TIETOVERKON DOKUMENTOINTI JA FYYSINEN TIETOTURVA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
syksy 2012
Tuukka Tikkunen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

TIKKUNEN, TUUKKA: Tietoverkon dokumentointi ja fyysinen tietoturva

Tietoliikennetekniikan opinnäytetyö, 35 sivua

Syksy 2012

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli yhtenäistää tietoverkon dokumentaatio Päijät-Hämeen keskussairaalalla ja ympäryskuntien terveysasemilla. Käytännön osuudessa tutkitaan, miten Päijät-Hämeen keskussairaalalla verkon dokumentointi on toteutettu, ja mietitään, voiko järjestelmää kehittää. Tutustutaan myös sairaalan fyysiseen tietoturvaan ja arvioidaan parannusmahdollisuuksia. Työn tavoite toteutui tietoverkon dokumentaation osalta.

Dokumentaatiolla tarkoitetaan yleisesti kaikkia ajan tasalla olevia sähköisiä tai fyysisiä asiakirjoja, joissa kuvaillaan tietojärjestelmän rakennetta ja sen eri osien toimintaa. Tarpeeksi yksityiskohtainen ja tiettyä sovittua rakennetta noudattava dokumentointi helpottaa kaikkea tietojärjestelmiin liittyvää toimintaa. Kun dokumentaatio on alusta pitäen pidetty selkeänä, nykyisen tietojärjestelmän uudistaminen ja laajentaminen helpottuvat.

Tietoturvallisuudella tarkoitetaan tietojenkäsittelyn toimivuuden, turvallisuuden, luottamuksellisuuden ja tulosten oikeellisuuden suojaamista kaikissa oloissa koko tiedon elinkaaren ajan. Yleisesti tietoturvallisuuden katsotaan koostuvan osista: eheys, luottamuksellisuus ja käytettävyys, joiden lisäksi mukaan on tullut myös kiistämättömyys ja pääsynvalvonta.

Päijät-Hämeen keskussairaalan tietoverkon dokumentaation osalta päädyttiin johtopäätökseen, jonka mukaan yritykseen olisi järkevää luoda ohjeistus, kuinka dokumentointi suoritetaan. Täten uuden työntekijän perehdyttäminen ja työnkierrätys helpottuvat. Yritys ei myöskään olisi riippuvainen yhden henkilön työpanoksesta.

Tietoturvan osalla suurimpana uhkana pidetään sitä että monesti tilat ja työkoneet jäävät lukitsematta. Olisikin tärkeää huolehtia, että tilat ovat valvottuja ja koneet lukkiutuisivat automaattisesti. Lisäksi on tärkeää huolehtia, että työntekijän atk-oikeudet rajoittuvat niihin, joita hän tarvitsee työtä tehdessään.

Avainsanat: dokumentaatio, fyysinen tietoturva

Lahti University of Applied Sciences
Faculty of Technology

TIKKUNEN, TUUKKA: Documentation of an information network and physical security

Bachelor's Thesis in Telecommunications Technology, 35 pages

Fall 2012

ABSTRACT

The objective of the thesis was to unify the documentation of the information network in Päijät-Hämeen keskussairaala (Päijät-Häme Central Hospital) and in the health centres of the neighbouring municipalities. In the study part it was analysed how the documentation of the information network of the hospital is executed and considered if the documentation can be improved. It also was analysed how the physical security is organized and how the physical security could be improved. The objective was fulfilled considering the documentation of the information network.

Documentation stands for every up-to-date record, physical or electric, which describe the structure of an information network and the functions of its components. Working with the information system is made easier if the documentation of the information network follows the appointed structure and if the documentation is detailed enough. Reforming and expanding an information network is also made easier when the documentation has been kept clear from the start.

Information security stands for securing functionality, securing safety and confidentiality of data processing, as well as securing the integrity of data for all of its life cycle. Information security is considered to consist of: confidentiality, integrity and availability with non-repudiation and access protection being added to the list later.

When considering the documentation of the information network of Päijät-Hämeen keskussairaala it would be rational to make instructions for documentation in the company. With instructions it would be easier for a new worker to get acquainted with the job, and circulation of workers would be made easier. Thus the company would not depend on the contribution of a single worker.

The biggest threat to physical security is when working spaces and computers are unlocked. It would be important to keep the working spaces supervised and the computers should lock themselves when not in use. Also it is important to limit workers data processing rights to only what he/she needs.

Keywords: documentation, physical security

SISÄLLYS

LYHENNELUETTELO

DVD	(Digital Versatile Disc) optinen datan tallennusväline.
IP-osoite	(Internet Protocol) numerosarja, joka yksilöi jokaisen Internet-verkkoon kytketyn tietokoneen.
MAC-osoite	(Media Access Control) verkkosovittimen ethernet-verkossa yksilöivä osoite.
WLAN	(Wireless Local Area Network) langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.

1 JOHDANTO

Vuoden 2007 alussa muodostui Päijät-Hämeen sosiaali- ja kuntayhtymä, joka toi lähikuntien terveydenhuollon keskussairaalan vastuulle. Nykyään on tärkeää, että yritysten tietoverkot ovat dokumentoitu selkeästi ja yhdenmukaisesti. Opinnäytetyön tavoitteena on tutkia miten Päijät-Hämeen keskussairaalan ja ympäryskuntien terveysasemien tietoverkko dokumentointi yhtenäistetään.

Opinnäytetyön teoriaosuudessa selvitetään, mitä tietoverkon dokumentoinnilla tarkoitetaan ja mihin dokumentointia tarvitaan. Toisena tavoitteena on selvittää, minkälainen rakenne hyvässä dokumentaatiossa on ja mitä on otettava huomioon.

Lisäksi selvitetään mitä tarkoitetaan yrityksen fyysisellä tietoturvalla, miten fyysinen tietoturva määritellään ja mistä fyysinen tietoturva koostuu. Käydään myös läpi lyhyesti tietoturvapolitiikkaa, tietoturvapolitiikan sisältöä, jatkuvuussuunnitelmia sekä tietoturvastrategiaa.

Tutkimusosuudessa luodaan katsaus Päijät-Hämeen keskussairaalan tietoverkon dokumentaation tämänhetkiseen tilaan ja mitä dokumentaation eteen tehtiin sairaalalla syksyllä 2007. Lisäksi pohditaan mitä dokumentaatiossa voisi parantaa sekä mitä on hyvä pitää mielessä dokumentaatiota tehdessä.

Tämän lisäksi tutkittiin Päijät-Hämeen keskussairaalan fyysisen tietoturvan tasoa. Tässä työssä tutkitaan mikä vaarantaa tietoturvan ja millä keinoin tietoturvaa voisi parantaa.

2 VERKON DOKUMENTOINTI

2.1 Dokumentoinnin määrittely

Dokumentiksi määritellään yleensä mikä tahansa tallennettu tieto. Tieto voi olla käsinkirjoitettua, mutta nykyään useammin dokumentit ovat tietokoneella tehtyjä ja tietokoneelle tallennettuja tiedostoja sisältäen tekstiä, taulukoita, kuvaajia ja kuvia. (Jaakohuhta 2000, 287 – 288.)

Yleisesti dokumentaatiolla tarkoitetaan kaikkia ajan tasalla olevia sähköisiä tai fyysisiä asiakirjoja, joissa kuvaillaan tietojärjestelmän rakennetta ja tietojärjestelmän eri osien toimintaa. Hallinnollisesti dokumentointi olisi järkevää antaa jonkun tai joidenkin määrättyjen henkilöiden vastuulle. (Jaakohuhta 2005, 325.)

Normaalisti dokumentointi tehdään kahdella eri periaatteella: loogisella kuvauksella ja fyysisellä kuvauksella. Loogisessa kuvauksessa järjestelmän looginen rakenne pyritään esittämään niin, että laitteiden ja niiden liitäntöjen suhde on helposti hahmotettavissa. Fyysisellä kuvauksella puolestaan kerrotaan, miten tietoverkko fyysisesti on rakennettu ja missä verkon komponentit (laitteet, kaapelit, jakamot jne.) sijaitsevat. (Jaakohuhta 2005, 326.)

2.2 Dokumentoinnin tarpeellisuus

Tietoliikenneverkkojen dokumentoinnin tärkeys on monesti aliarvioitua. On totta, että dokumentointi on usein kallista ja aikaa vievää, mutta pidemmän päälle on äärimmäisen tärkeää, että yrityksen verkon dokumentaatio on ajan tasalla. (Hakala 2006, 32.)

Tarpeeksi yksityiskohtainen ja tiettyä sovittua rakennetta noudattava dokumentointi helpottaa kaikkea tietojärjestelmiin liittyvää toimintaa, esimerkiksi

tietojenkäsittelyä, teknistä ylläpitoa ja tietohallintoa. Jos dokumentaatio on puutteellista, tästä johtuva selvitystyö ja ongelmien ratkonta viekin yleensä huomattavasti enemmän aikaa kuin riittävän dokumentaation luominen. (Hakala 2006, 32.)

Jotta vika-analysointi olisi tehokasta, vaatii tämä järjestelmien ylläpitäjiltä riittäviä tietoja järjestelmän rakenteesta ja toiminnasta. Tietojen riittävyys taas riippuu järjestelmän koosta, rakenteesta ja vian oletetusta haitasta organisaation toimintaan. On mahdollista määritellä, mitä vähintään tulisi olla olemassa, jotta vikojen hallinta ja korjaus olisi mahdollista. Näitä ovat esimerkiksi:

- järjestelmän rakenteesta ajan tasalla oleva dokumentaatio
- tiedot laitteiden ja ohjelmistojen maahantuojista ja toimittajista
- tieto varaosien saatavuudesta
- tieto palveluiden saatavuudesta
- perusvälineet välittömien vikojen tunnustamiseksi
- taitoa tunnistaa ja korjata vikoja.

(Jaakohuhta 2005, 324 – 325.)

Dokumentoinnilla voidaan nostaa järjestelmän palvelutasoa, koska hyvin dokumentoidussa ympäristössä

- vikaselvitykset lyhenevät
- palveluiden osto helpottuu
- suunnittelu helpottuu
- henkilöstöstä johtuvat riskit pienevät
- käytön turvallisuus paranee ja
- käyttöönotto helpottuu.

(Jaakohuhta 2005, 325.)

Kun dokumentointi on asianmukaisella tasolla, kaikenlaiset ongelmat ovat huomattavasti helpompi ratkaistavissa. Tutkimalla dokumentteja saadaan nopeasti rajattua alue tai tila, missä mahdollinen vika sijaitsee. Tämä on erityisen tärkeää

suurissa organisaatioissa, joissa kaapelointia voi olla kymmeniä kilometrejä per kiinteistö tai kiinteistöjä on useita (Jaakohuhta 2005, 333.)

Tilanteissa, joissa yritykselle ei ole järkevää pitää satunnaisesti tarvittavaa resurssia, kuten valokuitujen hitsauslaitteita, tietoliikennelaboratoriota, tietoverkkoasiantuntijaa, on ulkopuolisen resurssin käyttö huomattavasti järkevämpää. Tällöin palvelun saatavuuden takaamiseksi on tehtävä sopimus palveluntarjoajan kanssa, jossa sovitaan, mikä palvelu on kyseessä ja missä ajassa palvelu on saatava. (Jaakohuhta 2005, 333.)

Hyvin toteutetun dokumentaation avulla pienenee riski siitä, että kaikki tiedot nykyisestä tietoverkon rakenteesta menetetään esimerkiksi tapaturman sattuessa vastuuhenkilölle. Lisäksi jos on olemassa ohjeistus, kuinka olemassa olevaa verkon dokumentaatiota luetaan ja päivitetään, vähennetään samalla riippuvuutta henkilöstä joka yleensä on vastuussa dokumentaation ylläpidosta. (Järvinen 2002, 112.)

Myös käytön turvallisuus paranee dokumentoinnin myötä. Tiedetään tarkasti, missä seinän sisäiset sähkö- ja muut kaapeloinnit kulkevat, joten esimerkiksi seinään porattaessa ei satu vahinkoja. Saavuttaessa uuteen tai remontoituun tilaan dokumenteista selviää helposti, missä tarvittavat kytkentäpisteet sijaitsevat, jolloin koneiden ja työpisteiden sijoittelu on helppoa. (Hakala 2006, 34.)

2.3 Dokumenttien rakenne

Etukäteissuunnittelu (KUVIO 1) on tärkeää dokumenttien muotoa ja rakennetta harkittaessa. Muodon suunnittelua helpottavat seuraavat kysymykset:

- Mihin tarkoitukseen dokumentti on ensisijaisesti tarkoitettu?
- Asettavatko lainsäädäntö tai sopimukset vaatimuksia muodolle?
- Ketkä käyttävät / kenellä lupa käyttää dokumenttia?
- Kuinka usein dokumenttia luetaan?
- Kuinka usein dokumenttia muokataan?
- Tehdäänkö muutokset käsin vai päivittyykö dokumentti automaattisesti? (Hakala 2006, 34.)

Kun edellä mainittuihin kysymyksiin on löydetty sopiva vastaus, on sen jälkeen yleensä löydetty myös dokumentoitaville tiedoille sopiva muoto. Muodon valitsemisen jälkeen dokumentin sisäinen rakenne voidaan suunnitella huomioiden muodon asettamat rajoitukset. (Hakala 2006, 34.)

2.4 Dokumenttien tallennus ja versiointi

Vaikka dokumentointi olisikin asian mukainen, tämä ei sinällään vielä takaa dokumentoinnin toimivuutta. Dokumentit tulee tallentaa joko paperille tai sähköiseen muotoon, ja niiden on oltava nopeasti ja ainoastaan niiden henkilöiden käytettävissä, joilla niihin on lupa. Tämän lisäksi on tärkeää olla olemassa menetelmä joka varmistaa että käytössä on dokumentin viimeisin hyväksytty versio. Mahdollisuus tarkastella dokumentin edellisiä versioita on myös tärkeää. (Hakala 2006, 37).

Päijät-Hämeen keskussairaalalla käytössä oleva tietoverkon suunnitteluun käytettävä netViz -ohjelma esimerkiksi varmisti, että vain yhdellä henkilöllä voi olla sama projekti auki kerrallaan kirjoitusoikeudella. Muut voivat kyllä katsoa samaa

projektia, mutta vain lukuoikeudella. Täten ei ole mahdollista muokata samaa dokumenttia yhtä aikaa, mahdollisesti kirjoittaen toisen tekemän työn päälle.

2.5 Tallennuksen suunnittelu

Sähköiseen tallennukseen ja julkaisemiseen kannattaa laatia oma suunnitelmansa (kuvio 1). Lähtökohtana tulisi olla informaation helppo saatavuus ja toisaalta tiedon luottamuksellinen säilyttäminen. (Hakala 2006, 39.)

Sähköisien dokumenttien yleisin tallennus- ja julkaisutapa yrityksissä on tiedostopalvelimen jaettu hakemisto. Useasti kuitenkin suunnittelu saatetaan jättää huomioitta ja seurauksena hakemistorakenne ja kansiot ovat nimeämättömiä ja rakenne epämääräinen. Tästä on seurauksena järjestelmän käyttäjät eivät löydä etsimiään asiakirjoja. Ongelma on ratkaistavissa vastuuhenkilön nimeämisellä ja järkevän nimeämiskäytännön luomisella tiedostoille. (Hakala 2006, 40.)

Arkistoinnin ohjeistus	
Dokumentti	**Keskeinen sisältö**
Arkistointisuunnitelma	Dokumenttien ja tietojen luokitusjärjestelmän kuvaus Arkistoinnin vastuuhenkilöt Arkistointitilat Arkistointimenetelmät (tulostus, mikrofilmaus, magneettiset tai optiset mediat) Luokituksen mukaiset yleiset säilytysajat Luokituksen mukaiset yleiset hävittämiskäytännöt Periaatteet tutkimus- ja historiallisen materiaalin valitsemiseksi Arkistotapahtumien raportointimenetelmät Arkistoinnin kehittäminen ja arkistointisuunnitelman tarkistaminen
Arkistointiohje	Dokumenttityyppi Dokumentin omistava prosessi Dokumentin arkistoinnista vastaavat henkilöt Arkistointipaikka (fyysinen tila tai tietojärjestelmä) Tallennustapa (media) Säilytysaika Hävittämistapa Arkistointitapahtumista raportointi

KUVIO 1. Sähköisten dokumenttien tallennus- ja julkaisuohjeet (Hakala 2006, 40)

2.6 Versioinnin suunnittelu

Jotta voidaan olla varmoja, että käytetään tiedostosta voimassa olevaa kuvausta tai että tarkasteltavat tiedot ovat ajan tasalla, dokumentit on versioitava. Versioinnilla on myös merkittävä osuus laatujärjestelmien jäljitettävyysvaatimuksen ylläpidossa. Tällöin vertaamalla dokumenttien eri versioita voidaan selvittää, mitä muutoksia organisaation toiminnassa on tapahtunut, milloin muutos on tehty ja kuka sen on tehnyt. Organisaatiolle on erityisen tärkeää tietää, mitä muutoksia on tehty ja mitkä ovat olleet niihin johtaneet syyt. (Hakala 2006, 42.)

Erityisesti tietojärjestelmädokumenteissa on mahdollista, että samanaikaisesti noudatetaan useita eri versioita. Esimerkiksi tietokantapalvelimen

asetusdokumenteista saatetaan samanaikaisesti noudattaa useita eri versioita. Tällöin on pidettävä huolta, siitä että myös vanhemmat asetusdokumenttiversiot ovat saatavilla ja että tutkimalla versiohistoriaa nähdään selkeästi, mitä versioita saadaan käyttää missäkin käyttöjärjestelmässä. (Hakala 2006, 42.)

2.7 Dokumentoinnin tarkkuus

Kun dokumentointia aloitetaan, suurin virhe on liian suuri dokumentointitarkkuus, josta seurauksena saattaa olla, että dokumentointi jää alun jälkeen ylläpitämättä. Lisäämällä yhden tason dokumentointitarkkuuteen dokumentoitavan materiaalin määrä kasvaa moninkertaiseksi. (Jaakohuhta 2005, 326.)

Onkin välttämätöntä dokumentoida vain ne verkon osat, joiden vikaantuminen voi aiheuttaa merkittäviä vahinkoja. Dokumentoinnissa tarvitaan eräitä verkon kannalta merkittäviä perustietoja, joita ovat mm.

- laitteen MAC-osoite
- laitteen IP-osoite
- tietoverkkolaitteiden käyttöjärjestelmäversiot
- palvelimien ja työasemien käyttöjärjestelmäversiot
- sovellusohjelmien versiot
- laitetyyppi ja merkki ja mahdollisesti versiot
- muut tiedot, joita tarvitaan suunnittelua tai laiteinventointia varten

(Jaakohuhta 2005, 326.)

3 FYYSINEN TIETOTURVA

3.1 Fyysinen tietoturva

Tietoturvallisuudella tarkoitetaan tietojenkäsittelyn toimivuuden, turvallisuuden, luottamuksellisuuden ja tulosten oikeellisuuden suojaamista kaikissa oloissa koko tiedon elinkaaren ajan. Tavoitteen saavuttaminen edellyttää koko tietojenkäsittely-ympäristön huomioimista. (Paananen 2003, 418.)

Tietoturvallisuus voidaan jakaa seuraaviin osa-alueisiin (Paananen 2003, 418 – 419.)

- Hallinnollinen turvallisuus: tietoturvallisuuden linjaukset, niiden johtaminen, toiminnan organisointi, vastuiden jakaminen ym.
- Henkilöturvallisuus: työntekijöiden ohjeistus, koulutus, henkilöiden aiheuttamat tahattomat vahingot ja tahalliset sabotaasit; uusien työntekijöiden taustojen tarkistus rekrytoinnin yhteydessä, perehdytyskoulutus sekä salassapito- ja kilpailukieltosopimukset
- Käyttötoimintojen turvallisuus: tietokoneiden ja verkon aktiivilaitteiden päivittäiseen käyttöön liittyvien asioiden turvaaminen (mm. laitteiden ylläpito, käyttö, huolto, valvonta)
- Laitteistoturvallisuus: tietokoneiden ja verkon aktiivilaitteiden toiminnan varmistaminen ja varautuminen esimerkiksi sähkönsyötön katkoksiin
- Ohjelmistoturvallisuus: käytettyjen tietokoneohjelmien suojaaminen, lisenssien hallinta ja ohjelmien rekisteröinti; ohjelmien luvallisuuden varmistaminen ja ohjelmien laittoman kopioinnin ja käytön estäminen
- Tietoaineistoturvallisuus: levyjen, levykkeiden, nauhojen ja tulosteiden turvallinen käsittely niin, etteivät luottamukselliset tiedot joudu vääriin käsiin tiedon itsensä tai sen tallennusmedian elinkaaren loppuessa
- Tietojenkäsittelyn turvallisuus: laitteiden käyttöön ja operointiin liittyvät työtehtävät ja niiden varmistaminen poikkeustilanteissa
- Tietoliikenteen turvallisuus: tietoliikenteen jatkuvuuden turvaaminen, siirrettävän tiedon salaaminen ja sen eheyden varmistaminen

- Toimitilaturvallisuus: toimitilojen fyysinen suojaus (kuten kulunvalvonta, murtosuojaus, lukitukset sekä suojaus sähkömagneettista hajasäteilyä vastaan), jonka tavoitteena on estää laitteiden varastaminen, palo- ja vesivahingot, salaa tapahtuva televalvonta sekä asiattomien henkilöiden pääsy yrityksen tiloihin
- Yksityisyyden suoja: toiminnassa käytettävien henkilötietojen kerääminen ja suojaaminen niin, että niitä käsitellään vain asianmukaisiin tarkoituksiin ja henkilötietolain vaatimuksia noudattaen

3.2 Tietoturvallisuuden määritelmä

Kirjallisuudessa ja eri organisaatioiden julkaisemissa tietoturvastandardeissa tietoturvallisuuden määritelmä poikkeaa hieman toisistaan. Kaikki lähtevät kuitenkin samasta perusajatuksesta: organisaation tärkein omaisuus on tieto, joka halutaan pitää luetettavana, nopeasti, oikeassa muodossa ja ainoastaan oikeiden henkilöiden saatavilla. (Hakala 2006, 4.)

Tiedosta lähteviä määritelmiä on yleensä laajennettu sisältämään myös tietojen käsittelyssä tarvittavat laitteistot tietoliikennejärjestelmineen. Näissä määritelmissä huomiota on useasti kiinnitetty myös tietoliikennejärjestelmäinvestointien suojaamiseen niiltä luvattomilta käyttäjiltä, jotka sinänsä eivät ole kiinnostuneita organisaatiolla olevista tiedoista. (Hakala 2006, 4.)

Toinen yleinen määritelmän laajennus on luonteeltaan juridinen. Tietojärjestelmän halutaan myös luotettavasti ja aukottomasti kertovan, ketkä ovat luoneet siellä olevat tiedot. Tämä on ensiarvoisen tärkeää sähköisessä kaupankäynnissä ja julkisyhteisöjen sähköisessä asioinnissa. (Hakala 2006, 4.)

3.3 Klassinen tiedon arvoon perustuva määritelmä

3.3.1 CIA

Perinteisessä tiedon arvoon perustuvassa määritelmässä tietoturvallisuus koostuu kolmesta perustekijästä, jotka ovat

- luottamuksellisuus (Confidentiality)
- eheys (Integrity)
- saatavuus (Availability)

(Paananen 2003, 419).

Osa-alueet käsittelevät tietoa eri muodoissaan, kuten tiedostoina, www-sivuina, tiedonsiirtona. Tietoturvalla tarkoitetaankin tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista. (Järvinen 2002, 22)

3.3.2 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan sitä, että tietojärjestelmän tiedot ovat ainoastaan niiden henkilöiden käytettävissä ja muokattavissa joilla on niihin oikeus. Jotta valtuutetut käyttäjät voitaisiin tunnista, heidät täytyy ensin todentaa. (Järvinen 2002, 22.)

Luottamuksellisuuden ylläpitoon pyritään suojaamalla tietojärjestelmien laitteet ja tietovarastot käyttäjätunnuksin ja salasanoin. Erilaiset salakirjoitusmenetelmät soveltuvat myös arkaluontoisen tai erityisen arvokkaiden tietojen suojaamiseen. (Hakala 2006, 4.)

Saatavuus

Saatavuus tarkoittaa sitä, että tiedot saadaan tietojärjestelmästä oikeassa muodossa ja riittävän nopeasti. Ylläpidettäessä käytettävyyttä on huolehdittava siitä, että tieto- ja tietoliikennejärjestelmien laitteet ovat riittävän tehokkaita ja että

käytettävät ohjelmistot soveltuvat mahdollisimman hyvin järjestelmään tallennettujen tietojen käsittelyyn. (Hakala 2006, 4.)

Tietojen ja palveluiden saatavuus liittyy tietojärjestelmien toiminnan turvaamiseen. Esimerkiksi verkkoyhteyksien tulee toimia ja koneiden tulisi pyöriä aina silloin, kun tietoa tai palvelua halutaan käyttää. Verkkopalvelussa tämä tarkoittaa yleensä 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. Toimistojärjestelmissä riittää yleensä arkipäivien työtunnit, jolloin viikonloppuja ja öitä hyödynnetään päivitysten ajamiseen ja varmuuskopiointiin. (Järvinen 2002, 24.)

Lisäksi pyrkimyksenä on automatisoida tiedon jalostus mahdollisimman pitkälle. Käyttäjän tulisi saada haluamansa tiedot järjestelmästä itselleen sopivassa muodossa, kuten valmiina raportteina tai yhteenvetoina. (Hakala 2006, 4 – 5.)

Tiedon saatavuuteen saattaa myös liittyä yllättäviäkin ongelmia. Esimerkiksi jos yritys tai käyttäjä tarvitsee tiedostoja, jotka on tuotettu yli 10 vuotta sitten. Tällöinkin tiedostot saattavat olla varmistettu ja arkistoitu huolella, mutta tiedostojen avaamiseen käytetyt sovellukset eivät enää olekaan tallella, tai ohjelmat eivät toimi enää nykykoneissa. (Järvinen 2002, 24.)

3.3.4 Eheys

Puhuttaessa eheydestä tarkoitetaan tällä laajasti ymmärrettynä, sitä että tietojärjestelmän sisältämät ovat paikkaansa pitäviä eivätkä sisällä tahallisia tai tahattomia virheitä. Eheyteen pyritään pääasiassa ohjelmointiteknisin ratkaisuin. (Hakala 2006, 5.)

Tiedon eheydellä tarkoitetaan myös sitä, ettei minkään ulkopuolisen tahon ole mahdollista päästä luvatta muuttamaan tiedon sisältöä. Muutoksiksi luetaan esimerkiksi tiedostojen poistamista tai niihin muutoksien tekemistä. Esimerkiksi virukset rikkovat ohjelma- tai dokumenttitiedostojen eheyden tarttuessaan niihin. (Järvinen 2002, 23.)

Sovelluksiin voidaan esimerkiksi ohjelmoida erilaisia syöttörajoitteita tai syötteen tarkistuksia ja tallennus- ja tiedonsiirto-operaatioihin varmistussummia tai tiivisteitä. Laitteistotasolla pyritään estämään virheet käyttämällä esimerkiksi virheenkorjaavia muisteja tai väyliä. Tietoliikenneratkaisuissa suositaan usein virheen tunnistus- ja korjausmekanismeilla varustettuja protokollia ja laitteita. Useimmat salakirjoitusmenetelmät ja -tuotteet soveltuvat myös eheyden ylläpitoon. (Hakala 2006, 5).

Laajennettu tietoturvallisuuden määritelmä

Nykyään klassista määritelmää pidetään riittämättömänä. Tämä johtuu siitä, ettei klassinen määritelmä huomioi riittävästi tiedon tuottajan tai omistajan identiteettiä eikä huomioi itse laitteistojen tai tieto- ja tietoliikennejärjestelmien arvoa. Yleisin laajennettu määritelmä käsittää viisi osatekijää (KUVIO 2):

- luottamuksellisuus
- käytettävyys
- eheys

- kiistämättömyys
- pääsynvalvonta

3.4.1 Kiistämättömyys

Kiistämättömyydellä tarkoitetaan tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävän henkilön tiedot. Voidaan määrittää kaksi syytä, miksi kiistämättömyyteen pyritään: tiedon alkuperä halutaan varmistaa tai olemassa olevien tietojen luvaton käyttö niissä tilanteissa, joissa tietojärjestelmän omistaja joutuu harkitsemaan oikeudellisia toimia järjestelmän käyttäjää vastaan. (Hakala 2006, 5.)

Kiistämättömyyden tarve tulee myös vastaan sähköisessä kaupankäynnissä. Tällöin ostotapahtuman vaiheet, tilauksen tekeminen, tilauksen vastaanotto ja tuotteen toimittaminen, pitää voida sitovasti todistaa. (Järvinen 2002, 28.)

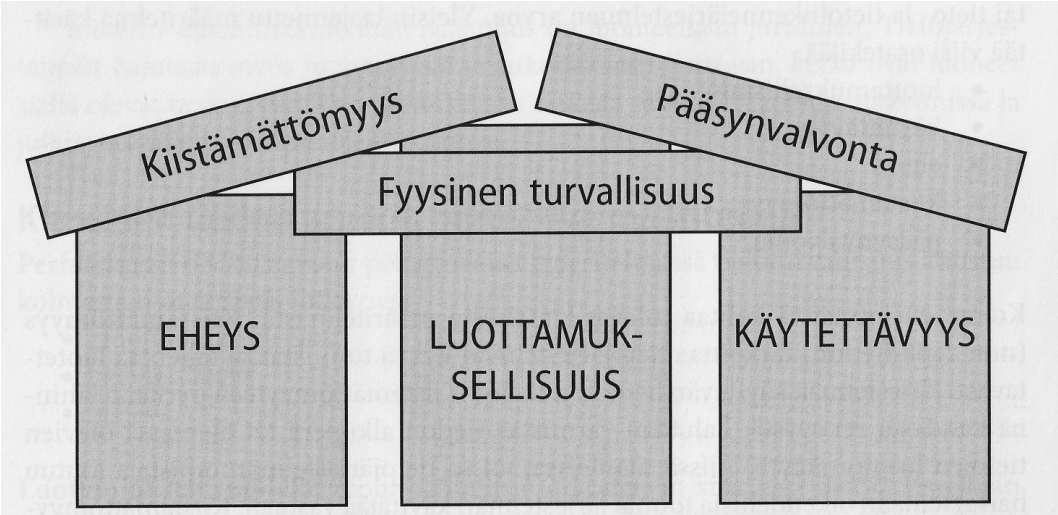
Kiistämättömyyteen pyritään käyttämällä salausmenetelmiin liittyviä tunnistusmekanismeja tai biometrisiä tunnisteita. Käyttäjäntunnistusmenetelmistä yleisimmät hyödyntävät salaustekniikoita, käyttävät älykortteja tai muita pieniä mukana kuljetettavia laitteita. Näihin laitteisiin on tallennettu käyttäjän henkilötiedot sekä rajallisen ajan voimassa oleva käyttölupa, sertifikaatti. Biometriseen tunnistukseen käytetään mm. sormenjälki- tai silmänpohjantunnistuslaitteita. (Hakala 2006, 5.)

3.4.2 Pääsynvalvonta

Pääsynvalvonnalla tarkoitetaan niitä menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Varsinaisiin tietoihin pääsyn rajoittaminen kuuluu luottamuksellisuuden ylläpitoon. Organisaatiolle on kuitenkin tärkeää estää ulkopuolisia tai omaa henkilökuntaansa käyttämästä sen laitteita tai tietoliikenneyhteyksiä omiin tarkoituksiinsa. Luvattomat järjestelmän käyttäjät kuormittavat laitteita sekä tietoliikenneverkkoja ja heikentävät näin käytettävyyttä. Luvaton käyttö saattaa myös altistaa organisaation tietojärjestelmän haittaohjelmien leviämiselle, mikä puolestaan johtaa eheys- ja luottamuksellisuusongelmiin. (Hakala 2006, 5 – 6.)

Käytön seuranta onkin tärkeä osa pääsynvalvontaa. Tietojärjestelmän ylläpitäjien tulisi pitää kirjaa käyttäjistä, jotka ovat avanneet tai muokanneet tiedostoja, käyttäneet ohjelmia ja ylipäätänsä kirjautuneet sisään. Näistä tapahtumista tehdyistä lokitiedoista hyödytään, kun jäljitetään vahingossa tai tarkoituksella tehtyjä tietoturvarikkomuksia. (Järvinen 2002, 27.)

Pääsynvalvontaan on jouduttu kiinnittämään entistä suurempaa huomiota langattomien verkkojen yleistyttyä. Ulkopuoliset henkilöt pyrkivät käyttämään langattomia verkkoja omaan Internet-liikenteeseensä. Tietokonekaupoista ja postimyynnistä on saatavissa runsaasti laitteita ja ohjelmia, joiden avulla voidaan hakea langattomia verkkoja ja tarvittaessa murtaa niissä käytetyt yksinkertaiset salaukset verkkoon pääsemiseksi. (Hakala 2006, 6.)



KUVIO 2. Tietoturvallisuuden osatekijät (Hakala 2006, 6)

3.5 Tietoturvapolitiikka

3.5.1 Tietoturvapolitiikan määrittely

Tietoturvapolitiikka on johdon hyväksymä näkemys tietoturvan päämääristä, periaatteista ja toteuttamisesta (KUVIO 3). Tietoturvapolitiikka on organisaation tietoturvan peruskivi. Tietoturvapolitiikka voi olla muutaman sivun tiivistetty kuvaus tietoturvaan liittyvistä asioista, ja se voi olla nähtävissä vaikkapa yrityksen nettisivulla. Tällöin tietoturvapolitiikka rinnastetaan mm. ympäristö- ja henkilöstöpolitiikkaan. Politiikka kuvaa asiakkaille, työntekijöille ja sijoittajille, mitkä ovat yrityksen arvot, näkemykset ja tavoitteet tällä alueella. Politiikka ei sisällä yksityiskohtaisia toimintaohjeita esimerkiksi varmuuskopioinnista, virustentorjunnasta tai salasanapolitiikasta. Nämä kuvataan yksityiskohtaisissa toimintaohjeissa, jotka ovat vain niitä työssään tarvitsevien henkilöiden saatavilla. (Järvinen 2002, 113.)

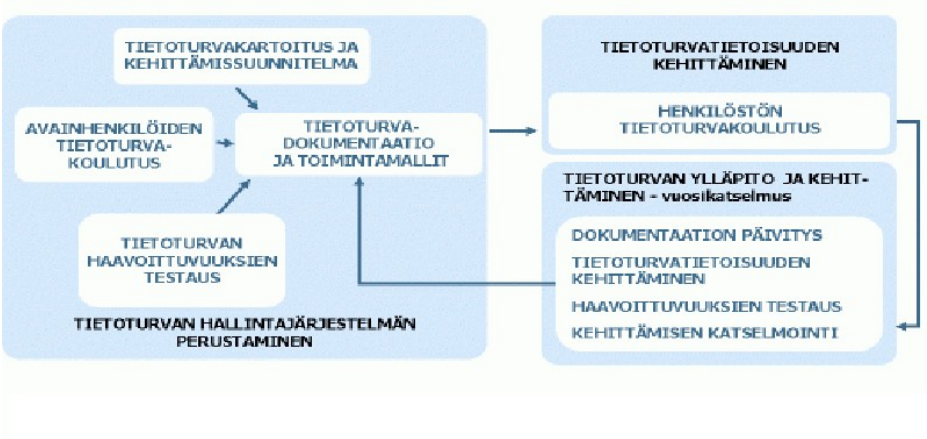
Tietoturvapolitiikka laaditaan kirjalliseen muotoon ja tietoturvapolitiikan tarkoituksena on toimia keskipitkän (n. 5 vuotta) ja pitkän (n. 10 vuotta) aikavälin

ohjeena tietojärjestelmän suunnittelijoille ja eri liiketoimintaprosessien vastuullisille esimiehille. Koska tietoturvapolitiikka laaditaan tekniikassa ja toiminnoissa tapahtuviin muutoksiin nähden huomattavan pitkälle ajanjaksolle, ei ole tarkoituksena sisällyttää siihen tietoturvallisuuden toteutukseen liittyviä yksityiskohtia. (Hakala 2006, 7.)

3.5.2 Tietoturvapolitiikan sisältö

Tietoturvapolitiikka on tärkein organisaation tietoturvakäytäntöjä ja tietoturvallisuusprosessia ohjaava dokumentti. Hyvä tietoturvapolitiikka sisältää seuraavat osa-alueet (KUVIO 4):

- organisaation oman tietoturvallisuuden määritelmän, turvallisuuden keskeiset kohteet, laajuuden sekä turvallisuuden tärkeyden organisaation toiminnalle
- johdon tahdonilmaus ja tuki tietoturvan tavoitteiden saavuttamiseksi ja siihen liittyvien periaatteiden noudattamiseksi osana organisaation liiketoimintastrategiaa
- rakenteet, joiden avulla tietoturvallisuuteen pyritään, erityisesti ne rakenteet, joilla riskit tunnistetaan
- yhteenveto tietoturvakäytännöistä, noudatettavista standardeista ja yleisperiaatteista
- yhteenveto lainsäädännön, sopimusten ja kauppatapojen asettamista vaatimuksista
- yhteenveto turvallisuusajattelun edistämistoimista ja turvallisuuskoulutuksen järjestämisestä
- kuvaus liiketoiminnan jatkuvuuden hallinnasta ja sen liittymisestä tietoturvallisuuteen
- määritelmät tietoturvallisuuteen liittyvistä vastuualueista ja turvallisuuteen vaikuttavien tapahtumien raportoinnista
- käytännöt ja seuraukset turvallisuuspolitiikan rikkomuksista
- luettelo politiikkaa tarkentavista tietoturvaohjeista ja standardeista (Hakala 2006, 9.)



KUVIO 3. Tietoturvan hallinta (Navicre 2007)

Tietoturvapolitiikka pitäisi kirjoittaa aina sellaiseen muotoon, että myös muut kuin tietojenkäsittelyn tai hallinnon ammattilaiset voivat ymmärtää sen sisällön. Dokumentti on luonteeltaan julkinen ja on tarkoitettu koko organisaation henkilöstölle. Lisäksi tietoturvapolitiikkadokumenttia jaetaan asiakkaille ja yhteistyökumppaneille osoituksena organisaation vakavasta pyrkimyksestä suojata omat ja sidosryhmiensä tiedot. (Hakala 2006, 9.)

3.5.3 Riskikartoitus

Ennen kuin tietoturvapolitiikka luodaan, on määriteltävä, mitä varsinaisesti pyritään turvaamaan ja mitkä ovat tärkeimmät uhkat. Yritystoiminnan kannalta keskeistä on selvittää yrityksen tärkeimmät prosessit ja pyrkiä turvaamaan niissä käytettävän tietotekniikan toiminta. Riskikartoituksessa pyritään kuvittelemaan ennakolta kaikki mahdolliset uhkat: mitä ne ovat, miten ne voivat toteutua ja mikä on vahingosta seuraava kustannus. Riskin matemaattinen kaava on seuraava:

riski = vahingon kustannukset * vahingon todennäköisyys
(Järvinen 2002, 114.)

Riskejä vastaan voidaan varautua hankkimalla turvalaitteita, suojaohjelmia tai vakuuttamalla toiminta. Pienemmät riskit saatetaan katsoa niin vähäpätöisiksi, että riskit ovat mielekästä kantaa itse. Varautumisen on oltava järkevässä suhteessa kustannuksiin. Jos tarkasteltava tieto ei ole luottamuksellista ja on helppo luoda

tarvittaessa uudelleen, tiedon suojaamiseen ei kannata käyttää paljon rahaa. Resurssit kannattaa kohdistaa riskeihin, joiden toteutuminen tietää suuria kustannuksia (Paananen 2003, 423.)

3.5.4 Jatkuvuussuunnitelma

Tietotekniikasta riippuvan organisaation on laadittava jatkuvuussuunnitelma, jossa kuvataan tietotekniikan ja tietoliikenneyhteyksien varautuminen erilaisiin häiriöihin. Suunnitelman keskeinen osa on toipumissuunnitelma, joka määrittelee, miten varajärjestelmät ja -yhteydet otetaan käyttöön. (Paananen 2003, 423.)

Kehittynyt tekniikka antaa monenlaisia mahdollisuuksia toiminnan turvaamiseen. Nopeiden verkkoyhteyksien ansiosta tärkeimmät tietojärjestelmät voidaan kahdentaa ja sijoittaa satojen kilometrien päähän toisistaan. Näin vakavakaan maanjäristys, tulipalo tai terroriteko ei pääse keskeyttämään toimintaa lopullisesti, sillä varajärjestelmä voidaan ottaa käyttöön hyvinkin nopeasti ja sen tiedot ovat aina ajan tasalla. (Järvinen 2002, 114.)

3.5.5 Tietoturvastrategia

Riskien kartoittamisen ja vallitsevan tietoturvan tason selvittämisen jälkeen laaditaan tietoturvastrategia. Strategiassa kuvataan, miten yritys aikoo kehittää tietoturvaansa, mitä tavoitteita yritys asettaa turvallisuudelle ja millä keinoin turvataso aiotaan saavuttaa. Jotta tavoitteisiin todella päästäisiin, tietoturvastrategian tulee sisältää aikataulut ja vastuuhenkilöt havaittujen puuteiden korjaamiselle. (Paananen 2003, 424.)

Tietoturvastrategiaan kuuluvat mm. seuraavat:

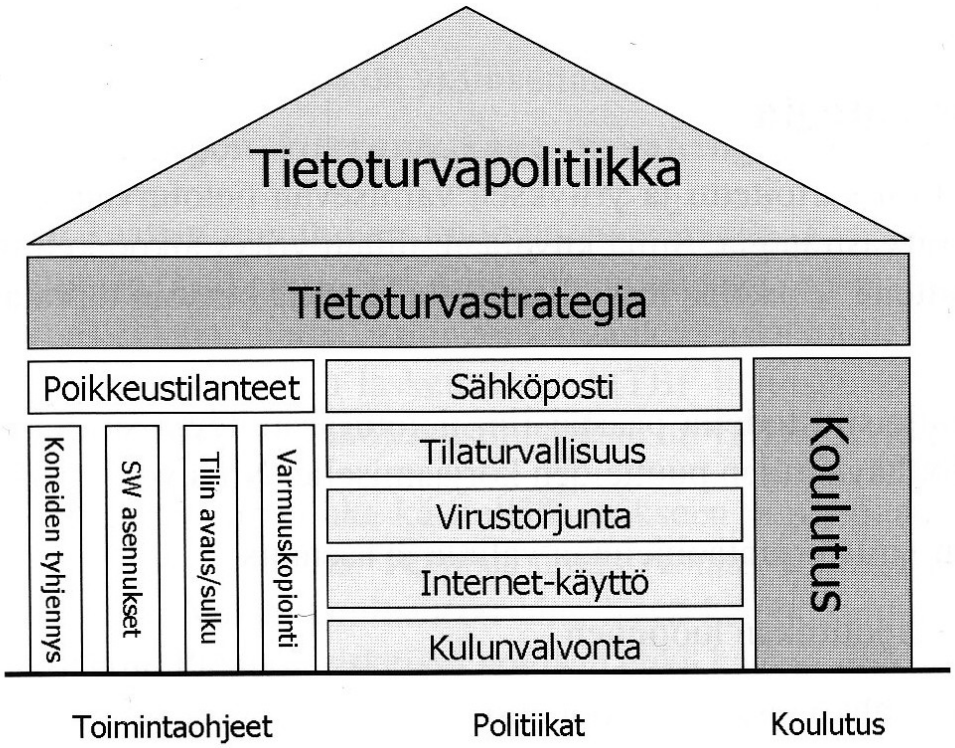
- uuden virustorjuntaohjelman valinta ja asennus

- salasanapolitiikan luominen
- salatun sähköpostin käyttöönotto
- henkilöstön tietoturvakoulutuksen käynnistäminen
- palvelinohjelmien päivitysten varmistaminen
  (Järvinen 2002, 115).

3.5.6 Toimintaohjeet

Tietoturvan alimman tason muodostavat yksittäiset toimintaohjeet. Jotta tietoturva on ja pysyy riittävän hyvällä tasolla on luotava yhteisiä pelisääntöjä, järjestettäväkoulutusta ja poikkeustilanteisiin varautumista sekä jaettava yksityiskohtaisia toimintaohjeita. (Paananen 2003, 424.)

Ohjeissa kuvataan, miten yksittäiset tehtävät suoritetaan. Uudenkäyttäjän perustaminen, vanhan poistaminen työsuhteen päättyessä, ohjelmien turvapäivitysten asentaminen ja virustentorjunnan päivittäminen ovat esimerkkejä toimintaohjeilla kuvattavista tehtävistä. Nimetty vastuuhenkilö huolehtii siitä, että ohjeet pysyvät ajan tasalla vaikka laite- ja ohjelmaympäristö muuttuvat. (Järvinen 2002, 115.)



KUVIO 4. Yrityksen tietoturva (Järvinen 2002, 116)

3.6 Tietoturvaohjeita

Kun työpaikalla käytetään tietokonetta, on syytä muistaa muutamia sääntöjä. Säännöt koskevat sekä omaa tietokonetta että palveluita, joita käytetään verkon kautta. Nämä säännöt olisi hyvä olla tulostettuna esimerkiksi työpisteen seinällä.

- Käyttäjä vastaa omasta koneestaan.
- Koneelle kirjaudutaan ainoastaan omilla tunnuksilla.
- Asiaton pääsy tietojärjestelmiin estetään lukitsemalla kone aina, kun poistutaan työtiloista. Voidaan käyttää myös salasanallista näytönsäästäjää.
- Muista uloskirjautuminen ohjelmista ja koneelta.
- Laitteiden ja ohjelmien asentamista ja päivittämistä voi tehdä vain tietohallinto.

- Jos kovalevy tai muu tallennusmedia rikkoontuu, viedään viallinen tallennusmedia tietohallintoon, joka huolehtii tallennusmedian asianmukaisesta hävittämisestä.

(Käyttäjän tietoturvaohje 2003.)

Kaikki tietojärjestelmät vaativat käyttöoikeuden. Käyttöoikeus on henkilökohtainen, ja se on yhdistetty työntekijän henkilöllisyyteen ja työtehtävään.

- Henkilökohtaisia tunnuksia tai salasanoja ei tule antaa toisen henkilön käyttöön, ei edes atk-henkilöstölle. Tiedusteluihin on syytä suhtautua epäilevästi.
- Salasana on vaihdettava riittävän usein.
- On syytä pitää huolta että salasanat ovat riittävän monimutkaisia.
- Salasanoja ei pidä kirjoittaa muistiin.
- Organisaation henkilökohtaista tunnusta tai salasanaa ei tule käyttää rekisteröityessä Internetiin.

(Käyttäjän tietoturvaohje 2003.)

Sähköposti ja Internet ovat hyviä työvälineitä tiedonhakuun ja yhteydenpitoon. Tämä liikenne on kuitenkin salaamatonta, joten niiden käyttö vaatii huolellisuutta.

- Internet ja sähköposti on tarkoitettu vain työkäyttöön.
- Ei ole luvallista välittää salassa pidettävää materiaalia Internetin kautta, ilman tietohallinnon lupaa.
- Salaustuotteiden käyttö tulisi opetella, jotta tieto ei kulje salaamattomana.
- Internetin kautta saatavia ohjelmia ei pidä asentaa tai käyttää.
- Virkasähköpostia saa käsitellä vain oman organisaation laitteilla.
- Liitetiedostot voivat sisältää haittaohjelmia. Epäilyttäviä viestejä ja liitetiedostoja on syytä varoa.

(Käyttäjän tietoturvaohje 2003.)

Etäkäyttö tarkoittaa organisaation tietoverkkon tai sen osan käyttöä organisaation ulkopuolelta. Etätyö tarkoittaa muualla kuin vakinaisessa työpisteessä tehtävää työtä. Näitäkin koskevia ohjeita on useita.

- Etäkäyttö ja etätyö ovat sallittuja ainoastaan, jos siitä on tehty erillinen sopimus.
- On pidettävä mielessä, ettei kaikkia töitä voi tehdä tietoturvallisesti etätyönä.
- Työnantaja hoitaa etäkäytössä olevien laitteiden, ohjelmistojen sekä tietoliikenneyhteyksien asennuksen ja hankinnan.
- On huolehdittava että tunnukset ja salasanat ovat ainoastaan työntekijän hallinnassa.
- Etätyö on rajattava aineistoon joka paljastuessaan ei vaaranna työpaikan tietoturvallisuutta.

(Käyttäjän tietoturvaohje 2003.)

4 YRITYKSEN VERKON DOKUMENTOINTI

4.1 Dokumentoinnin tämänhetkinen tila kohdeyrityksessä

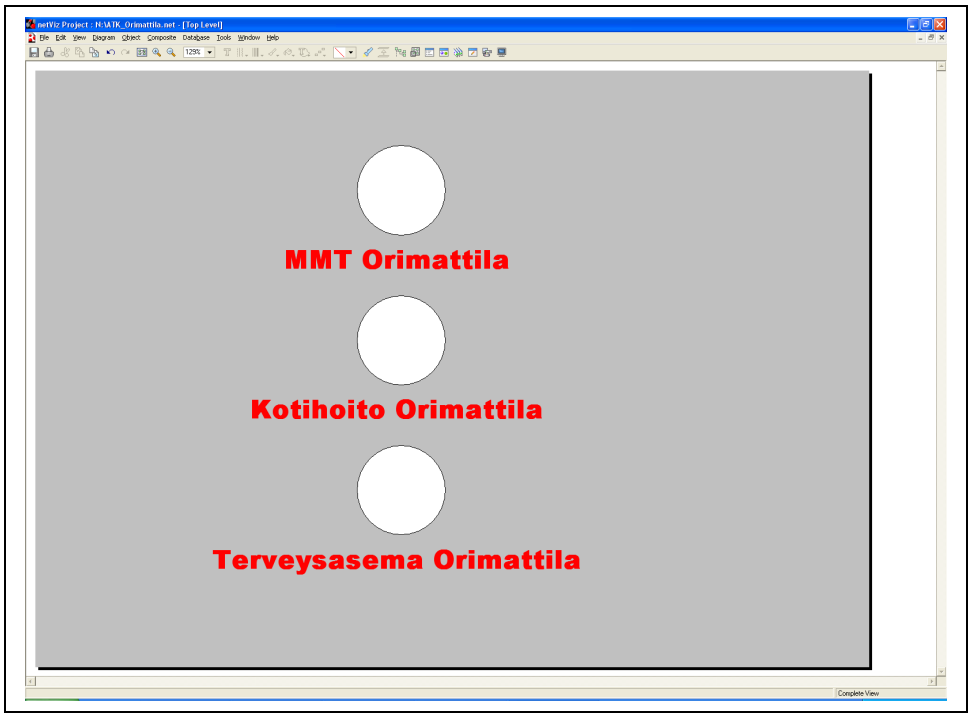
Tietoverkon dokumentointi aloitettiin Päijät-Hämeen keskussairaalalla syksyllä 2007. Tietoverkon dokumentointi suoritettiin Lahtea ympäröivissä lähikunnissa. Tämä johtui siitä, että vuoden 2007 alussa muodostui Päijät-Hämeen sosiaali- ja kuntayhtymä, joka toi lähikuntien terveydenhuollon keskussairaalan vastuulle. Verkon dokumentointi tehtiin lähikunnissa, kuten Iitissä, Pukkilassa, Orimattilassa, Nastolassa, Sysmässä ja Hartolassa kiertämällä terveysasemilla ja dokumentoimalla verkon rakenne eri toimipisteillä.

Tutkimuksen lähtökohta oli tutustua senhetkiseen dokumentointiin keskussairaalan omasta tietoverkosta, koska on tärkeää, että johdonmukaisuus säilyy eri osastoja tai konttoreita dokumentoitaessa. Verkon dokumentointi oli toteutettu NetViz -ohjelmalla. Avattaessa ohjelma näkyviin tulee päätaso, jossa on palloilla tai pilvillä kuvattu eri osastoja ja eri osastojen välillä viivat kuvastamassa osastojen välisiä yhteyksiä. Keskussairaalla näitä pilviä oli kymmeniä, joita klikkaamalla pääsi kyseiselle osastolle. Osastolla kuvan pohjana on oikea tarkka pohjapiirustus, jossa ilmenee huoneet ja huonenumerot. Näiden lisäksi piirustuksissa näkyvät ATK-rasiat ja -työpisteet, puhelimet, WLAN-tukiasemat sekä viivoina kaapeleiden vedot.

Toimeksianto ja tavoite työpaikalla oli selvittää paikkakohtaisesti dokumentaation laatu ympäryspaikkakunnilla ja yhtenäistää dokumentaatio Päijät-Hämeen keskussairaalan kanssa. Lähtötilanne dokumentoinnissa oli, että useimmille paikoille saavuttaessa kuultiin, että mitään edeltävää dokumentaatiota ei ole olemassa tai korkeintaan paikallisen järjestelmänhallitsijan päässä.

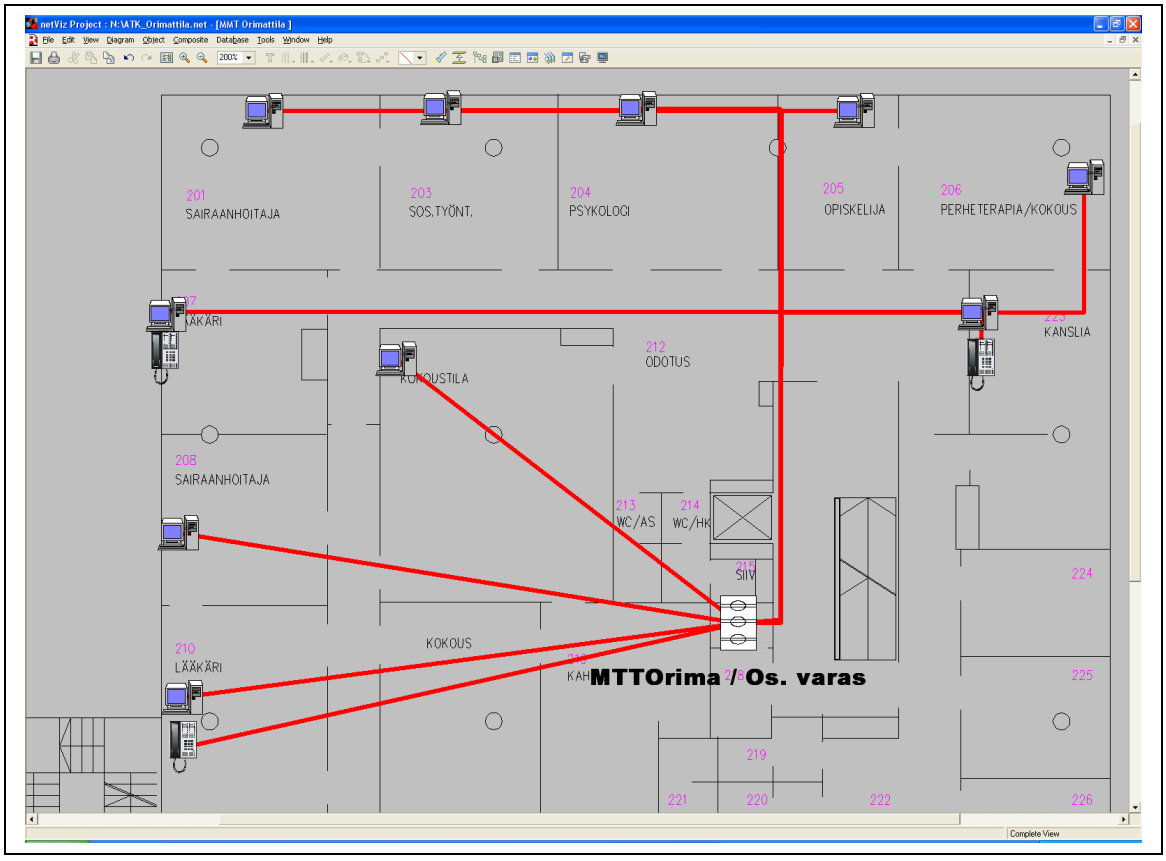
Tietoverkon dokumentointi aloitettiin kytkinpisteeltä. Kytkinpisteellä tutkittiin käsin, mihin kytkimen tai kytkimien portteihin paneeleista lähtevät johdot menevät. Kun kytkinpiste saatiin dokumentoitua, kierrettiin rakennusta huone kerrallaan tutkien mistä löytyy ATK-pistokkeita, työasemia, puhelimia ja tulostimia. Koska monet rakennukset olivat vanhoja ja muutamaan kertaan remontoituja, monessa paikassa ATK-pistokkeiden merkinnät eivät olleet johdonmukaisia. Esimerkiksi samassa rakennuksessa samasta kerroksessa saattoi löytyä jopa kolmella eri tavalla merkittyjä pistokkeita.

Lopulta kun rakennus oli kierretty ja kaikki tarvittava dokumentoitu palattiin sairaalalle ja siellä NetViz -ohjelmaa käyttäen tieto siirrettiin sähköiseen muotoon. NetViz -ohjelmassa voidaan lisätä rakennuksen pohjapiirustus pohjaksi, jolle sitten lisätään tarvittavat ATK-tarvikkeet kuten työasemat, pistokkeet, erilaiset kaapelointityypit, ja jopa kytkentäkaapit voidaan tehdä paneeleineen ja kytkimineen.



KUVIO 5. NetViz -dokumentoinnin päätaso

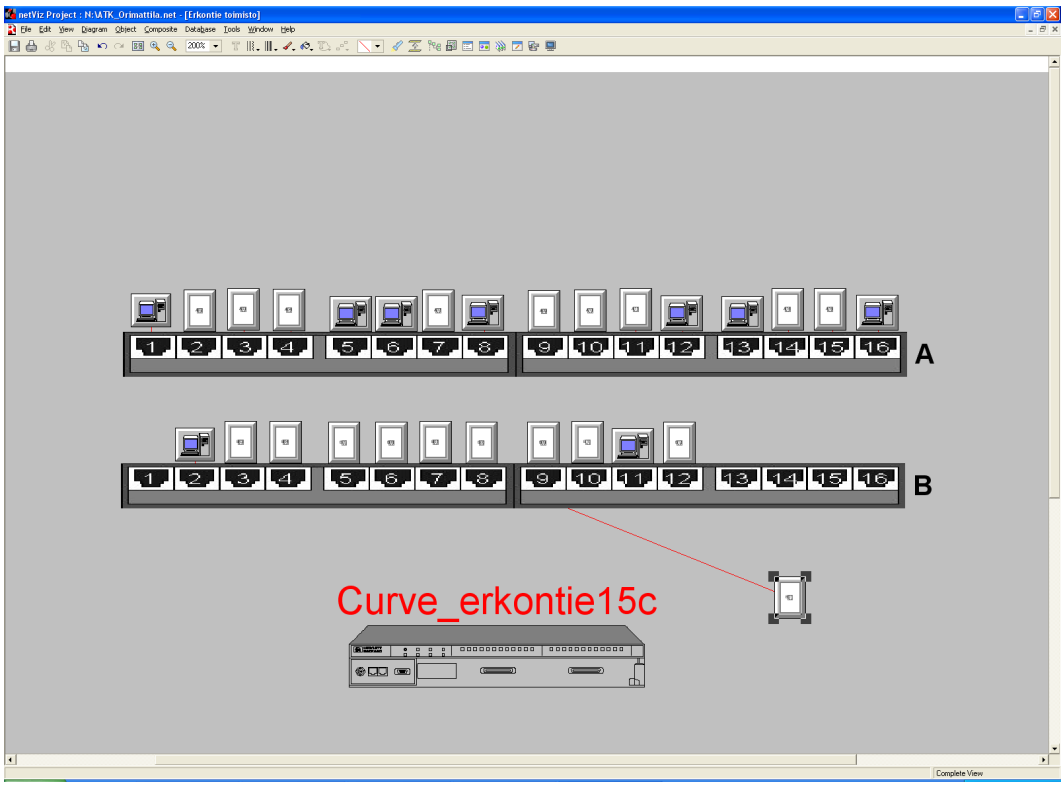
Kuviossa 5 nähdään Orimattilan tietoverkon dokumentointi. Päätasolla näkyy Orimattilassa olevat eri osastot, joita klikkaamalla pääsee tutustumaan haluttuun osastoon tarkemmin. Esimerkiksi kuviossa 6 nähdään mielenterveysosaston pohjapiirustus, siellä olevat työpisteet, kytkentäpiste sekä kaapelointi. Huomioitavaa kaapeloinnissa on se, että kun tiedetään, mitä kautta kaapelit kulkevat, esimerkiksi huonetta reunustavassa kourussa, kaapelien kulkureitti piirretään tarkasti. Jos taas kaapeleiden reitti ei ole selvillä, tämä piirretään ainoastaan suorana viivana kytkentäpisteelle. On tärkeää, että dokumentoitavassa pohjapiirustuksessa näkyy myös huoneiden numerot, koska ne todennäköisesti eivät tule muuttumaan tulevaisuudessa toisin kuin ovessa oleva nimi tai huoneen tämänhetkinen käyttötarkoitus.



KUVIO 6. Netviz -dokumentoinnin kuva osastosta

Kuviossa 7 nähdään paikallinen kytkentäpiste. Tämä on varsin vaatimaton varustettuna vain kahdella 16 paikkaisella paneelillaan ja yhdellä kytkimellä. Kuviossa 7 nähdään, mitä missäkin paneelin portissa on takana, onko siinä kone vai

pelkästään tyhjä rasia tai mahdollinen puhelin tai tulostin. Jokainen näkyvissä olevista ikoneista on raahattu paikalleen, ja kuten kuvasta nähdään, siinä on vielä yksi tyhjää seinäpistoketta kuvaava ikoni, joka on vielä siirrettävänä oikealle paikalleen.

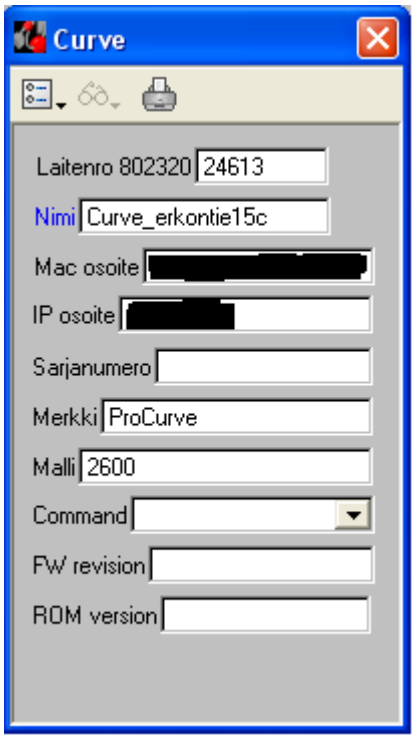


KUVIO 7. NetViz -dokumentoinnin kuva reitityspisteestä

Kuviossa 8 nähdään avustava ikkuna, jossa nähdään tiedot sillä hetkellä valittuna olevasta ikonista. Tässä näkyvissä on kytkentäpisteen kytkin. Ikkunasta nähdään tärkeimmät tiedot, kuten laitenumero, nimi, MAC- ja IP -osoitteet, sarjanumero, merkki ja malli, sekä tietoa mahdollisista käyttöjärjestelmän versioista. Lisäksi NetViz -ohjelma osaa Command-käskyn avulla jopa kokeilla saako kyseiseen kytkimeen yhteyttä.

Kytkimiä kuvattaessa joutuu tietoa syöttämään enemmän kuin normaalia työpistettä dokumentoitaessa. Normaalisti työpisteissä riittää tiedoiksi huoneen

nimi tai huonenumero, kytkentäpiste sekä tieto, mistä paneelista ja miltä paikalta yhteys on peräisin.



KUVIO 8. NetViz -dokumentoinnissa käytettävä ”inspector”

4.2 Parannusehdotuksia kohdeyrityksen tietoverkon dokumentointiin

Dokumentointi Päijät-Hämeen keskussairaalassa on itsessään toteutettu hyvin. Olemassa olevasta tietoverkosta on saatavissa tarkat tiedot, ja kun tietoverkkoa laajennetaan, tämä on helppo tehdä laajentamalla nykyistä dokumentaatiota. Tästä huolimatta on aina muutamia asioita, joita voisi miettiä.

Kun uusi työntekijä, tai esimerkiksi vieras, tutustuu nykyiseen tietoverkkodokumentaatioon, on dokumentaatiosta vaikea saada otetta. Jotta tietoverkon dokumentointi yrityksen sisällä on tulevaisuudessakin johdonmukaista ja toteutettu samalla tyylillä, olisi tärkeää tehdä opas tai ohjeistuslehtinen. Oppaan ei tarvitse olla pitkä, kunhan siinä vain käydään läpi tarvittavat tiedot nykyisestä

dokumentointityylistä, ja vaikkapa lyhyt ohjeistus NetViz -ohjelman käyttöön. Esimerkiksi tilanteessa, jossa syystä tai toisesta kaikki verkkodokumentaatiosta vastuussa olevat henkilöt ovat poissa, on helpompi lähteä ratkaisemaan tilannetta tutkimalla kyseistä ohjeistusta.

Tällä hetkellä kaikki dokumentaatio sijaitsee verkkolevyllä yhdessä hakemistossa. Olisikin tärkeää ajatella tilannetta, jossa tämä verkkolevy vikaantuu tai tyhjenee. Varajärjestelmä onkin hyvä olla olemassa, esimerkiksi automaattinen varmuuskopiointi tärkeistä tiedoista tarkasti mietityllä sopivalla aikavälillä. Toinen vaihtoehto on, että työntekijä itse tallentaa tietoverkkodokumentaation omalle koneelleen, mutta tässä on oltava tarkkana, että muistaa tallentaa aina muutokset myös verkkolevyllä olevalle viralliselle dokumentaatiolle.

4.3 Hyvä muistaa tietoverkkoa dokumentoitaessa

Ehkä tärkein asia tietoverkkoa dokumentoitaessa on säilyttää johdonmukaisuus. On äärimmäisen tärkeää, että siirryttäessä tasolta toiselle tai yrityksen eri konttoriin, tietoverkko on dokumentoitu samalla tavoin. Jos dokumentoinnin eri osissa ilmenee tyylillisiä erilaisuuksia, on dokumentoinnin laajentaminen vaikeaa. Samoin uuden työntekijän, jolla on tehtävänään tutustua olemassa olevaan dokumentointiin, on vaikeaa päästä sisään ja ymmärtää kyseistä tietoverkkoa.

Toinen tärkeä asia on, missä säilyttää esimerkiksi yrityksen tietoverkkoa koskevaa dokumentointia. Dokumentointi tulisi säilyttää vain yhdessä paikassa ja siihen tulisi myöntää oikeuksia vain niitä tarvitseville. Kirjoitusoikeus yrityksen tietoverkkodokumentointiin olisi hyvä olla vain muutamalla työntekijällä. Toisaalta tästäkin voi seurata ongelmia. Jos esimerkiksi työpaikalla on kaksi dokumentoinnista vastaavaa työntekijää ja toinen näistä on pidempään poissa, periaatteessa tämän toisen työntekijän tulisi olla jatkuvasti työpaikalla. Tietenkään

työpaikalla, jossa tietoverkko on stabiili eikä siis ole muuttumassa mihinkään, ei dokumentoinnista vastaavien henkilöiden läsnäolo ole niin tärkeää.

4.4 Yrityksen tietoverkon dokumentointi tulevaisuudessa

Laadittaessa ohjeistusta yritykselle tietoverkon dokumentoinnista on ohjeistuksesta ilmettävä, mitä tietoja kerätään. Päijät-Hämeen keskussairaalan tapauksessa dokumentista on löydyttävä seinärasioinnin kohdalla rasian-, pistokkeen- sekä huoneen numerot ja se, mihin kytkentäpisteeseen rasia on yhteydessä. Kytkinpisteeltä lähtevissä johdoissa tulisi näkyä, mihin rasiaan, huoneeseen tai kytkinpisteeseen johto on yhteydessä.

Ohjeistuksesta tulisi myös ilmetä vastuunjako: kenen kuuluu kerätä tieto ja vastata, että tieto on ajanmukaista. Päijät-Hämeen keskussairaalalla sairaalainsinööri vastaa siitä, mitä ja missä dokumentoidaan, sekä dokumentoinnin oikeellisuudesta ja siitä kuka tietoja voi käyttää. Kun uudistustöitä tehdään Päijät-Hämeen keskussairaalalle kuuluvissa rakennuksissa, dokumentoinnista vastaava työntekijä kerää sairaalainsinöörin pyynnöstä tarvittavat tiedot huoneista ja kytkinpisteeltä ja siirtää tiedot NetViz -ohjelmaan.

5 YRITYKSEN FYYSINEN TIETOTURVA

Päijät-Hämeen keskussairaalalla fyysisen tietoturvan taso on tällä hetkellä melko hyvä. Jos kuitenkin lähdetään tutkimaan asioita, jotka riskeeraavat yrityksen fyysisen tietoturvallisuuden, voidaan aloittaa tekemällä jako rakenteellisiin ja henkilöstöstä johtuviin riskeihin.

Henkilöstöstä johtuvat riskit voidaan myös jakaa kahteen osaan. Henkilöstöstä johtuvat tahattomat riskit kuvaavat vaikkapa kun työntekijä unohtaa tehdä jotakin ja samalla riskeeraa yrityksen tietoturvallisuuden. Kun puhutaan henkilöstöstä johtuvista tahallisista riskeistä, tarkoitetaan henkilöä, joka tieten tahtoen haluaa vahingoittaa yrityksen omaisuutta. Molemmat ovat kuitenkin suuri huolenaihe yritykselle.

5.1 Kohdeyrityksen tämänhetkinen fyysinen turvallisuus

Tärkein rakenteellinen riski on paloturvallisuus. Paloturvallisuus on järjestetty keskussairaalla hyvin, talo on jaettu osastoihin ja osastot ovat eristettynä palo-ovilla. Sammutusvaahtopulloja ja sammutuspeitteitä on riittävän tiheässä, ja sprinklerijärjestelmä on kattava. Lisäksi käytävät pyritään pitämään tyhjinä.

Sähköturvallisuus on myös hyvin järjestetty. Sähkökaapit ovat lukossa, ja niihin pääsevät vain sähkömiehet. Sähkö- ja muu kaapelointi on pyritty pitämään erillään, mahdollisia tulipaloja silmälläpitäen. Kaapelointi ja rasiointi tapahtuvat vain sähköammattilaisten tekemänä.

Päijät-Hämeen sosiaali- ja terveydenhuollon kuntayhtymän työasemien, tietoliikenneverkon ja tietojärjestelmien käyttöoikeus annetaan vain niille, jotka ovat allekirjoittaneet tietosuoja- ja tietoturvasitoumuksen. Siinä määritellään salassapitovelvollisuus, käyttäjätunnusten ja salasanojen oikea käyttö sekä

työasemien, tietojärjestelmien ja ohjelmien käyttö. Samassa ohjeistuksessa puututaan seuraamuksiin rikkomuksista. Lisäksi ohjeistuksessa on lueteltu tietoturvaa ja tietosuojaa koskevat tärkeimmät lakipykälät, jotka koskevat sosiaali- ja terveysalaa.

Kulunvalvonta on tarkasti järjestetty ja ohjeistettu. Ohjeistuksessa puututaan avaimien ja kuluntunnisteen turvalliseen säilyttämiseen ja käyttöön. Lisäksi ohjeistuksessa määritellään tarkasti mekaanisten avainten, puhelinten ja henkilökortin turvallisesta käyttämisestä. Työntekijöillä on avainkortit, joilla pääsee sähkölukollisista ovista alueille, jotka ovat potilailta kiellettyjä. Kun korttia käytetään, tästä tallentuu tieto koneille, joilta nähdään, kuka menee, minne menee ja milloin. Lisäksi tärkeimmillä ovilla ja alueilla on kameravalvonta.

Kuitenkin kulunvalvontaan liittyy myös tietoturva-aukkoja. Useat toimistotilat ovat yleensä lukitsemattomia, esimerkiksi tilat missä, itse työskentelin, ja osastolla vierailevia ihmisiä ei kirjata ylös mihinkään. Omalla osastolla käytettävillä tietokoneilla ei mitään äärimmäisen tärkeitä dokumentteja käsitelty, työhön kuului esimerkiksi verkon valvontaa ja dokumentointia, mutta silti voidaan pitää riskinä, että tilat ovat avonaiset. Useasti myös koneet pidetään auki ja lukitsemattomina, jolloin kuka tahansa voisi väärinkäyttää toisen konetta ja oikeuksia.

Työntekijöille annettavien atk-oikeuksien kanssa ei myöskään ole seurattu mitään selkeää linjaa. On ollut tapauksia, jolloin jos jokin ohjelma jota työntekijä on yrittänyt käyttää, ei olekaan toiminut, on työntekijälle annettu lisää oikeuksia niin kauan, että ohjelma on saatu toimimaan. Tähän liittyy riski että työntekijä pääsee käsiksi tietoihin, joihin hänen ei pitäisi päästä.

Oman tietoturvariskinsä luovat kytkentäkaapit. Näissä yhdistyvät johdot jotka tuovat tietoliikenneyhteyden konehuoneelta osastolle, ja johdot, jotka vievät yhteyden osaston eri huoneille. Nämä kaapit ovat usein lukitsemattomia ja sijaitsevat osaston käytävillä. Kuka tahansa voisi siis ohi kulkiessaan tehdä kiusaa

irrottamalla johtoja tai vaihtamalla näiden paikkoja. Joku tietoliikenteeseen perehtynyt voisi jopa yrittää salakuunnella liikennettä.

5.2 Parannusehdotuksia yrityksen fyysiseen tietoturvaan

Ehkä yleisin tahaton tietoturvariski on jättää työpaikalla työkone päälle lähtiessään käymään vaikkapa syömässä. Tulisi aina muistaa vähintään lukita kone poistuessaan työpisteeltä. Varsinkin, jos työpiste tai -huone on avonainen, eli sinne saattaa saapua vierailijoita. Pienen huolimattomuuden vuoksi voi vähimmillään menettää päivän työpanoksen, jos vaikka joku käy sulkemassa ohjelman, jolla on tehty töitä koko päivän, tai pahimmassa tapauksessa yrityksen tärkeät dokumentit vaarantuvat.

Olisi muistettava pitää työtilat, missä käsitellään tärkeää tietoa, esimerkiksi organisaation tietoverkon dokumentaatiota, lukittuna. Jos tiloja on mahdotonta pitää suljettuina, tulisi aina huolehtia, että joku on paikalla valvomassa, ettei koneilla käy luvattomia käyttäjiä. Asettamalla määrityksiksi koneille, joilla työskennellään, että ne menevät lukkoon vaikkapa minuutin tai parin kuluttua, kun kone on ollut käyttämättömänä, estetään suuri osa mahdollisesta luvattomasta käytöstä.

On tärkeää rajata tiedot, joihin työntekijällä on pääsy. Uuden työntekijän tulisi päästä käsiksi ainoastaan niihin tietoihin, joita tarvitsee työtä tehdessään. Kun työntekijä ei pääse käsiksi arvokkaisiin tietoihin, ei hänelle tule myöskään halua hyötyä niistä.

Tilanteeseen, jossa joku työntekijä tai ulkopuolinen yrittää tahallaan vaarantaa tai rikkoa yrityksen tietoturvan, on hieman hankalampi varautua. Mutta koska tietomurto tai vahingonteko voi käydä hyvinkin kalliiksi yritykselle, on tähän hyvä varautua. Paras keino varautua mahdollisiin tietomurtoihin on pitää tärkeät kohteet

(tilat, koneet, kytkentäkaapit) lukittuna sekä käytetyt tietokoneohjelmistot päivitettynä uusimpiin versioihin.

5.3 Hyvä muistaa fyysisestä tietoturvasta

Nykyään suuren riskin muodostavat myös työntekijöiden omat tallennusmediat. Esimerkiksi muistitikulle mahtuu nykyään helposti jo DVD levyllisen verran dataa. Monet yritykset yleensä kieltävätkin omien muistitikkujen tuomisen työpaikalle, ei ainoastaan siinä pelossa, että joku yrittäisi anastaa tietoa, vaan pelkästään senkin takia, että yrityksen sisäverkko on todennäköisesti hyvin suojattu ulkoapäin siihen kohdistuville hyökkäyksille ja haittaohjelmille. Jos työntekijä tuo vahingossa tai tahallaan jonkin haittaohjelman tai viruksen ja virus leviää yrityksen sisäverkkoon, voi tällä olla äärimmäisen tuhoisia ja kalliita vaikutuksia.

Etätyöskentely on yleistymässä ja on myös laskettavissa riskiksi. Työskennellessään kotoaan käyttäen yrityksen tietoverkkoa tai muuta materiaalia työntekijän on muistettava pitää huolta tietoturvasta. Yrityksen tietoturvan on säilyttävä, ja onkin tärkeää pitää huolta, ettei tietoturvan kannalta tärkeimpiä töitä voi tehdä kotoa käsin.

Yrityksen tulisi järjestää tietoverkkonsa niin, että ulkopuolelta tuleva liikenne on tarkasti valvonnassa. Tähän riittää yleensä tehokas ja hyvin ylläpidetty palomuuri. Tietomurtoa yrityksen sisältä käsin yrittävä ulkopuolinen tulisi estää jo aiemmin mainittujen keinojen avulla (kulunvalvonta, huoneet lukossa, koneet lukossa).

6 YHTEENVETO

Tietoverkkojen dokumentointi on yrityksissä yhä vaativampaa. Yritysten kasvu ja tietoverkkotekniikan monimutkaistuminen asettaa haasteita dokumenttien ylläpidolle. Tavoitteena oli tutkia miten tietoverkon dokumentointi oli toteutettu Päijät-Hämeen keskussairaalalla ja yhtenäistää dokumentointi koskemaan lähikuntien terveysasemia.

Kun suunnitellaan tietoverkon dokumentaatiota yrityksessä, tärkein asia on rajata mitä tietoa kerätään. Liian yksityiskohtaisesti dokumentoitu tietoverkko tekee dokumenteista sekavia. Dokumentoitaessa on tärkeää myös säilyttää johdonmukaisuus, jotta dokumenttien laajentaminen tulevaisuudessa helpottuu. Teoriaosuudessa käytiin läpi, mistä tietoverkko dokumentaatio koostuu ja mitä siltä vaaditaan.

Toisena tavoitteena opinnäytetyössä oli tutkia ja arvioida fyysisen tietoturvallisuuden tilaa Päijät-Hämeen keskussairaalalla. Teoriaosuudessa käytiin läpi fyysisen tietoturvan eri osa-alueita, mitä vaatimuksia fyysinen tietoturva asettaa yrityksille ja kuinka tietoturvan tavoitteisiin päästäisiin.

Tietoturva on sosiaali- ja terveydenhuollon kriittinen tekijä, koska asiakkaan ja potilaan on luotettava ehdottomasti tietojensa tietosuojaan. Tämä luottamus on palvelun kulmakivi. Vaikka jokainen työntekijä sitoutuu ja allekirjoittaa tietoturvasopimuksen Päijät-Hämeen keskussairaalalla, olisi tärkeää järjestää tietoturvakoulutusta yleisesti pienissä ryhmissä, jotta jokainen työntekijä ymmärtää tietoturvallisuuden tärkeyden arkipäivän toiminnassa.

Tietoturvan kehittäminen ja ylläpitäminen on loputonta kilpajuoksua väärinkäyttöä vastaan. Pelkästään fyysiset ja henkiset resurssit usein rajoittavat tietoturvan ylläpitämistä huipputasolla. Hyvällä ohjeistuksella ja rajaamalla kulku- ja käyttöoikeuksia päästään jo pitkälle. Mutta kuitenkin tietoturva on usein yhtä hyvä tai huono kuin sen heikon lenkki. Ajattelematon, hyväuskoinen käyttäjä on usein suurin vaara tietoturvalle.

LÄHTEET

Hakala, M. 2006. Tietoturvallisuuden käsikirja. Jyväskylä. Docendo Finland Oy.

Jaakohuhta, H. 2000. Lähiverkot – Ethernet. Jyväskylä. Oy Edita Ab, IT Press.

Jaakohuhta, H 2005. Lähiverkot – Ethernet. Uudistettu painos. Jyväskylä. Oy Edita Ab, IT Press.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä. Docendo Finland Oy

Navicre. 2007. Tietoturvan hallintapalvelut kunnille. [verkkojulkaisu]. [viitattu 23.3.2008]. Saatavissa:
http://www.navicre.com/index.php?14

Paananen, J. 2003. Tietotekniikan peruskirja. Jyväskylä. Docendo Finland Oy

Käyttäjän tietoturvaohje. 2003. [verkkojulkaisu]. Valtiovarainministeriö. [viitattu 23.3.2008]. Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/51027/51024_fi.pdf

Yritysturvallisuus EK Oy. 2007. Tietoturvallisuus. [verkkojulkaisu]. Yritysturvallisuus EK Oy. [viitattu 24.3.2008]. Saatavissa:
http://www.ek.fi/ytnk/yritysturvallisuus/tietoturvallisuus.php