinosuuskunnan tiloihin Ylivieskaan. Muut tietojärjestelmälaitteistot on sijoiteltu niin, että ne ovat suojassa epäpuhtauksilta joko omassa laitekaapissa tai teknisessä tilassa. Näihin tiloihin on järjestetty asianmukainen ilmanvaihto, jolla pyritään pitämään laitteisto puhtaana ja viileänä. Paloilmoitinjärjestelmä on tällä hetkellä toimistotiloissa ja näiden yhteydessä olevissa teknisissä tiloissa.

Palvelinsovelluksia on monenlaisia, kuten kirjautumispalvelimet, tulostinpalvelimet, tiedostopalvelimet, varmuuskopiointi, Fsecure Policy Manager 10 ja WSUS (päivityspalvelimet), tietokantapalvelimet, työajanseuranta, postipalvelimet ym. Muutamasta palvelimesta kerron tarkemmin: AD1 on päivityspalvelin, jolla jaetaan Windows-päivitykset ja viruspäivitykset. AD2 on tulostinpalvelin, jolla jaetaan yrityksen kaikki verkkotulostimet. Sovelluspalvelin on tuotannonohjauksen palvelin. Kirjautumispalvelimet Terminal2 ja termsrv1 huolehtivat etätyöpöytien kirjautumiset yrityksen verkkoon.

Yrityksen ohjelmistohankinnat suoritetaan ainoastaan luotettaviksi havaituilta yrityksiltä. Yrityksen kaikki ohjelmistot eivät ole lisensoituja, vaan seassa on myös niin sanottuja freeware-ohjelmia.

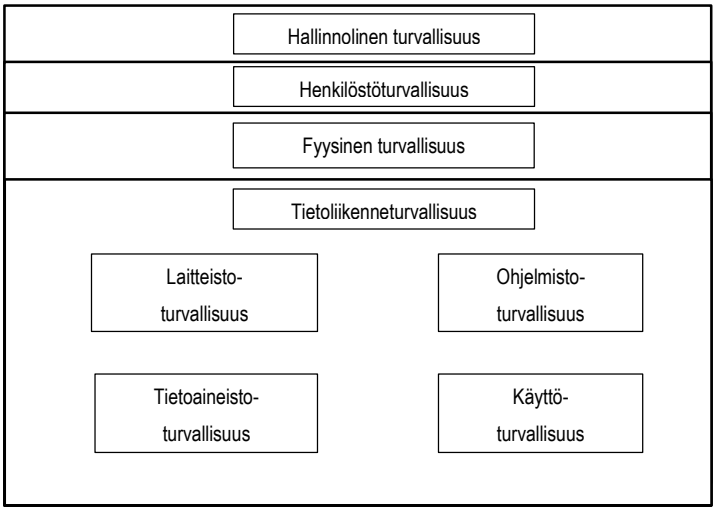
Niillä, joissa on lisenssi, kuten Autocad- ja Windows-ohjelmat, asia on kunnossa. Microsoftin tuotteista ei ole tarkkaa tietoa lisenssien lukumäärästä, paitsi palvelinlisenssit, jotka ovat kunnossa. Työasemakoneiden mukana tulleista OEM-lisensseistä ei ole tiedossa tarkkaa lukumäärää.

Tuotannonohjaussovellus (V10) on käytössä Miilukangas Ky:ssä, Miilux Oy:ssä ja Miilupipe Oy:ssä. Viimeksi mainitussa se on otettu käyttöön 2011. Miiluxilla V10 on käytössä palkanlaskennassa ja taloushallinnossa. Rakennus Miilukankaalla on Jydacom, johon kirjaudutaan omilla tunnuksilla (osittain). Kaikille henkilöille ei ole omia tunnuksia. Lisäksi maksuliikennettä hoidetaan Nordean ja Osuuspankin kortinlukulaitteilla.

4 TOTEUTUS

Tietoturvallisuus on monien asioiden summa, jossa jokaisella on oma tehtävänsä, jotta kokonaisuus toimii luotettavasti. Tietoturvallisuuden osina käsitellään yleensä seuraavia tekijöitä: 1. Saatavuus tai käytettävyys, jolla tarkoitetaan sitä, että tieto on saatavilla silloin, kun sitä tarvitaan. 2. Luottamuksellisuus tarkoittaa sitä, että tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus. 3. Eheys tarkoittaa sitä, että tieto ei saa muuttua tahattomasti tai hyökkäyksessä, tai muutos pitää ainakin havaita. Toisinaan eheys määritellään myös tietojen loogisuudeksi ja paikkaansa pitävyydeksi.

Valtionhallinnon tietoturvallisuuden johtoryhmän hyväksi havaitut tietoturvallisuusohjeet ja -määräykset toimivat myös pienissä ja keskisuurissa yrityksissä. Nämä laajalti käytössä olevat ohjeet ja määräykset ovat johdonmukaisia ja käsittelevät tietoturvallisuuden kaikkia kahdeksaa osa-aluetta (kuva 2).



KUVA 2. Tietoturvan osa-alueet.

Valtiovarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI toimii hallinnon

tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. (Tietoturvallisuus, hakupäivä 24.5.2012.)

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTIn toimialaan kuuluvat kaikki valtionhallinnon tietoturvallisuuden osa-alueet: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. (Tietoturvallisuus, hakupäivä 24.5.2012.)

Tässä osassa kerrotaan, miten määritelmässä esitetyt toiminnot on toteutettu. Tämä on se osio, joka kertoo, miten yrityksen tietoturvapolitiikka ja tietoturvasuunnitelma on tehty. Tämän lisäksi kerrotaan, kuinka näiden puutteiden johdosta joudutaan toimintakäsikirjassa olevia tietoturvan ja tietotekniikan ohjeistusta uusimaan.

4.1 Tietoturvapolitiikka

Tietoturvapolitiikka on yksi osa tietoturvallisuutta. Sillä määritellään yrityksen toimintaa tietoturvallisessa toiminnassa. Tietoturvapolitiikkaa luodessa tulee ensimmäiseksi tarkastella yrityksen tietoriskejä. Tietoriskien pohjalta lähdetään kehittämään yritykselle tietoturvapolitiikkaa ja tietoturvasuunnitelmaa. Ilman tätä riskienkartoitusta on vaikea hahmottaa yrityksen tilaa ja toiminnan hyviä ja huonoja puolia. Tietoturvapolitiikan tulee tukea tietoturvallisuuden kehittymistä.

4.1.1 Tiedonhankinta

Kun aloin tehdä yritykselle tietoturvapolitiikkaa, tutkin eri aineistoja ja lähteitä. Tähän kuului lukuisten yritysten ja yhteisöjen tietoturvapolitiikkojen tutkimista ja sen analysointia, mitä hyvää ja huonoa niissä oli. Tätä nykyä pienet ja keskisuuret yritykset ja julkinen sektori ovat alkaneet luoda tietoturvapolitiikkoja ja tietoturvasuunnitelmia omaan toimintaansa. Kaikissa näissä oli yhteisenä tekijänä VAHTIn käyttäminen eräänlaisena runkona, josta kukin sektori oli tehnyt omanlaisensa tulkinnan. Kunnat, koulut, yliopistot ja muu valtionhallinto käyttävät suoraan VAHTI-ohjeistusta.

Oma pyrkimykseni oli käyttää hyväksi molempien sektoreiden hyviä puolia. Kuntasektorin täsmällinen ja pikkutarkka toimintamalli, jossa jokaiselle henkilölle on määritelty tehtäväkokonaisuus ja

tarkka vastuualue, antaa hyvän lähtökohdan tietoturvallisuuden suunnitteluun. Toisaalta pienien ja keskisuurten yritysten hiukan laajempi ajattelu tehtävistä ja töiden tekemisestä antaa taloudellisen näkökulman tietoturvallisuuden suunnitteluun. Pienissä ja keskisuurissa yrityksissä ei ole jokaiseen tehtävään järkevää palkata uutta henkilöä, vaan sen työn tekee se henkilö, jonka toimenkuvaan se parhaiten sopii. Ongelmia aiheutti erityisesti organisaation kapeus. Organisaatiossa on muutama henkilö joille tämä tietoturvapolitiikassa määritellyt tehtävät ja vastuut kuuluvat.

VAHTI-ohjeen mukaisessa tietoturvapolitiikassa on paljon sellaisia käsitteitä kuten toimintayksikkö, tietoturvavastaava, yksiköidenjohtajia, tietoturvaryhmä ja omistaja. Näistä viimeisin aiheuttaa jo ongelmia tulkinnassa, tarkoitetaanko tässä yrityksen omistajia vai tietoaineiston omistajaa. Pienissä ja keskisuurissa yrityksissä tietoaineistonomistaja on useimmiten yritys, joka ei aina ole niin helposti ymmärrettävä asia.

4.1.2 Rakenne

Tietoturvapolitiikka muodostaa selkärangan tietoturvallisuuden jatkuvalle kehittämiselle. Tietoturvapolitiikassa otetaan kantaa seuraaviin asioihin: tietoturvallisuuden tavoitteisiin, rooleihin, vastuisiin, koulutukseen, tietojen suojaukseen ja seurauksiin laiminlyönneistä tietoturvallisuudessa. Tietoturvapolitiikalle ei ole valmista mallia, johon voitaisiin rakentaa yrityksen tai organisaation tietoturvapolitiikka.

Tietoturvapolitiikan on tarkoitus olla lyhyt ja ytimekäs selostus, jossa kerrotaan tietoturvallisuuden päälinjat ilman mitään teknisiä yksityiskohtia, jotka voivat olla yrityksen kannalta vahingollisia. Se kirjoitetaan yleisellä tasolla, että jokainen, joka sen lukee, ymmärtää lukemansa. Tietoturvapolitiikka on julkinen asiakirja, joka on mahdollista julkaista yrityksen internet-sivulla.

Yrityksen tietoturvapolitiikka rakentui neljästä osasta: päämäärät ja tavoitteet, organisointi ja vastuut, toteutuskeinot ja tietoturvallisuuden seuranta ja ongelmien käsittely. Miilukankaan tietoturvapolitiikka on liitteenä 4.

4.1.3 Sisältö

Tietoturvapolitiikassa ensimmäiseksi kerrotaan tietoturvallisuuden päämärät ja tavoitteet. Päämäärät ja tavoitteet ovat turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeät tiedot, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta ja estää niiden valtuudeton käyttö sekä

tahaton tai tahallinen tiedon tuhoaminen ja vääristyminen. Tietoturvatyö on jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa koko Miilukankaan osalta. Sillä pyritään ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista toipumiseen.

Organisointi ja vastuut kohdassa kerrotaan, kuinka nämä edellä mainitut päämärät ja tavoitteet vastuutetaan organisaatiossa. Tietoturvallisuus toteutuu tehokkaimmin, kun toimintaa ohjaavat nimetyt vastuuhenkilöt ja kaikki tiedon käsittelijät huolehtivat oman tehtäväkenttänsä turvallisuudesta parhaalla mahdollisella tavalla. Jokaisella Miilukankaan työntekijällä on siten vastuu tietoturvallisuuden toteuttamisesta ja valvonnasta ja velvollisuus noudattaa Miilukankaan antamia tietoturvallisuuteen liittyviä sääntöjä ja ohjeita.

Toteutuskeinoissa kerrotaan, kuinka yritys aikoo toteuttaa päämäärissä ja tavoitteissa määrittelemänsä asiat. Olennaisena osana tietoturvallisuuden toteutuskeinoja ovat henkilöstön kouluttaminen, tietoriskien arviointi, tietoturvallisuuden kehittäminen ja sidosryhmien kanssa sovittavat sopimukset.

Tietoturvallisuuden seuranta ja ongelmien kohdassa kerrotaan, kuinka yritys varmistaa sen, että kaikki edellä mainitut seikat toteutuvat. Seurantaa toteutetaan niin teknisillä apukeinoilla kuin hallinnollisilla menetelmillä. Eräs hallinnollinen keino on sisäisten auditointien suorittaminen. Näin pystytään koko organisaation tietoturvallisuus tarkistamaan.

4.2 Tietoturvasuunnitelma

Miilukankaalle tekemäni tietoturvasuunnitelma on julistettu salaiseksi. Yrityksille tehtävät tietoturvasuunnitelmat ovat yleensä kokonaan salaisia tai osittain salaisia. Osittain salaisissa tietoturvasuunnitelmissa kerrotaan ainoastaan yleisiä asioita ja käsitteitä sekä eri kohtien vaikutukset organisaation tietoturvallisuuteen. Kokonaan salaisiksi julistetuista tietoturvasuunnitelmista löytyy ainoastaan selitys, että tällainen asiakirja löytyy organisaatiosta sekä kuka sitä ylläpitää.

Kuten aiemmin kerroin, ensin täytyy selvittää organisaation tietoriskit, jonka jälkeen luodaan tietoturvapolitiikka ja lopuksi tehdään tietoturvasuunnitelma. Tietoturvasuunnitelma sisältää paljon yksityiskohtaista tietoa organisaation tietoteknisistä ratkaisuista, salasanakäytännöistä, palvelimien asetuksista, palvelimien verkko-osoitteista ja palomuurin asetuksista. Tässä dokumentissa kerron mihin asioihin kiinnitin huomiota yrityksen tietoturvasuunnitelmaa tehdessä.

Tietoturvasuunnitelma on eräänlainen ohjekirja yrityksen johdolle, mutta ennen kaikkea se on työkalu yrityksen IT-osastolla työskenteleville henkilöille. Sieltä voidaan tarkastaa, kuinka jokin tietoturvallisuuden kohta on siinä käsitelty. Tietoturvasuunnitelmalla ohjeistetaan ja opastetaan yritystä korjaamaan tietoriskikartoituksessa ilmenneitä epäkohtia. Tietoturvallisuuden tärkein tavoite on tukea organisaation toimintaa ja tavoitteiden saavuttamista huolehtimalla tietoaineistojen luottamuksellisuudesta, eheydestä ja saatavuudesta. Tämä on mahdollista ainoastaan ottamalla tietoturvallisuus huomioon tiedon elinkaaren kaikissa vaiheissa. (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 25. Hakupäivä 3.12.2012.)

Tietoturvasuunnitelman tavoite on varmistaa, että jokainen tietojärjestelmän osa suojataan riittävän hyvin siihen kohdistuviin riskeihin verrattuna. Tällä tavalla voidaan varmistaa, että järjestelmä on riittävän turvallinen ja ettei tietoturva kuluta ylimääräisiä resursseja. (Ruohonen 2002, 6.)

Tietoturvasuunnitelmassa kerrotaan käytössä olevat ratkaisut ja periaatteet. Suunnitelman tarkoitus on käsitellä yrityksen tietoturvaan liittyviä asioita. Dokumentti on tehty tietoturvapolitiikassa määritettyjä linjauksia noudattaen. (Lehto 2010, 13.)

4.2.1 Tiedonhankinta

Tietoturvasuunnitelmaa tehdessä törmäsin ongelmaan, jota en ollut tullut ajatelleeksi eikä internetistä löytynyt vastausta. Ongelman aiheutti tyyli, jolla kirjoitin tietoturvasuunnitelman. Se poikkeaa hiukan tavanomaisesta seitsemän tietoturvallisuuden osa-alueen käsittelytavasta. Tietoturvasuunnitelma toteutettiin tietoriskikartoituksen pohjalta, jossa aihetta on käsitelty hiukan eri tavalla. Siinä käsitelty tapa oli monella tapaa hyvä koska se tehtiin organisaatiokohtaisella ajattelulla, kun taas normaalisti se tehdään tietoturvallisuuden seitsemän osa alueen mukaan. Tämä aiheutti sen, että jouduin eri lähteistä keräämään tiedon yrityksen tietoturvasuunnitelmaan. Useassa kohdassa jouduin käyttämään paljon eri lähteitä, koska yhdestä lähteestä ei löytynyt yksiselitteistä vastausta jonkin tietoriskin pienentämiseksi.

Tietoturvasuunnitelman runko rakentui tietoriskikartoituksen pohjalta tulleeseen jaotteluun. Jokaisessa osa-alueessa kerrotaan hiukan osa-alueeseen liittyvää teoriaa, nykytilanne ja korjaustoimenpiteet.

4.2.2 Rakenne

Tietoturvasuunnitelma koostui tietoriskikartoituksen kuudesta eri osa-alueesta, jotka olivat tietoriskien hallinta ja johtamien, henkilöstön toiminta, toimitilat, tietojärjestelmien suojaus, sidosryhmät ja toiminnan kehittäminen.

4.2.2.1 Tietoturvallisuuden johtamien

Tiedoista huolehtiminen on tärkeässä roolissa organisaation toimintojen, turvallisuuden ja jatkuvuuden varmistamisessa. Tietoturvallisuuden organisointi ja toteutus tulee tehdä siten, että se tukee parhaalla mahdollisella, kustannustehokkaalla tavalla organisaation hyvän hallintotavan toteuttamista sekä perustehtävä- ja strategiatavoitteiden saavuttamista. Tietoturvallisuuden toteuttamisessa keskeisiä ovat myös hyvän tiedonhallintatavan velvoitteet, joiden kautta tietoturvallisuudella on tärkeä rooli turvallisen tietoteknisen ympäristön ja tietohallintotoiminnan ylläpitämisessä ja kehittämisessä. (Johdon tietoturvaopas 2/2011, 11. hakupäivä 5.1.2013.)

Tietoturvatyölle tarvitaan johdon tuki, jolla varmistetaan työn toteuttamisen edellytykset. Tietoturvallisuuden tulee olla kiinteä osa organisaation johtamista, suunnittelua ja jatkuvaa kehittämistä. Johdon tulee osoittaa tietoturvatyölle riittävät resurssit ja tarvittavat ohjausmekanismit organisaation tietoturvatavoitteiden saavuttamiseksi. Tietoturvallisuuden tavoitteet ja toimenpiteet näiden saavuttamiseksi pystytään arvioimaan riskienarvioinnin ja vuosisuunnittelun avulla. (Johdon tietoturvaopas 2/2011, 12. hakupäivä 5.1.2013.)

Kirjassaan Esimies ja tietoriskien hallinta Tuija Kyrölä (2001, 208.) sanoo: ”Johdon vastuulla on varmistaa liiketoiminnan jatkuminen häiriötilanteissa ja käsiteltävien tietojen suojaamistahdon konkretisointi.” Johdon tärkeimpiä tehtäviä on kiinnittää huomioita organisaation kokonaisvaltaiseen tietoriskien ja tietoturvallisuuden hallintaan, joka kattaa sekä oman toiminnan, että kaikki sidosryhmät, asiakkaat, sopimuskumppanit ja erilaiset palveluntarjoajat. Tietoriskit nousevat kokoajan suurempaan rooliin yrityksien riskienhallinta prosesseissa. Haastavaksi tämän tekee se, että yritykset ovat kasvavassa määrin riippuvaisia erilaisista ulkoisista sidosryhmistä. Tämän takia tietoriskit eivät ole enää yrityksen omassa hallinnassa.

Johdon keskeiset tietoturvavelvoitteet voidaan tiivistää seuraaviin kymmeneen kohtaa. Tätä voidaan kutsua johdon tietoturvavelvoitteiden muistilistaksi:

1. Lainmukaisuuden varmistaminen

2. Riskienhallinnan- ja hallintajärjestelmän toteuttaminen
3. Tietoturvapolitiikkaan sitoutuminen
4. Tietoturvajohtaminen
5. Tietoturvavastuuhenkilön nimeäminen
6. Tietoturvallisuuden organisointi
7. Tietoturvallisuuden toteutumisen varmistaminen
8. Tietoturvallisuuden tietoturvasuunnittelun edellytysten luonti
9. Poikkeama- ja erityistilanteiden hallinta
10. Tietoturvaraportointivelvollisuuksista huolehtiminen

(Johdon tietoturvaopas 2/2011, 14. hakupäivä 5.1.2013.)

Yritysjohdon laiminlyödessä tietoturvallisuuden ylläpidon he altistavat yrityksen turhille riskitekijöille. Kyseinen riski on helposti poistettavissa tai ainakin pienennettävissä, sillä tietoturvaa voidaan parantaa pienillä keinoilla, eikä se vaadi suuria summia rahaa. Yrityksen hallinnollisilla toimenpiteillä ja tehtäväkohtaisilla koulutuksilla voidaan valistaa henkilöstöä tarpeeksi. Koulutustenkaan ei tarvitse olla laajoja ja useita tunteja kestäviä. Esimerkiksi viikoittain lähetettävällä tietoturvasähköpostilla tavoitetaan koko henkilöstö ja ohjeita saadaan levitettyä työntekijöiden tietouteen heidän omien esimiestensä välityksellä. (Laakso 2010, 33–34.)

4.2.2.2 Henkilöstön tietoturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa, erotuksena kuitenkin henkilöturvallisuudesta, jolla käsitetään ihmisiin kohdistuvien riskien hallintaa. Henkilöstöturvallisuus ymmärretään osaksi yleisempää turvallisuuskäsitettä. Tietoturvallisuudessa henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä. Henkilöstöturvallisuuden merkitys tietojen turvaamiselle on suuri, koska ihmisen toiminta merkittävässä roolissa tietoja käsitellessään. (Tärkein tekijä on ihminen 2/2008, 12. hakupäivä 10.11.2012.) Henkilöstö käsittelee tietoja vastaanottamalla, muokkaamalla, tallentamalla, välittämällä ja lopulta hävittämällä tiedon tarvittaessa. Henkilöstöturvallisuus ja henkilöstön toiminta tietoa käsitellessään ilmenee hyvin kuvasta 3.

Henkilöstöturvallisuus sisältää kaksi toisistaan riippuvaista vaatimusta:

- käytettävyysvaatimus ja tietojen eheysvaatimus
- salassapitovaatimus.

KUVA 3. Henkilöstöturvallisuuden haaste suojata tietoa ja turvata sen saanti (Tärkein tekijä on ihminen 2/2008, 12. hakupäivä 10.11.2012.)

Tieto on immateriaalista, sitä voi monistaa ja lähettää ilman, että alkuperäinen tieto katoaisi. Toisaalta tieto voidaan helposti hukata tai tuhota vahingossa. Organisaatioiden sähköisesti ja paperimuotoon tallennettu tietomassa on valtava. Tiedon hallinnasta on tullut organisaatioiden toiminnan keskeinen haaste. Henkilöstöturvallisuus on organisaation tietoturvallisuuden keskeinen alue ja se koskettaa kaikkia työntekijöitä. Henkilöstöturvallisuustyö on luonteeltaan ennalta ehkäisevää. Henkilöstöturvallisuuteenkin pätee turvallisuustoimintaa yleisesti kuvaava toteamus, että myös tällä osa-alueella maksetaan enimmäkseen siitä, että mitään ikävää ei tapahdu. (Tärkein tekijä on ihminen 2/2008, 12. hakupäivä 10.11.2012.) Tietoriskien ja tietoturvallisuuden koordinoinnin ja hallinnan kulut ovat usein yleiskuluja. Juuri siksi työn resurssien tulee olla organisaation käytössä ja heille hyödyksi.

4.2.2.3 Toimitilojen turvallisuus

Toimitilojen turvallisuus liittyy tietoturvallisuuden fyysiseen turvallisuuteen. Fyysistä tietoturvallisuutta ei mielletä helposti tietoturvallisuuden osa-alueeksi, mutta todellisuudessa sillä on suuri merkitys tietoturvalle. Järjestelmien hyvä tekninen toteutus ei auta jos kuka tahansa pääsee yrityksen toimitiloihin käyttämään yrityksen tietokoneita ja järjestelmiä tai jopa viemään ne mukanaan. (Ruohonen 2006, 4.) Organisaatio tarvitsee toimintansa harjoittamiseen toimitilat. Toimitilojen on hyvä näyttää jo fyysisiltä piirteiltään sellaisilta, että se ei houkuttele luvattomaan käyttöön. Sillä se on perusta kaikelle muulle tietoturvatyölle. Laaksonen ym. (2006, 126.) mukaan fyysinen turvallisuus sisältää organisaation tuotanto- ja toimitilojen fyysisen suojaamisen liittyvät asiat, joilla pyritään estämään organisaation tarvitsemien tietojen tuhoutumien, vahingoittuminen tai joutuminen vääriin käsiin.

Yrityksen kaikki toimitilat eivät ole keskenään fyysisesti samanarvoisia tietoturvallisuuden kannalta. Korkean suojauksen tason vaativat yrityksen oman vahvuusalueisiin kuuluvat tilat, esimerkiksi tuotekehitystilat, atk-laitetilat sekä hallinnolliset tilat. Näistä yksi haastavimpia ovat atk-laitetilat, koska nämä ovat monessa yrityksessä osittain palveluntarjoajienkin tiloissa, sillä nämäkin kuuluvat yrityksen fyysisen turvallisuuden piiriin.

Korkealla suojaustasolla tarkoitetaan esimerkiksi aidattua aluetta, jossa on hallittu kulunvalvonta ja kattava kameravalvonta toimitiloissa sekä hälytysjärjestelmä. Näiden lisäksi eri tiloihin voidaan laittaa etähallittavia sähkölukkoja sekä määritellä henkilöstölle näihin oviin erilaisia kulkuoikeuksia. Nykyaikaisilla kulunvalvontajärjestelmiin liitetyillä kulkukorteilla on helppo hallita henkilöstön liikkumista toimitiloissa. Organisaation avaintenhallinta on yksi tärkeä osa fyysistä turvallisuutta. Senkin täytyy olla ajan tasalla ja järjestetty niin, että tiedetään kenellä on avaimet mihinkin tiloihin.

4.2.2.4 Tietojärjestelmien suojaus

Tietojärjestelmien suojaus on ehkä näistä kaikista osa-alueista teknisin, joka on tekniikkaan ja ohjelmistoon liittyvä kokonaisuus. Tähän liittyvät kytkimet, reitittimet, palvelimet, palomuurit, tietoliikenneyhteydet ja ennen kaikkea ohjelmistot mitä organisaatioissa käytetään. Monesti luullaan tekniikan pelastavan tietojärjestelmät ulkoisilta uhilta, mutta todellisuudessa tekniikkakaan ei poista henkilöiden vaikutusta järjestelmiin. Tätä osa-aluetta kutsutaan monesti tekniseksi tasoksi. Tämän osa-alueen käsittelyn pääpaino on teknisissä ja ohjelmistollisissa ratkaisuissa. Tämä osa-alue on

oikeastaan ainoa, joka koskee vain ICT- ja tietoturvahenkilöstöä sekä muita tietoaineistojen käsittelystä vastaavia henkilöitä.

Tietojärjestelmien suojaukseen kiinteänä osana liitetään myös termit, kuten etätyö ja etäkäyttö, päätelaite, suojattava kohde, suojaustaso, tietoaineisto, tietojenkäsittely-ympäristö, tietoturvataso ja tärkeys- ja turvallisuusluokka. Näistä olennaisia termejä selvennän hieman seuraavaksi.

Etäkäytöllä tarkoitetaan yrityksen toimitilojen ulkopuolelta tapahtuvaa satunnaista tietojärjestelmien ja palveluiden käyttöä. Tavallisimpia etäkäyttöä kuvaavia toimia ovat sähköpostin ja kalenterin sekä organisaation intranetin tai työryhmäpalveluiden hyödyntäminen organisaation tarjoamalla kannettavalla tai älypuhelimella. Etätyö poikkeaa etäkäytöstä siinä, että etätyö on luvanvaraista, mutta pohjautuu normaalisti tarkkaan, ennakolta sovittuun työmäärään ja työtehtävään, joka tyypillisesti tehdään kotoa. Teknisesti etätyö ja etäkäyttö voidaan toteuttaa samanlaisille teknisillä ratkaisuilla. Lisähaastetta etätyössä tulee mahdollisesti kotona säilytettävien tietoaineistojen säilyttämisen ja käsittelyn osalta. (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 15. hakupäivä 3.12.2012.) Teknisinä ratkaisuina käytetään VPN (Virtual Private Network) eli virtuaalista yksityisverkkoa. Tämä voidaan toteuttaa joko ohjelmistopohjaisesti tai laitteistopohjaisesti. Ohjelmistopohjaiset ratkaisut ovat joustavia, kun taas laitteistopohjaiset ovat tehokkaampia.

Tietojenkäsittely-ympäristöllä tarkoitetaan organisaation ICT-palveluiden kautta käyttöönsä hankkimaa kokonaisuutta, jonka avulla se tuottaa tarvitsemansa perustietotekniikan ja ydintietojärjestelmiin liittyvät kokonaisuudet. Organisaatio voi vastata kokonaan tai osittain kokonaisuuden tuottamisesta itse tai se voi hankkia tarvitsemiaan ICT-palveluita osittain tai kokonaan ulkoistettuna. Ulkoistaminen ei poista organisaation vastuuta huolehtia kokonaisuuden tietoturvavaatimustentäyttämisestä. (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 16. hakupäivä 3.12.2012) Organisaation tietojenkäsittely-ympäristö koostuu kuvan 4 mukaisista palveluista ja teknisistä ratkaisuista.

KUVA 4. Organisaation tietojenkäsittely-ympäristö (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 17. hakupäivä 3.12.2012.)

ICT-palveluiden runko muodostuu työasemista ja päätelaitteista. Päätelaitteita tulee tarkastella laajemmin koska älypuhelimetkin ovat nykyään myös päätelaitteita. Tavallisesti päätelaitteeksi mielletään kannettava tai tablet-tietokone, mutta tähän kategoriaan voidaan myös lisätä pääteistunnot. Päätelaitteen tyypistä ja mallista riippumatta laitteen tulee täyttää ICT-palveluiden asettamat vaatimukset.

Tietoturvallisuuden kannalta keskeisimpiä päätöksiä on se, mille tietoturvatasolle päätelaitteet ja tietokoneet vakioidaan tai rakennetaan. Päätelaitteiden ja palvelimien tietoturvallisuus tulee rakentaa kerrostetun tietoturva-arkkitehtuurin mukaisesti. Tällöin yhden tai useamman teknisen tietoturvakontrollin pettäessä toiminnassa olevat tekniset ratkaisut joko estävät tai rajoittavat syntynyttä uhkaa. Kerrostuneisuuden tulee alkaa päätelaitteista ja jatkua tietoliikenneverkkojen ja laitteiden kautta käytettäviin palvelimiin ja palveluihin. (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 41. hakupäivä 3.12.2012.)

Kannettavat päätelaitteet ovat tyypillisesti kannettavia tietokoneita, tabletteja tai älypuhelimia. Niiden muuttuvat ja vaihtelevat käyttöympäristöt aiheuttavat tietoturvallisuuden haasteita. Laitteiden fyysistä tietoturvallisuutta ei voida varmistaa. Tästä johtuen laitteessa olevien tietojen tarvittavasta salaamisesta tulee huolehtia. Tämä voidaan toteuttaa kiintolevyn salaavalla ohjelmistolla, joka on organisaation ICT-tuen keskitetyssä hallinnassa. Kannettavia laitteita käytettäessä myös tietolii-

kenneyhteydet on eri tavoin toteutettuja. Päätelaite on suositeltavaa varustaa joko kaiken tietoliikenteen automaattisesti salaavalla ratkaisulla (esimerkiksi VPN/SSL-VPN) tai salata tietoliikenne asiakasohjelmittain (client-tasolla). Tarvittaessa käyttötilanteissa tulee huolehtia myös vahvasta käyttäjän ja päätelaitteen tunnistamisesta. (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 45, hakupäivä 3.12.2012.)

Pääteistunnoilla tarkoitetaan sellaista ICT-palveluiden käyttöä, jossa palvelun käyttämiseen tarvittava yhteys luodaan asiakasohjelman (client-ohjelmisto) tai www-selaimen sijaan pääteistuntona (terminal session). Käytössä olevalta laitteelta kuten pöytätietokoneelta, kannettavalta tietokoneelta, tabletilta, älypuhelimelta tai niin sanotulla tyhmällä päätteellä muodostetaan salattu ja tarvittaessa vahvasti tunnistettu istunto päätepalvelimeen, jossa toimii halutun ICT-palvelun käyttämisen mahdollistava asiakasohjelma tai www-selain. Pääteistunnon toimintaperiaate on kuvattu liitteessä 5. Pääteistunnot ovat kustannustehokas ja tietoturvallinen ratkaisu useissa ympäristöissä. Usein palveluntarjoaja toteuttaa pääteistunnon ja sitä kutsutaan virtuaaliympäristöksi, jota on helppo muokata organisaation tarpeiden mukaan. (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 45–46, hakupäivä 3.12.2012.)

Tietoturvatasoista ja tärkeys- ja turvaluokista puhuttaessa törmätään myös käyttäjien tunnistamiseen. Tietojärjestelmien turvallinen ja asianmukainen käyttö pohjautuu käyttäjien tunnistamiseen. Käyttäjän tunnistustapoja on kahdenlaisia: kevyt ja vahva tunnistus. Tunnistamista kutsutaan kevyeksi tunnistamiseksi, kun se nojautuu vain yhteen todentamiseen kuten käyttäjätunnus ja salasana, pelkkä sirukortti tai pelkkä biotunniste. Vahva tunnistaminen nojautuu kahteen tai useampaan todentamiseen kuten verkkopankkitunnukset ja vaihtuva salasana sekä varmenteellinen sirukortti ja salasana. Silloin, kun käyttäjät käyttävät organisaation sisällä heille myönnettyjä laitteita ja resursseja, riittäväksi tunnistusmenettelyksi katsotaan kevyttä tunnistamista. Vahvaa tunnistamista tarvitaan silloin, kun käytetään organisaation ulkopuolelta yrityksen palvelimia tai tietokantoja turvattomista verkoista.

Hyvään tiedonhallintatapaan kuuluu järjestelmien toiminnan seuraaminen, ei-toivottujen tapahtumien ennakointi, tapahtuneisiin tilanteisiin reagointi sekä toiminnan kehittäminen tehtyjen muutoksien pohjalta. Järjestelmän ylläpitäjän ja omistajan pitää tietää, kuinka järjestelmä toimii tai mitä se ei tee normaali tilanteessa. (Lokiohje 3/2009, 20. hakupäivä 12.1.2013.) Mikään järjestelmä ei ole turvallinen ja siltä tarvitaan koko ajan palautetta. Lokien tuottama data auttaa järjestelmän ylläpitäjiä kehittämään järjestelmää, reagoimaan ongelmiin ja auttaa selvittämään tietoturvapoikkeamia.

Loki tallentaa tapahtumia, jotka ovat tapahtuneet organisaation järjestelmissä, verkoissa tai muussa ympäristössä ja toiminnassa. Lokitiedot voivat olla automaattisten järjestelmien keräämiä merkintöjä tai manuaalisesti kerättäviä lokitietoja, kuten esimerkiksi vierailijaloki. (Lokiohje 3/2009, 13. hakupäivä 12.1.2013.) Tietoturvallisuuden ja tietosuojan kannalta on erittäin tärkeää, että nämä tiedot suojataan luotettavasti ja vaatii täten seurannan.

VAHTI-ohjeessa on lokeja käsitelty neljässä luokassa, jotka ovat ylläpitoloki, käyttöloki, muutosloki ja virheloki. Monet lokit voivat kuulua sisällöltään moneen edellä mainittuun lokiin eikä niitä täten voida yksiselitteisesti sijoittaa johonkin luokkaan. (Lokiohje 3/2009, 29. hakupäivä 12.1.2013.) Näitä lokeja on erilaisia erilaisiin käyttötarkoituksiin. Lokitietoja tarkastelemalla pystytään esimerkiksi tutkimaan normaalista käyttötilanteesta poikkeavia arvoja.

4.2.2.5 Sidosryhmien tietoturvallisuus

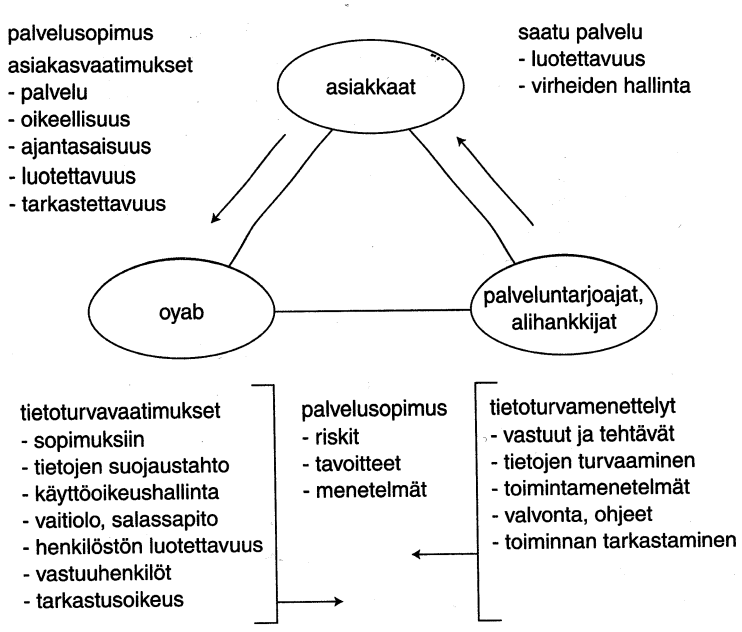
Sidosryhmien tietoturvallisuus on haastavin ympäristö hallita tietoriskejä, koska tässä toimitaan oikeastaan tietoturvallisuuden kaikilla osa-alueilla. Organisaatiot ovat hyvin pitkälle riippuvaisia ulkoisista sidosryhmistä. Sidosryhmät voidaan jakaa kahteen pääryhmään: asiakkaisiin ja palveluntarjoajiin, toiselta nimeltään ostopalvelu. Asiakkaat voivat vaatia tietynlaista menettelyä heidän töidensä osalta, mikä tekee tietoturvallisuuden hallinnasta varsin vaikeaa jos jokainen asiakas haluaa omanlaistansa menettelyä. Ostopalvelut muodostuvat usein laajoiksi, ja varsinainen palveluntuottajan henkilöstö saattaa jäädä huomioitta, kun laaditaan sopimuksia. (Tärkein tekijä on ihminen 2/2008, 43. hakupäivä 10.11.2012.)

Käsiteltäviin tietoihin liittyvät riskit täytyy tunnistaa liikesuhteissa. Sidosryhmät listataan, välitettävät tiedot tunnistetaan, sopimuksiin liitetyt tietojen käsittelykäytännöt ja niiden puutteet kartoitetaan ja tietoriskit arvioidaan. Selvitys antaa hyvän perustan yhteisten käytäntöjen, toimintamenetelmien ja suojauskeinojen kehittämiselle. Näin pystytään varmistamaan se, että osapuolten kanssa välitetään vain sellaista tietoa, jota he tarvitsevat, ja että yrityksen tahto tietojen suojaamisessa toteutuu. Sidosryhmiä ovat mm. päämiehet, kumppanit, asiakkaat, palvelujen tarjoajat ja ohjelmisto- ja muut toimittajat. On tärkeää tunnistaa kaikki osapuolet, kuten tutkimus- ja oppilaitokset kotimaassa ja ulkomailla. (Kyrölä 2001, 43.)

Asianmukaisella tietojen suojaamisella turvataan yrityksen toimintaympäristöä, yhteiskuntaa sekä asiakkaiden ja yhteistyökumppaneiden tietoja. Tietojen luvaton päätyminen sivullisille voi täyttää rikoksen tunnusmerkistön. Se voi myös vaarantaa toimintaympäristön turvallisuuden ja palveluiden

jatkuvuuden tai rikkoa yksilöiden perusoikeuksia, yksityisyyden suojaa ja turvallisuutta. Organisaation tulee omaan toimintaan liittyvien tietojen salassapidon lisäksi huolehtia sidosryhmiensä ja erityisesti asiakkaidensa tiedoista. Muun muassa henkilötietoihin ja yritysten liike- ja ammattisalaisuuksiin liittyy salassapitovelvoite. (Johdon tietoturvaopas 2/2011, 13. hakupäivä 5.1.2013.)

Yksikään yritys ei ole olemassa itseään varten, vaan ne toteuttavat omistajien ja sijoittajien niille haluamaa tehtävää. Omistajat valitsevat yrityksen johtoon pätevät henkilöt, jotka osakeyhtiölain mukaan vastaavat liiketoiminnan jatkuvuuden hallinnasta. Jatkuvuuden hallintaa on myös varautuminen tietoriskeihin ja tietoturvallisuuden parantaminen. Johdon tehtävänä on määritellä vaatimukset toiminnan häiriöiden hallintakyvylle, tunnistaa asiakkaiden vaatimukset ja eri sidosryhmien odotukset sekä pyrkiä kehittämään tietoriskien hallintamenettelyjä. Kuvassa 5 kuvataan asiakkaan, asiakaspalveluyrityksen ja yritykselle palveluja tarjoavan alihankkijan välisiä suhteita. Asiakas ostaa palveluita ja sopii niistä yrityksen kanssa, jolloin asiakkaalla on oikeus vaatia esimerkiksi hänen tietojensa huolellisesta käsittelyä ja yrityksellä velvollisuus käsitellä niitä huolellisesti. Yritys hankki alihankintapalveluita, jolloin yritysten kesken tehdään palvelusta sopimus, johon tulee liittää ostavan yrityksen ja sen asiakkaiden tietojen käsittelyvaatimukset sekä kummankin yrityksen oikeudet ja velvollisuudet tietoriskien hallinnassa. (Kyrölä 2001, 52.)



KUVA 5. Yrityksen ja sidosryhmien vaatimukset tiedon käsittelylle (Kyrölä 2001,52.)

Suurin osa sovelluksista ja tiedostoista sekä niiden käsittelemistä ja tuottamista tiedoista sijaitsevat fyysisesti palveluntarjoajan tiloissa. Tiedot tulee suojata asiattomalta muuttumiselta, tuhoamiselta, kopioinnilta, urkkimiselta, siirrolta ja paljastumiselta Teknisen ympäristön toiminnan turvallisuus ja tietojen suojaaminen on arvioitava niin omassa ympäristössä kuin palveluntarjoajankin ympäristössä. (Kyrölä 2001, 80.)

Palveluyritysten ja asiakkaiden kanssa tulisi tehdä turvallisuus- tai salassapitosopimus. Turvallisuussopimus on laajempi koko yritystä ja sen turvallisuutta koskeva sopimus ja salassapitosopimukset koskevat henkilöstöturvallisuutta. Sopimukset ovat luonteeltaan yritysten välisiä turvallisuusjärjestelyjä koskeva yleissopimus, jossa määritellään sopijapuolten kesken noudatettavista turvallisuusmenettelyistä. (Tärkein tekijä on ihminen 2/2008, 43. hakupäivä 10.11.2012.)

4.2.2.6 Kehittäminen ja toiminnan jatkuvuus

Miilukankaalla on paljon tehtäviä tulevaisuudessa, jotka pitää laittaa vielä kuntoon. On tehty tietoturvasuunnitelma, jolla on haettu tietoriskikartoituksen puutteiden korjaukset. Tietoturvapolitiikka ja tietoturvasuunnitelma eivät ole staattinen olotila vaan ne vaativat koko ajan parantamista ja kehittämistä. Tulee laatia joukko erilaisia ohjeita, joista osa päivitetään myös yrityksen toimintakäsikirjaan.

Tietoturvallisuuden toiminnan kehittämisen kulmakiviä ovat henkilöstön jatkuva kouluttaminen ja opastaminen. Parempaa reagoimista vikatilanteisiin pitää kehittää ja niiden kirjaamista esimerkiksi Arrow-kunnossapito-ohjelma. Näin voidaan seurata laitteiden vikaantumista ja vikaantumistaajuutta. Näillä keinoilla voidaan todentaa itselle ja sidosryhmille, että näitä asioita seurataan jatkuvasti. Yhteistyön tiivistämistä myös palveluntarjoajien kanssa tulee kehittää. Epäselviä käytäntöjä ja toimintatapoja pystytään parhaiten poistamaan opastuksella ja tekemällä dokumentit tehdyistä muutoksista. Olkoot ne muutokset sitten palvelintasolla tai jonkin sovelluksen käyttöönotossa.

Tietoriskikartoitus tulee tehdä kahden vuoden välein ja samassa laajuudessa kuin ensimmäinenkin. Kuten auditoinnissakin, ensin tutkitaan onko edelliset riskit ja puutteet korjattu, ja sen jälkeen selvitetään nykytilanne. Tietoturvapolitiikka tulee tarkastella kerran vuodessa, onko tullut muutoksia organisaatiossa tai toimintatavoissa. Tietoturvasuunnitelmaa tulee päivittää joka vuosi, koska järjestelmät ja näihin liittyvät ohjelmistot muuttuvat koko ajan. Tällä tavalla pystytään varmistamaan se, että yrityksessä tehdään määrätietoisesti tietoturvallista työtä.

Tiedostojen ja kansioiden turvallisuusluokittelun tarpeesta tulee selvittää, onko yrityksellä sellaisia tiedostoja ja kansioita jotka vaatisivat tämän toimenpiteen. Uusien ohjelmien ja näiden kehitysversioiden parempaa testaamista palveluntarjoajien kanssa tulee kehittää. Tällä tavalla pystytään varmistamaan ohjelman oikea toiminta yrityksen verkossa.

Tietojärjestelmien tietoturvallisuuden keskeinen tekijä on sovellusten tietoturvallisuus. Monet kehitettävät sovellukset asennetaan siten, että niihin on päästään myös internetistä, jolloin tietoturvallisuuden hyvä toteuttaminen korostuu. Erillisiin tietoturvatuotteisiin, kuten palomuureihin ja nykyään esimerkiksi sovelluspalomuureihin, on jouduttu tukeutumaan muun muassa sovellusten heikon tietoturvallisuuden takia. Edellä mainittujen lisäksi on jouduttu järjestelmiin lisäämään tunkeutumisen havainnointi- ja estojärjestelmiä. Sovelluskehityksen tietoturvallisuudessa tulee ottaa huomioon kehitettävän sovelluksen tietoturvaominaisuudet, itse sovelluskehitysprosessin tietoturvallisuus sekä tietoturvatietoiset sovelluskehittäjät ja testaajat. Sovelluskehittäjiltä ja kehityskumppaneilta tulee vaatia tietoturva osaamisesta ja tietoturvallisuuden integroinnista sovelluskehitysprosesseissa. Tietoturvallisuus tulee ottaa huomioon koko sovelluksen elinkaaren ajan. Kaikki edellä mainitut vaatimukset eivät sovi kaikille sovelluksille. Kaikissa sovelluksissa ei ole välttämättä kirjautumispakkoa, mikä osaltaan vaikuttaa vaatimuksiin. (Sovelluskehityksen tietoturva-ohje 1/2013, 17. hakupäivä 8.2.2013.)

4.3 Toimintakäsikirja

Yrityksessä on käytössä toimintakäsikirja, joka sisältää joukon standardeja ja laatukäsikirjan osan. Toimintakäsikirjan tarkoituksena on ohjata yrityksen toimintaa siten, että se noudattaa standardien vaatimuksia ja yhdenmukaistaa työskentelytapoja. Nämä muutokset, joita tietoturvapolitiikka ja tietoturvasuunnitelma aiheuttavat, joudutaan myös kirjaamaan yrityksen toimintakäsikirjaan. Tässä työssä oli erittäin suurena apuna yrityksen laatuvastaava Matti Hippeläinen, jonka kanssa yhdessä katsoimme ne kohdat, jotka kirjataan toimintakäsikirjaan. Ne seikat, jotka joudutaan kirjaamaan toimintakäsikirjaan, ovat määrittelemättömiä tehtäviä ja vastuita sekä erilaisia yksittäisiä menettelyohjeita.

Toimintajärjestelmän tietoturvallisuuden työohjeessa kuvataan tietoturvakäytännöt ja -säännöt yleisellä tasolla. Tietoturvallisuuden työohje koostuu yksittäisistä toimintaohjeista, kuten sähköposti-, mobiililaite- ja VPN-ohjeista ja erilaisten ohjelmien käyttämiseen liittyvistä ohjeista sekä henkilöstön johtamiseen liittyvistä ohjeista. Ohjeet, joita toimintakäsikirjaan liittyy, voidaan jakaa kahteen kategoriaan: päivitettäviin ja uusiin ohjeisiin. Uusista ohjeista voidaan mainita esimerkiksi VPN-ohje ja

päivitettävistä ohjeista tietoturvallisuuden työohje. Nämä edellä luetellut asiat kootaan omiin käsikirjoihinsa taikka omiksi toimintajärjestelmän työohjeiksi. Toimintajärjestelmän näkökulmasta tämä tullaan toteuttamaan siten, että kun tietoturvatyöohje on päivitetty, ne lisätään kaikkien kolmen yhtiön johtoprosessin työohjeeksi, kuten muutkin mahdolliset tietoturvatyöhön liittyvät ohjeet.

Kirjassaan Yrityksen tietoturvakäsikirja Laaksonen ym. (2006, 112.) toteavat laadusta ja tietoturvallisuudesta seuraavaa: ”Laadunhallintajärjestelmän keskeiset asiat liittyvät johtamiseen, resurssienhallintaan, prosessienhallintaan sekä jatkuvaan mittaamiseen ja toiminnan kehittämiseen aivan vastaavasti kuin tietoturvallisuuden hallintajärjestelmissä. Laadun ja tietoturvallisuuden tavoitteiden asettaminen ja seuranta ovat samankaltaiset. Samoin tavat, joilla asiat viedään henkilöstön tietoisuuteen.”

5 YHTEENVETO

Opinnäytetyöni lähti liikkeelle Miilukankaalle tekemästäni tietoriskikartoituksesta, jossa yrityksen johto ja IT-osaston henkilöstö katsoivat tarpeelliseksi luoda yritykselle tietoturvapolitiikan ja tietoturvasuunnitelman. Opinnäytetyön tavoitteena oli laatia yritykselle toimiva tietoturvapolitiikka sekä ennen kaikkea hyödyllinen tietoturvasuunnitelma. Opinnäytetyön mielekkyyttä ja tarpeellisuutta nosti juuri se seikka, että yritys koki sen tarpeelliseksi ja tärkeäksi omalle organisaatiolleen. Opinnäytetyö toteutettiin kahdessa osassa. Ensin luotiin tietoturvapolitiikka keväällä 2012 ja toisessa vaiheessa tietoturvasuunnitelma syksyn 2012 ja kevään 2013 välisenä aikana.

Tietoturvapolitiikan ja tietoturvasuunnitelman tekemisessä oli mielenkiintoista ja haastavaa, kuinka saada kaikki tietoriskikartoituksessa tulleet puutteet korjattua. Tietoturvapolitiikkaa ja tietoturvasuunnitelmaa ei pystytä tekemään luotettavasti tai ainakaan kattavasti ilman kunnollista tietoriskien kartoitusta. Aloittaessani opinnäytetyön tekemisen viime keväänä, tästä aiheesta ei ollut montakaan opinnäytetöitä tehty, vaan jouduin keräämään haluamani aineiston ja taustatiedon monesta eri tietolähteestä.

Opinnäytetyötä tehdessä oppi paljon uutta tietoturvallisuuteen liittyvistä asioista. Kaikki eivät olleet pelkästään teknisiä vaan myös ihmisiin liittyviä asioita. Tietoturvasuunnitelman laatiminen vaati erittäin paljon taustatyötä ja eri lähteiden yhdistämistä yhdeksi kokonaisuudeksi. Työlle antoi lisähaastetta se seikka, että tietoturvasuunnitelmani rakenne poikkesi tavanomaisesta kahdeksan osa-alueen jaottelusta. Toisaalta tapa, jolla toteutin tietoturvapolitiikan ja tietoturvasuunnitelman, sopii erittäin hyvin pienille ja keskisuurille yrityksille.

Tavoitteeni opinnäytetyössä oli tehdä sellainen dokumentti, josta on hyötyä yrityksen liiketoiminnalle ja ennen kaikkea yrityksen henkilöstölle parantuneena tietoturvallisuutena. Omasta mielestäni työlle asetetut tavoitteet täyttyivät.

LÄHDELUETTELO

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

Johdon tietoturvaopas. 2011. Valtiovarainministeriö, hallinnon kehittämisosasto. Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2011. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20111207Johdon/Johdon_tietoturvaopas.pdf. Hakupäivä 5.1.2013.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Juva: WSOY

Laakso, M. 2010. Pk-yrityksen tietoturvasuunnitelman laatiminen. Turun ammattikorkeakoulu tietojenkäsittelyn koulutusohjelma. Opinnäytetyö.

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

Lehto, M. 2010. Tietoturvasuunnitelma Raahen Kaupungille. Oulun seudun ammattikorkeakoulu Raahen tekniikan ja talouden kampus. Opinnäytetyö.

Lokiohje. 2009. Valtiovarainministeriö, hallinnon kehittämisosasto. Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2009. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf. Hakupäivä 12.1.2013.

Miilukangas Ky kotisivu. http://www.miilukangas.fi/konserni/fi. Hakupäivä 24.4.2012.

Miilupipe Oy kotisivu. http://www.miilupipe.fi/. Hakupäivä 7.4.2013.

Miilupipe Oy toiminta-ajatus. http://www.miilupipe.fi/index.php?option=com_content&view=article&id=47&Itemid=27&lang=fi. Hakupäivä 7.4.2013.

Miilux Oy kotisivu. http://www.miilux.fi/. Hakupäivä 7.4.2013.

Miilux Oy suojausteräkset. http://www.miilux.fi/suojausterakset. Hakupäivä 7.4.2013.

Ruohonen, M. 2002. Tietoturva: Docendo Finland Oy.

Sovelluskehityksen tietoturva-ohje 2013. Valtiovarainministeriö, hallinnon kehittämisosasto. Valtionhallinnon tietoturvallisuuden johtoryhmä 1/2013. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20130207Sovell/VAHTI_1_Sovelluskehityksen_tietoturvaohje_NETTI.pdf. Hakupäivä 8.2.2013.

Teknisen ICT-ympäristön tietoturva-ohje. 2012. Valtiovarainministeriö, hallinnon kehittämisosasto. Valtionhallinnon tietoturvallisuuden johtoryhmä 3/2012. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf. Hakupäivä 3.12.2012.

Tietoturvallisuus. Valtionvarainministeriö. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp. Hakupäivä 24.5.2012.

Tärkein tekijä on ihminen. 2008. Valtiovarainministeriö, hallinnon kehittämisosasto. Valtionhallinnon tietoturvallisuuden johtoryhmä 2/2008. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf. Hakupäivä 10.11.2012.

LIITTEET

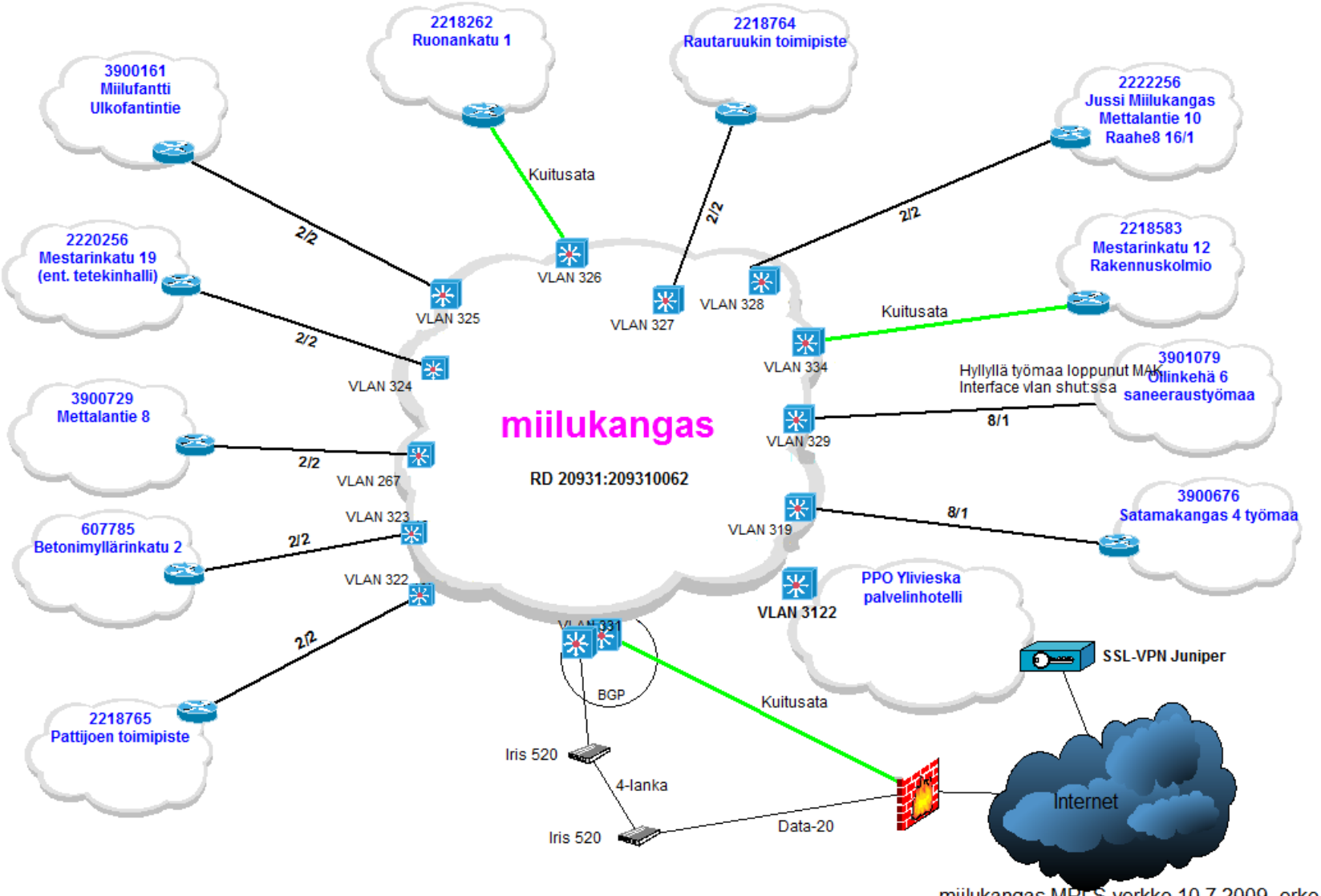
Liite 1 Miilukangas verkkokuva

Liite 2 Palvelimet ja palvelinsovellukset

Liite 3 Verkon rakenne ja accesspoint

Liite 4 Tietoturvapolitiikka

Liite 5 Etäkäyttötavan ja pääteistunnon ero (Teknisen ICT-ympäristön tietoturva-ohje 3/2012, 47. Hakupäivä 3.12.2012.)

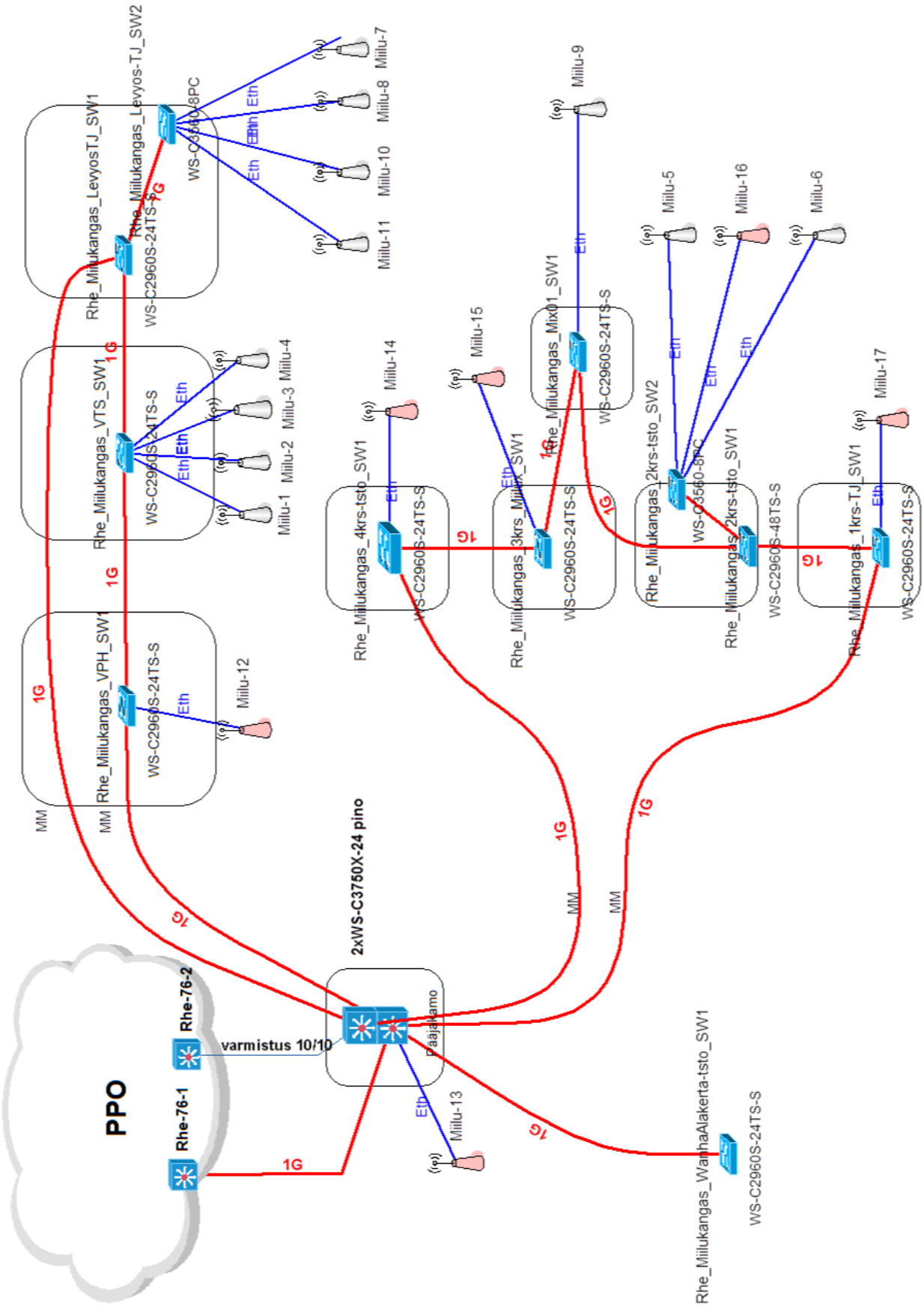


miilukangas MPLS-verkko 10.7.2009 -erko

LIITE 1

			Miilukankaan palvelimet				
palvelimen nimi/ Palvelut/ ohjelmat							
AD1, virusupdate.fi	F-Secure Policy Manager 10	WSUS	PD controller 1		Dedikaatti	Windows Server 2008	x64
AD2	Printer Spooler		PD controller 2		Virtuaali palvelin	Windows Server 2008	
DC1	File Server, vanha PDC				Dedikaatti	Windows Server 2003	32bit
DC2	File Server, vanha PDC			Nestix	Dedikaatti	Windows Server 2003	32bit
Sovellus	Sovellusten jakaminen	V10	Skannaus	Arrow maint	Dedikaatti	Windows Server 2008	x64
Terminal2	RDP - palvelin				Dedikaatti	Windows Server 2008	x64
RDP-Sovellukset	V10	JD	Rita	Arrow Maint			
MKY2	Tietokantapalvelin	Progress			Dedikaatti	Windows Server 2008	
MKY1	Tietokantapalvelin	MS SQL 2005	Oracle		Virtuaali palvelin	Windows Server 2003	32bit
Termsrv1	Vanha RDP - palvelin				Dedikaatti	Windows Server 2003	32bit
Tiedosto	Tiedostojen jakaminen				NAS	NAS	
M2	Miilux tilaustenkäsittely	PPO:n varmistus ym. palvelimet				Red Hat Linux	
Varmistus palvelimet							
Zilar	Työajanseuranta					Linux	
www.ppohosted.fi	Postipalvelin	Hosted exchange					

LIITE 2


PPO
Rhe-76-1
Rhe-76-2
varmistus 10/10
2xWS-C3750X-24 pino
Pääjakamo
1G
MM
Eth
Rhe_Miilukangas_LevyosTJ_SW1
Rhe_Miilukangas_Levyos-TJ_SW2
WS-C2960S-24TS-S
WS-C3560-8PC
Miilu-7
Miilu-8
Miilu-10
Miilu-11
Rhe_Miilukangas_VTS_SW1
Miilu-1
Miilu-2
Miilu-3
Miilu-4
Rhe_Miilukangas_VPH_SW1
Miilu-12
Rhe_Miilukangas_4krs-tsto_SW1
Miilu-14
Rhe_Miilukangas_3krs_MiiluX_SW1
Miilu-15
Rhe_Miilukangas_Mix01_SW1
Miilu-9
Rhe_Miilukangas_2krs-tsto_SW2
Miilu-5
Miilu-16
Miilu-6
Rhe_Miilukangas_2krs-tsto_SW1
WS-C2960S-48TS-S
Rhe_Miilukangas_1krs-TJ_SW1
Miilu-17
Miilu-13
Rhe_Miilukangas_WanhaAlakerta-tsto_SW1

LIITE 4

MIILUKANKAAN TIETOTURVAPOLITIIKKA

Miilukankaan toiminta ja palvelut ovat yhä enemmän riippuvaisia tietotekniikkapalveluiden saatavuudesta ja luotettavasta toiminnasta. Tietotekniikan hyödyntäminen ja tietoturvallisuuteen panostaminen ovat johdon strategisia päätöksiä, joilla vaikutetaan Miilukankaan toimintakykyyn merkittävällä tavalla.

Miilukankaan toiminta perustuu tietoon. Tiedon turvaaminen on oleellinen osa Miilukankaan toiminnan ja palveluiden laatua, kokonaisturvallisuutta ja Miilukankaalla tapahtuvaa päivittäistä tietojen käsittelyä. Tietoturvallisuuden hyvä hallinta edellyttää kaiken toiminnan jatkuvaa seurantaa, suunnittelua, varautumista uhkatilanteisiin, sovittujen toimintatapojen noudattamista, ohjeita, koulutusta ja viestintää. Tavoitteena on luoda ja ylläpitää luotettava ja turvallinen ympäristö henkilökunnan ja ylimmän johdon ja niiden piirissä toimivien sidosryhmien tietojen käsittelyyn.

Tietoturvapolitiikka on Miilukankaan ylimmän johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot Miilukankaalla. Tietoturvapolitiikka annetaan tiedoksi kaikille Miilukankaan työntekijöille tietoturvan perusasiakirjana. Politiikkaa tarkennetaan tietoturvasuunnitelmassa, tietojenkäsittelyn säännöissä, ohjeissa ja käytänteissä, joka koskee koko Miilukangasta.

1 Päämäärät ja tavoitteet

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Miilukankaan tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeät tiedot, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta sekä estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen. Tietojen turvallisuudesta on huolehdittava manuaalisesti ja tietotekniikan avulla tapahtuvassa tiedon käsittelyssä, tiedon kaikissa olomuodoissa ja tiedon koko elinkaaren ajan.

Tietoturvatyö on jatkuvaa kehittämistä, suunnittelua, toteuttamista ja seurantaa koko Miilukangas konsernissa. Sillä pyritään ehkäisemään sisäisistä ja ulkoisista tietoon kohdistuvista uhkista aiheutuvat vahingot tai rajoittamaan ne hyväksyttävälle tasolle sekä varautumaan poikkeamatilanteista

toipumiseen. Miilukangas varautuu tietoturvatoimillaan häiriö- ja poikkeustiloihin siten, että Miilukankaan toimintaa voidaan jatkaa mahdollisimman häiriöttömästi kaikissa olosuhteissa.

Miilukankaan kunkin yhtiön perusluonne ja tarpeet turvallisuuden tehostamiseen otetaan huomioon tietoturvan suunnittelussa ja toteutuksissa. Miilukankaan tietoturvallisuudesta huolehditaan Suomessa voimassa olevien kansallisten ja kansainvälisten tietoturvallisuutta koskevien säädösten mukaisesti.

2 Organisointi ja vastuut

Tietoturvallisuuden kehittäminen ja toteuttaminen on jatkuvaa laaja-alaista toimintaa, johon tarvitaan tiivistä ja rakentavaa yhteistyötä kaikkien yritykseen kuuluvien henkilöiden ja ryhmien kesken. Tietoturvallisuus toteutuu tehokkaimmin, kun toimintaa ohjaavat nimetyt vastuuhenkilöt ja kaikki tiedon käsittelijät huolehtivat oman tehtäväkenttänsä turvallisuudesta parhaalla mahdollisella tavalla.

Jokaisella Miilukankaan työntekijällä on siten vastuu tietoturvallisuuden toteuttamisesta ja valvonnasta ja velvollisuus noudattaa Miilukankaan antamia tietoturvallisuuteen liittyviä sääntöjä ja ohjeita.

Vastuu Miilukankaan toiminnasta ja myös sen turvallisuudesta on Miilukankaan omistajilla. Johtoryhmä hyväksyy Miilukankaan tietoturvapolitiikan sekä päättää Miilukankaan tietoturvallisuuden kehittämisen linjauksista, strategisesta ohjauksesta ja resursseista. Tietoturvallisuus on osa Miilukankaan kokonaisturvallisuutta. Johtoryhmä koordinoi tietoriskien hallintaa ja tietoturvallisuuden kehittämisen toimenpiteitä osana Miilukankaan kokonaisturvallisuuden kehittämistä.

Miilukankaan tietohallintopäällikkö vastaa kaikkien yhtiöiden tietoturvallisuudesta, ja tietoturvallisuuden kehittämistoimien resursoinnista ja toimeenpanosta Miilukankaalle hyväksyttyjen tietoturvaperiaatteiden ja tavoitteiden mukaisesti. Miilukankaan yhtiöt varautuvat toimintasuunnitelmissaan oman ympäristönsä tietoturvallisuuden toteuttamiseen yhdessä it-osaston kanssa.

Tietojärjestelmien omistajat vastaavat tietoturvallisuuden toteutumisesta järjestelmissä.

Tietohallintopäällikkö vastaa Miilukankaan tietoturvallisuuden toteuttamisesta. Tähän kuuluvat toiminnasta ja säädöksistä syntyneiden tarpeiden tunnistaminen, tietoriskien arvioinnin menettely ja tietoturvatietouden edistäminen, hallintajärjestelmään kuuluvat suunnitelmat ja niiden päivittäminen, toteutuneen toiminnan seuranta sekä tietoturvallisuuden tason raportointi johtoryhmälle. Tietohallintopäällikkö vastaa it-osaston hallinnoimien ja tuottamien järjestelmien ja palveluiden kuten tietoliikenneverkon sekä keskeisten järjestelmien ja verkkopalveluiden tietoturvan toteutumisesta.

Miilukankaan tietoturvallisuutta koskevat asiat eivät ole aktiivisen ulkoisen tiedottamisen aihe. Tietoturvallisuuteen liittyvästä tiedottamisesta vastaavat omistajat.

3 Toteutuskeinot

Miilukankaan tietojärjestelmien ja toimintojen tulee täyttää Miilukankaan tietoturvasuunnitelmassa kuvatut tietoturvallisuuden tavoitteet. Tietoturvallisuuden ylläpito ja kehittäminen on jatkuva prosessi, jossa käytetään hallinnollisia, fyysisiä ja tietoteknisiä ratkaisuja.

Tietoturvatoimien riittävä ja oikea taso varmistetaan tietoturvallisuuden riskienhallinnalla. Toimintaan, palveluihin ja järjestelmiin kohdistuva riskienarviointi toteutetaan säännöllisin väliajoin ja merkittävien muutosten yhteydessä. Tunnistettujen puutteiden korjaamiseen ja riskien pienentämiseen tarvittavat toimenpiteet kootaan tietoturvallisuuden kehittämisohjelmaksi. Korjaavien ja ehkäisevien toimenpiteiden suorittamisesta vastaavat tietojen ja järjestelmien omistajat. Miilukankaan yhtiöiden tietoturvatoteutukset kuvataan tarvittaessa erillisissä suunnitelmissa.

Miilukankaan yhtiöitä avustetaan tietoriskien hallinnassa menettelyohjeilla, suosituksilla sekä riskejä tunnistavalla ja ehkäisevällä välineistöllä. Henkilökunnalle tiedotetaan ja heille järjestetään koulutusta tietoturvallisuudesta ja heitä koskevista säännöistä ja suosituksista.

Toiminnan muutoksiin ja palveluiden tai järjestelmien hankintoihin sisällytetään tietoriskien arviointi ja tietoturvavaatimusten määrittely jo suunnitteluvaiheessa. Ennen hankkeen hyväksyntää valvotaan, että vaatimukset täyttyvät. Keskeisiin hankkeisiin otetaan tietoturvallisuuden asiantuntija mukaan alkuvaiheista lähtien. Tietojen turvallisesta käsittelystä solmitaan sopimukset myös Miilukankaan tietoja käsittelevien organisaatioiden sekä muiden yhteistyökumppanien kanssa.

Tietoturvallisuus huomioidaan Miilukankaan toimintaprosessien kehittämisessä ja toiminnan vuosisuunnittelussa.

4 Tietoturvallisuuden seuranta ja ongelmien käsittely

Tietoturvallisuudesta huolehtiminen edellyttää jatkuvaa seurantaa sekä turvallisuustason ja poikkeamien raportointia. Seurantaa toteutetaan teknisin ja hallinnollisin toimin. Tietohallintopäällikkö koordinoi tietoturvallisuuden seurantaa ja raportoi tietoturvallisuuden tasosta ja poikkeamista Miilukankaan johtoryhmälle. Tietohallintopäällikkö voi tarvittaessa käynnistää Miilukankaan tietojen käsittelyn turvallisuuteen liittyviä kartoituksia ja ryhtyä toimenpiteisiin havaittujen puutteiden korjaamiseksi.

Miilukankaan tietojenkäsittelyä ja tietojärjestelmien tietoturvallisuuden tasoa arvioidaan sisäisissä auditoinneissa, tarvittaessa myös ulkoista auditointia käyttäen, lain ja toiminnan vaatimusten mukaisuuden toteamiseksi sekä parannettavien kohteiden havaitsemiseksi.

Kunkin tietojärjestelmän, aineiston tai palvelun turvallisuuden valvonnan toteutumisesta on vastuussa sen omistaja. Jokaisen tiedonkäsittelijän velvollisuus on viipymättä ilmoittaa havaitsemistaan tietoturvallisuuden puutteista ja epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista tiedon tai tietojärjestelmän omistajalle tai tietohallintopäällikölle.

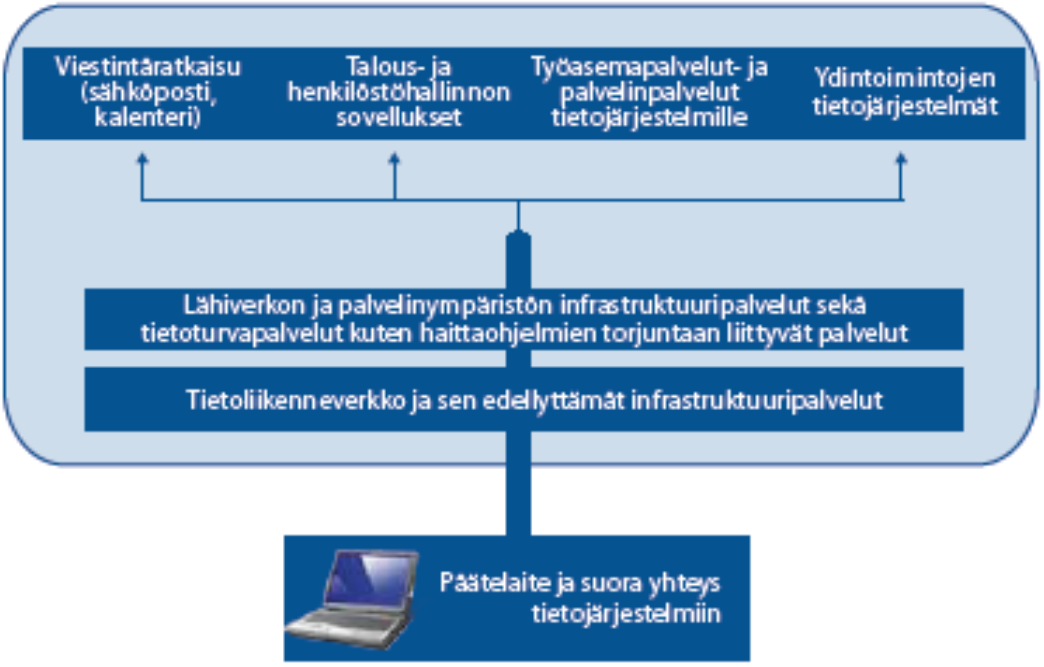
Jos tietojärjestelmästä tai tiedon hallintatavasta on uhkaa Miilukankaan tai sen sidosryhmän tietoturvallisuudelle, yhtiön omistajat voivat määrätä sille teknisiä tai hallinnollisia rajoituksia. Tietohallintopäällikkö vastaa tietoturvapoikkeamien jatkotoimenpiteistä. Vähäiset poikkeamat käsitellään it-osastolla. Yrityksen omistajat johtavat merkittävien poikkeamien sisäistä tutkintaa ja vastaavat yhteydenpidosta viranomaisiin.

Tietotekniikkarikkomusten seuraamuskäytännöstä määritellään erillisessä ohjeessa.

Hyväksynyt

Päiväys

KUVA 14. Perinteinen etäkäyttötapa muodostaa päätelaitteelta suoran yhteyden organisaation ICT-palveluihin. Päätelaitteen tietoturvallisuus on tärkeää, koska sen murtuminen saattaa mahdollistaa väärinkäyttäjälle suoran pääsyn organisaation palveluihin, tietovarastoihin tai pahimmillaan sisäverkkoon.



KUVA 15. Pääteistunto pienentää päätelaitteeseen kohdistuvia uhkia ja parantaa tietoturvallisuutta, koska siitä ei ole suoraa yhteyttä käytettäviin tietojärjestelmiin tai tietovarastoihin. Päätelaitteeseen siirretään pelkkä kuva virtualisoidulla työpöydällä tai päätepalvelimella toimivasta istunnosta.