PK-Yrityksen tietoverkot, palvelut ja tietoturva

Anssi Haapanen

Opinnäytetyö
Marraskuu 2011

Tietotekniikka
Tekniikka ja liikenne

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) HAAPANEN, Anssi	Julkaisun laji Opinnäytetyö	Päivämäärä 26.11.2011
	Sivumäärä 96	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (x)
Työn nimi PK-YRITYKSEN TIETOVERKOT, PALVELUT JA TIETOTURVA		
Koulutusohjelma Tietotekniikka		
Työn ohjaaja(t) HAUTAMÄKI, Jari		
Toimeksiantaja(t) Kannuksen fysikaalinen hoitolaitos (KFHL) PARANTALA, Minna		

Tiivistelmä

Opinnäytetyössä keskitytään toimeksiantajan palvelunhallinnan ja tietoturvan nykytilanteeseen, sen puutteisiin sekä kehitysehdotuksiin. Lähtökohtaisesti kartoitettiin yrityksen nykytilanne, joka analysoitiin ja tämän pohjalta laadittiin yritykselle palvelunhallintasuunnitelma, tietoturvasuunnitelma, riskianalyysi ja jatkuvuussuunnitelma.

Käytännön tasolla opinnäytetyössä tarjotaan yritykselle valmis ratkaisumalli, millä se voi jatkossa oman aikataulun mukaisesti siirtyä ehdotettuihin toimintamalleihin. Palvelut pyrittiin keskittämään mahdollisimman tehokkaasti, jotta ne eivät jää yrityksen ylläpitoon.

Palveluhallinnan pohjana suunnittelulle käytettiin pitkälti ITIL:n tarjoamia menetelmiä. Yrityksen tarpeet sekä selkeän ohjeistuksen laatiminen heille olivat ensisijaisen tärkeitä, jotta tämän työn tuloksia pystytään jatkossa hyödyntämään mahdollisimman tehokkaasti.

Suunnitelmat pohjautuvat kyseisen toimeksiantajan tarpeisiin, mutta niitä pystytään hyödyntämään myös muissa suunnittelutehtävissä muille tahoille. Kokonaisuus on pitkälti sidoksissa olemassa oleviin standardeihin palvelunhallinnasta ja tietoturvasta, joten näin ollen lopputuote on helposti muokattavissa vastaamaan muidenkin yritysten tarpeita.

Avainsanat (asiasanat)

ITIL, Tietoturva, Palvelunhallinta, SLA-sopimus, käytettävyys

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Author(s)
HAAPANEN, Anssi

Type of publication
Bachelor´s / Master's Thesis

Date
26112011

Pages
96

Language
Finnish

Confidential

( ) Until

Permission for web publication
(x)

Title
DATA NETWORKS, IT SERVICES AND SECURITY OF SMALL AND MEDIUM-SIZED ENTERPRISES

Degree Programme
Data Network Technology

Tutor(s)
HAUTAMÄKI, Jari

Assigned by
Kannuksen fysikaalinen hoitolaitos (KFHL)
PARANTALA, Minna

Abstract
This thesis was assigned by Kannuksen fysikaalinen hoitolaitos (KFHL), and it focuses on the KFHL's current level of service management and security. Additionally, it assesses the functionality of the current methods and provides a new model for management and security.

The process started with evaluating the KFHL's current situation and was followed with fault and risk analysis. Based on this, a new model for service management, security, network control, risk assessment and continuity plan was produced to better and more effectively serve and meet all the needs of the company.

The aim was to focus all the services required by the company to a single contractor to make management easier and to provide a single point-of-contact for all things IT for the company. The basis for this solution was provided by the standard ITIL, which heavily influenced the way this project was done. The KFHL's need for clear processes and methods regarding IT-management was the driving force behind the end product. In the end, two separate subcontractors had to be used for different services.

The end product of this thesis project was a completed management, security and continuity plan, for all the services required by the company. It also entails a risk assessment of the current situation. As the end product is heavily influenced by current IT-standards, it can be adapted and easily modified to be used by other companies.

Keywords
ITIL, Security, Service management, Service Level Agreement, availability

Miscellaneous

SISÄLTÖ

KUVIOT

1 TYÖN LÄHTÖKOHDAT

Tässä opinnäytetyössä tarkasteltiin yrityksen tietoverkkoa, palveluita sekä tietoturvaa. Nämä kaikki pyrittiin saattamaan paremmalle tasolle tavalla, joka toteutettuna hyödyttää toimeksiantajaa. Koska aihe oli varsin laaja sekä monta eri aspektia kattava. Siinä ei keskitytty ainoastaan yhteen eksaktiin aihealueeseen vaan vaikutteita otettiin useasta eri tietoliikenne tekniikan aihealueesta. Lopulta sitä rajattiin ottamalla huomioon ainoastaan seikat, jotka hyödyttävät toimeksiantajaa. Samalla lopputuotoksesta saatiin suhteellisen laaja yleisteos tietoliikennetekniikasta ja siihen liittyvistä asioista.

Opinnäytetyön tavoitteina oli parantaa toimeksiantajan toimintaa ja mahdollisesti tuottaa heille taloudellisia säästöjä. Projektiluontoisen työskentelyn kautta pyrittiin havaitsemaan mahdollisimman monet toimeksiantajan puutteet ja korjaamaan nämä toimeksiantajaa hyödyttävällä tavalla. Toimeksiantajan päätettäväksi jäi, mitkä osat koko opinnäytetyöstä otettaisiin käytännöntasolla käyttöön.

Yrityksen näkökulmasta erittäin tärkeät osa-alueet ovat ne, joilla voidaan saada toiminnassa aikaan taloudellisia sääntöjä. Samoin myös käytännöissä tulee pystyä olemaan KELA:n asettamien standardien tasolla tietojärjestelmissä ja toimintamalleissa (laskutus, asiakastietokanta ja vastaavat ratkaisut). Yrityksen toimiala huomioiden Kela on erittäin suuri asiakas, ja sen takia Kelan omien standardien täyttäminen on elintärkeää yrityksen toiminnan kannalta. Pyritään samalla kilpailuttamaan yrityksen käyttämiä palveluita ja näin tarvittaessa saamaan taloudelliset menot pienemmiksi.

2 TOIMEKSIANTAJAN ESITTELY

Seuraavassa esitellään hieman toimeksiantajan taustoja yrityksenä. Tässä kohdassa ei oteta vielä kantaa heidän tietoverkkoihin, palveluihin tai tietoturvaan.

2.1 Yrityskuvaus ja yleistä toimeksiantajasta

Toimeksiantajana opinnäytetyössäni toimii Kannuksen fysikaalinen hoitolaitos. Kyseinen yritys tarjoaa fysioterapia- ja kuntoutus-, sekä kuntosalipalveluita Kannuksen lähialueille. Yritys on perustettu vuonna 1985. Yritysmuoto on osakeyhtiö. Yrityksen omistaa Minna Parantala sekä Tiina Brandt. Minna Parantala toimii toimitusjohtajana. (Kannuksen fysikaalinen hoitolaitos 2011).

Yrityksen tarjoamat palvelut voidaan ryhmitellä seuraavasti: vaikeavammaiset ja lääkinnälliset kuntoutusasiakkaat, lähetepotilaat, hieronnat, liikuntaryhmät, omatoimiset kuntosalin käyttäjät sekä tuoteostajat. Yritys tuottaa myös Kelan vaikeavammaisten avokuntoutuspalveluja. (Koivisto 2007, 4).

Yritys työllistää tällä hetkellä 3 vakituista henkilöä, sekä yhden osa-aikaisen työntekijän. Yrityksen sisäinen rakenne on tällä hetkellä muuttuva, sillä osa henkilökunnasta on äitiyslomalla.

Yrityksellä on oma laatukäsikirja, jonka mukaan toimintaa harjoitetaan.

2.2 Kilpailuympäristö

Kannuksen fysikaalisen hoitolaitoksen toiminta ulottuu suurilta osin Kannus-Toholampi-Ullava –sektorille. Pieniä fysikaalisia hoitolaitoksia ja ammatinharjoittajia löytyy kaikista lähikunnista. Samantasoisia fysioterapiapalveluja on saatavissa Kokkolasta. Kannuksessa toimii myös sotainvalidien kuntoutuspalveluja tuottava Kitinkannus, jolla on myös sopimus vaikeavammaisten kuntoutuspalveluiden tuottamisesta. Suurin osa hoitolaitoksen asiakkaista tulee Kannuksesta, pienempi osa lähikunnista. (Koivisto 2007, 5-6).

2.3 Vahvuudet ja heikkoudet

Ohessa olevat vahvuudet ja heikkoudet on lainattu yrityksen omasta laatukäsikirjasta.

Vahvuutena Kannuksen fysikaalisessa hoitolaitoksessa on monipuolinen, ihmisläheinen fysioterapiaosaaminen, jossa on kivijalkana hyvä henkilökunta. Palveluiden osalta vahvuuksia ovat hyvä poliklinikkapuoli, osaava liikuntaryhmätoiminta ja korkeatasoinen vaikeavammaisten fysioterapiaosaaminen sekä lisäksi tarpeen mukaan asiakkaiden yksilöllinen kuntoutus. Vahvuutena on myös kuntosali, jossa ihmiset voivat käydä oma-aloitteisesti. (Koivisto 2007, 6).

Suurimpana heikkoutena voidaan pitää osaavien, hyvän työkokemuksen omaavien sijaisterapeuttien puutetta. Fysioterapeutteja koulutetaan isoilla paikkakunnilla ja yleensä valmistuneet fysioterapeutit jäävät sille tielle, eli asumaan ja työskentelemään suurempiin ympyröihin. Muuttaminen pienelle paikkakunnalle on vaikeaa sillä muualta tulevien puolisoille on vaikeaa saada vastaavaa työtä pieneltä paikkakunnalta. (Koivisto 2007, 6).

Yksi tärkeimmistä yrityksen kehittymiseen vaikuttavista asioista on työntekijöiden kouluttaminen ja erikoistuminen sekä tutustuminen kehityksen mukanaan tuomiin uusiin hoitomuotoihin. Näin yritys pysyy mukana kehityksessä. Uusien tilojen myötä on myös mahdollisuus kasvattaa asiakaspiiriä. (Koivisto 2007, 6).

Kannuksen Fysikaalisen hoitolaitoksen kehityksen jarruna ja suurimpana uhkana nähdään uusien, pitkäaikaisten työntekijöiden puute. Hoidon kehittymisen kannalta on tärkeää, että työntekijän ja asiakkaan välille muodostuu luottamuksellinen suhde, joten työntekijöiden vaihtuminen vaikuttaa asiakassuhteisiin.
(Koivisto 2007, 6).

3 LÄHTÖTILANTEEN KARTOITUS

Yrityksen puutteiden korjaaminen tarkoittaa valtaosin palvelun ulkoistamista jollekin taholle, sillä yrityksen henkilöstöstä ei löydy IT-henkilöä, joka kykenisi ylläpitämään rakennettua kokonaisuutta eikä uuden henkilön palkkaaminen tule kysymykseen tällä hetkellä.

Pahin ongelma yrityksen lähtötilanteessa on heidän käyttämänsä asiakastietokannan ylläpito-sovellus. Samalla ohjelmalla kirjataan potilastietoja sekä laskutetaan asiakkaita. Kyseinen ohjelmisto on vanha, ja sen kehitys on lopetettu (valmistajan toimesta). Koko asiakastietokanta on toimiston pöytäkoneella, josta sitä varmuuskopioidaan käsin muistitikuille. Tämä ei ainoastaan aiheuta lisätyötä työntekijöille, vaan on myös riskialtis tapa säilyttää dataa jonka katoaminen / tuhoutuminen olisi erittäin vakava tilanne yrityksen toiminnalle. Yrityksellä olisi mahdollisuus siirtyä sovelluksen valmistajan tarjoamaan uuteen selainpohjaiseen versioon. Tällöin sovelluksen valmistaja/ylläpitäjä on vastuussa asiakastietokantojen eheydestä ja sovellusten toimivuudesta. Tämä muutos on pakollinen seuraavan viiden vuoden kuluessa, sillä asiakkaita tarjoavat tahot, kuten KELA, edellyttävät tietojärjestelmiltä tiettyjä ehtoja, jotta asiakkaat voidaan toimeksiantajalle tarjota.

Mikäli siirryttäisiin selainpohjaisten sovellusten käyttöön, tulisi toimeksiantajan internetyhteyksien tila tarkastaa. Heillä on tällä hetkellä Pohjois-Pohjanmaan puhelimelta (PPO) kuluttajaliittymä. Tähän tulisi hankkia yritysliittymä ja laatia tarpeeksi tiukat SLA-sopimukset, jotta viankorjaus ongelmien sattuessa olisi mahdollisimman nopeaa ja tarvittaessa saataisiin rahallista korvausta sanktioiden muodossa operaattorilta, mikäli vikaa ei korjata tavoiteajassa. Tämä olisi erittäin kriittistä, koska kaikki toiminta olisi internetyhteyksien varassa käytännössä. Samoin tarvittavat käytettävyyssopimukset tulisi laatia sovellusten tarjoajan kanssa. Käytettävyys tulisi olla korkea. Ongelmana siirtymisessä uuteen järjestelmään ja toimintamalliin on sen hinta. Operaattoreiden kilpailutus ja tarjolla olevat access-tekniikat määrittelevät minkä tahon kanssa tätä lähdettäisiin työstämään.

Kapasiteetti ei tule olemaan missään vaiheessa ongelma. Kun mietitään uuden internetyhteyden hankintaa (yritysliittymä), tulee ottaa huomioon, että toimeksiantajalla on käytettävissä tällä hetkellä ainoastaan kaksi konetta. Näin ollen liikennemäärät eivät kasvaisi suuriksi.

Toimeksiantaja on myös ilmaissut kiinnostuksensa langattoman verkon rakentamiseen. Tässä olisi mahdollisesti yksi kehittämiskohde. Mikäli yritykseen hankitaan lisää koneita (kannettavia), niistä saataisiin paras hyöty irti ilman, että tarvitsee ryhtyä massiiviseen kaapelointiin yrityksen tiloissa. Verkko tulisi tietenkin salata hyvin, jotta luvaton pääsy voidaan estää yrityksen verkkoon.

Yrityksen web-sivut ovat tällä hetkellä ulkoisen tahon ylläpidossa. Tämä sopimus tulisi ottaa suurennuslasin alle ja kilpailuttaa muita tahoja.

Käytössä olevilla koneilla ei ole mitään yhtenevää linjaa käyttäjien hallinnassa. Palvelinta lienee turha hankkia, koska sen ylläpito osoittautuisi liian hankalaksi. Tähän tulisi ratkaisuna laatia mahdollisimman perusteellinen ohjeistus ja käytäntö, kuinka käyttäjätilien hallinta ja oikeudet järjestetään. Yksi vaihtoehto on ulkoistaa myös tämä jollekin taholle. Vaihtoehto on siis leasata koneet ulkoiselta taholta, jolloin voitaisiin sanella ehdot joiden tulee täyttyä. Samalla vastuu koneista olisi ulkoisella taholla ja ongelmien ilmetessä olisi selkeä taho keneen olla yhteydessä.

Tietoturva on tällä hetkellä täysin sovelluspohjaisten antivirus/palomuuriohjelmistojen varassa. Tähän tulisi saada myös välittömästi muutos. Yritysliittymän hankkiminen korjaisi osaltaan ongelmaa. Muussa tapauksessa on myös mahdollista hankkia asiakkaalle oma reititin ja rakentaa yhteys tätä kautta. Näin saataisiin jotain kontrollia tietoturvan hallintaan.

Selvitys näiden tarpeiden osalta suoritettiin pitkälti yrityksen edustajan esille tuomista asioista sekä itse lähtötilannetta tarkasteltaessa havaituista selkeistä puutteista. Itse kartoitusta ei suoritettu systemaattisesti jonkin tietyn kaavan mukaan.

4 TEORIA JA TAUSTATIETO -OSIO

Käydään läpi opinnäyteyön taustalla olevien asioiden teoria. Näiden asioiden tietämys ja tuntemus on tärkeää kokonaiskuvan ja toteutuksen ymmärtämisen kannalta.

4.1 Tietoverkot

Kun lähdetään suunnittelemaan tietoverkkoja tulee huomioida useita eri asioita verkon kannalta. Näistä eri kokonaisuuksista muodostuu täysi verkon rakenne. Käsittellään yrityksen lähiverkon rakentamista tässä teoriaosassa. Kun verkkoa lähdetään rakentamaan, OSI-malli on "de facto" ohje verkon suunnitteluun. OSI-malli koostuu seitsemästä tasosta. Kun verkkoja suunnitellaan ja ylläpidetään, toimivaksi malliksi on adoptoitu OSI-mallin mukaan toimiminen. Aloitetaan ensimmäiseltä tasolta ja liikutaan pikkuhiljaa korkeammalle hierarkiassa. Näin ongelmanratkaisun kuin suunnittelun ja kehityksenkin kannalta voidaan toimia systemaattisesti joka tilanteessa.

Tasot yksi (fyysinen) ja kaksi (linkkiyhteys) konkretisoituvat yrityksen näkökulmasta fyysisen median valinnasta. Millaista access-tekniikka hyödynnetään ulkoisissa yhteyksissä? Millaista kaapelointia käytetään sisäverkossa? Tämän mukaan määräytyy käytettävät modeemit/reitittimet. Mahdollisuudet eri tekniikoiden käyttöön ja linjan kättelyprotokolliin tarkastellaan kappaleessa 5, jossa valitaan käytettävä tekniikka. Verkon fyysisen topologian suunnittelu. Vedetään tarvittavat fyysiset kaapeloinnit. Tarvittavien verkkolaitteiden hankkiminen. (Cisco Systems Inc. 2009).

Taso kolme (verkkokerros) on sellaisenaan ehkä suurin ja tärkein kokonaisuus verkon toiminnan kannalta. Yrityksen verkko tulee segmentoida järkevästi. Luodaan toimiva IP-osoitteistus verkon laitteille. Verkon loogisen topologian suunnittelu sekä yleismaallinen kuva, kuinka verkon halutaan toimivan. Kun looginen kokonaisuus on hyvin luotu ja suunniteltu, helpottuu verkon hallinta, ja toiminta on helpompi pitää paremmalla tasolla. Laaditaan myös haluttu reititysmalli yrityksen tarpeisiin sopivaksi sekä valitaan käytettävät reititys protokollat jos tarpeen. (Cisco Systems Inc. 2009).

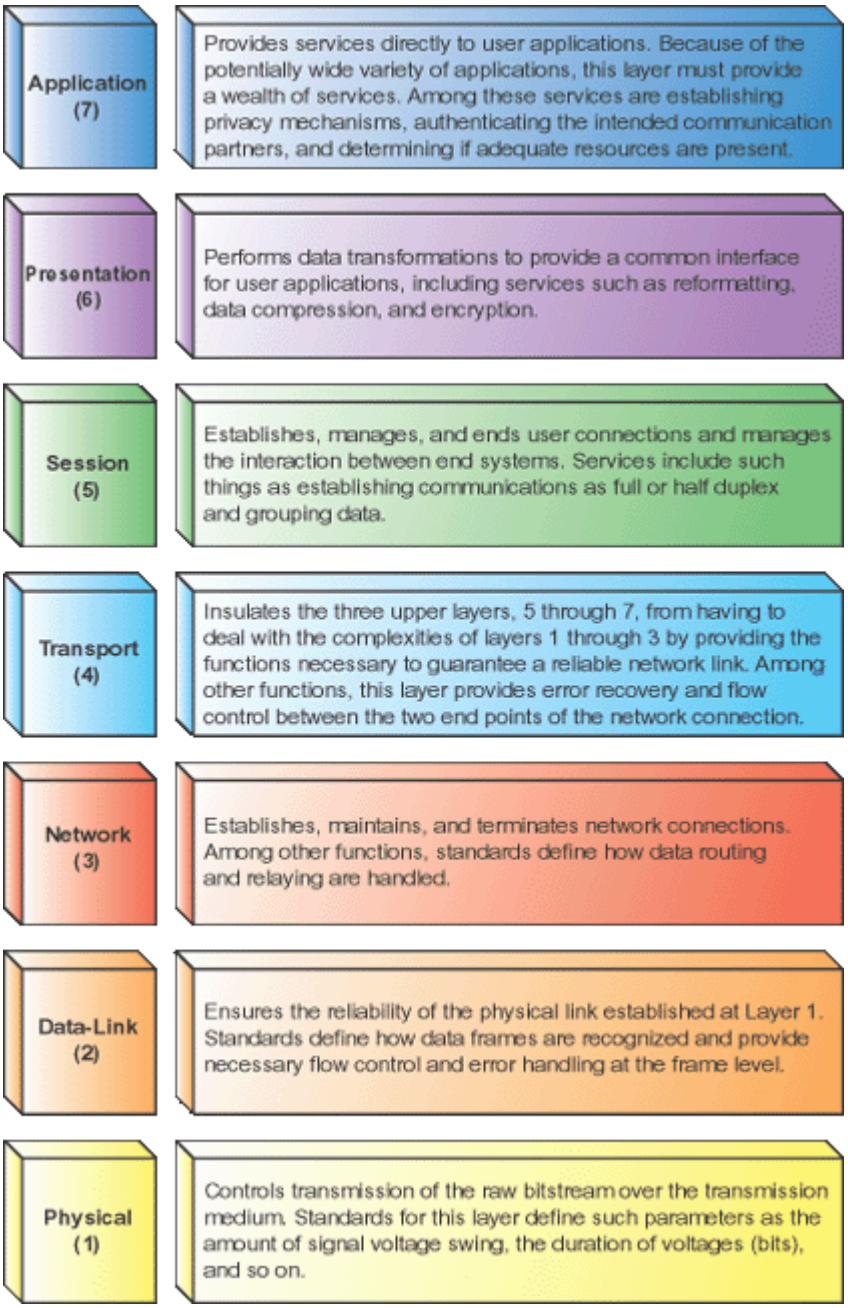
Neljäs taso määrittelee käytettävät protokollat ja kehysrakenteet. Tässä tulee yrityksen kannalta ottaa huomioon erityisesti verkon toiminnan kannalta käytettävät sovellukset ja liikenne. Tukeeko verkko kyseistä protokollaa? Tehdään tarvittavat säännöt sekä reititysmuutokset verkkoon, jotta kyseiset protokollat voivat toimia. Esimerkkinä toimisi esim. yritysverkko, jossa työntekijät käyttävät ohjelmistoa jossa on yhteinen tietokanta erillisellä palvelimelle. Kun koneet liikennöivät palvelimelle käytetään tähän TCP protokollaa porttiin 427. Vastaavanlaiset säännöt tulisi laatia kaikille sovelluksille ja tärkeintä on tunnistaa yrityksen tarvitsemat protokollat ja portit.
(Cisco Systems Inc. 2009).

Taso viisi on istuntokerros. Verkon suunnittelussa tässä vaiheessa otetaan huomioon eri sovellusten ja laitteiden yhteyden avaamiskäytännöt. Varsinkin jos yrityksellä on paljon palvelimia joissa sijaitsee toistuvasti käytössä olevaa dataa ohjelmistojen kannalta, kättely ja yhteyden avaaminen laitteiden välillä suunnitellaan tässä. Valtaosassa ohjelmistoja on olemassa olevat menetelmät ja yleensä eri vaihtoehdot istunnon avaamiseen. Nämä täytyy tunnistaa ja ottaa huomioon jotta palvelut saadaan toimimaan halutulla tavalla. Esimerkkeinä voitaisiin käyttää kirjautumista palvelimelle ja siinä käytettävää kättelymenettelyä. (Cisco Systems Inc. 2009).

Kuudes taso vastaa datan pakkaamisesta sellaiseen muotoon, että sovellukset voivat sitä hyödyntää. Tämä on yleensä myös jo "sisäänrakennettuna" käytetyissä sovelluksissa eikä edellytä muuta kuin oikeiden sovellusten valintaa sekä käytettyjen menetelmien sekä salauksen valintaa ja tunnistamista. Kun tiedetään tarkalleen, mitä verkossa liikkuu ja tapahtuu, voidaan verkkoa aina hallita paremmin.
(Cisco Systems Inc. 2009).

Seitsemäs ja viimeinen taso vastaa datan muuttamisesta selkokieliseksi loppukäyttäjälle jonkin ohjelmiston kautta. Tämä tulee verkonsuunnittelussa esiin esim. valitsemalla oikeanlaiset sovellukset käytettäviksi. Sovellusten tulee ymmärtää toisiaan (tiedostotyypit ja tuki toisilleen), jotta kokonaisuus toimisi. (Cisco Systems Inc. 2009).

KUVIO 1. OSI-malli



(Novell 2011).

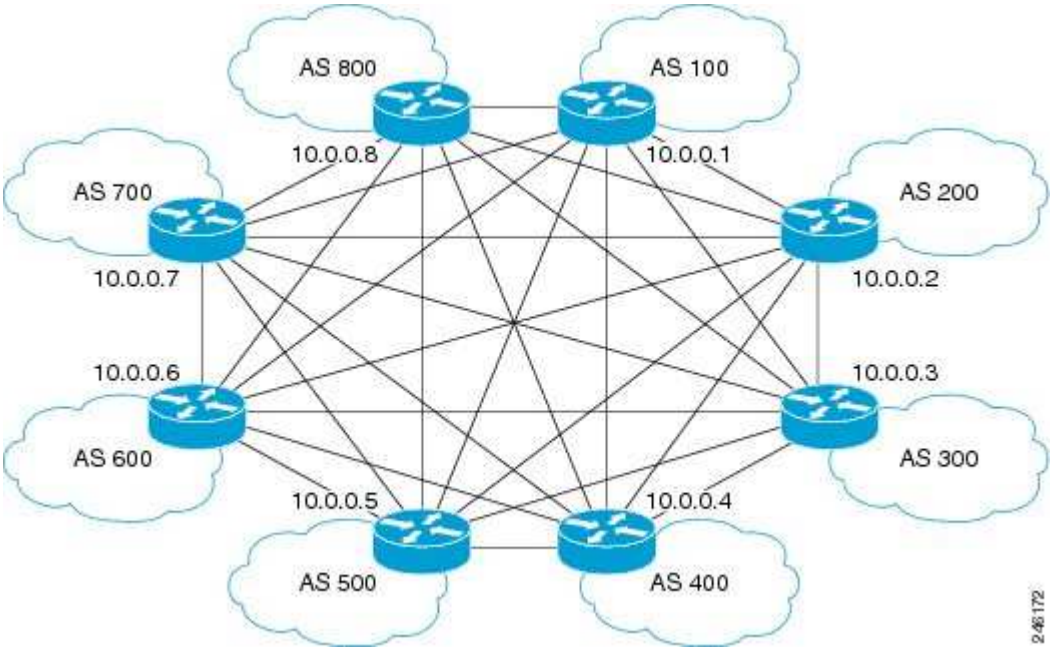
4.1.1 Topologia

Lähdettäessä suunnittelemaan verkon topologiaa, tulee ottaa huomioon verkon käyttötarkoitus. Tietyt perusasiat riippumatta verkon käyttötarkoituksesta tulee aina käsitel-

lä. Kaikkein tärkein aspekti missä tahansa verkossa on sen hyvä käytettävyys. Loppukäyttäjän tulee pystyä käyttämään verkkoa nopeasti ilman suuria viiveitä sekä luotettavasti (ei yhteyksien katkomista, datan saapuminen perille virheettömästi). Lähiverkko tulisi aina olla 100 % käytettävissä. Tästä syystä myös topologian redundanttisuus on otettava huomioon. Topologian suunnitellaan yleensä fullmesh -tyylillä, mutta muitakin vaihtoehtoja on. Topologiaa suunnitellessa tulee myös ottaa huomioon fyysisen tason ja loogisen tason vaatimukset. Nämä topologiat ovat harvoin identtiset.

Full Mesh-topologia on eräitä yleisimpiä tapoja suunnitella verkko. Tässä toteutuksessa verkon jokainen solmu on yhteydessä kaikkiin muihin solmuihin (kts. kuvio 2). Tällöin vaikka yksi linkki ei toimisi, löytyy kohteeseen aina toinen reitti. Erittäin toimiva malli, joskin hintavampi toteuttaa kuin monet muut vaihtoehdot.

KUVIO 2. Full mesh-topologia.

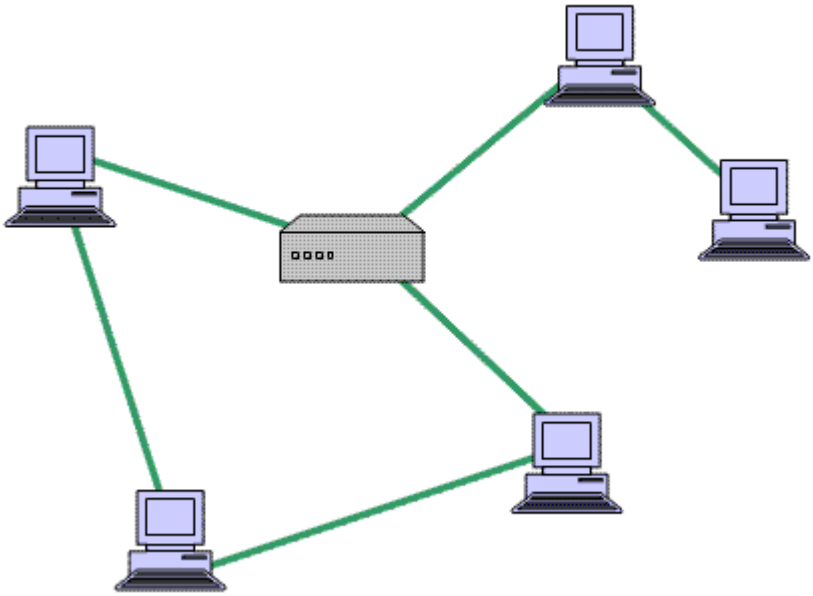


(Cisco Systems Inc. 2011).

Mesh-topologia on erilainen variaatio Full Mesh -toteutuksesta. Tässä vaihtoehdossa kaikki solmut eivät ole suoraan yhteydessä toisiinsa, vaan ainoastaan topologian kriittisimmissä pisteissä olevat solmut ovat yhteydessä useampiin solmuihin (kts. kuvio 3). Tällä toteutuksella ei saada redundanttisuutta sellaisenaan aikaan, ja tietyistä laitteista

voi muodostua turhankin kriittisiä verkon toiminnan kannalta. Mutta erilaisilla variaatioilla tästä toteutuksessa ja loogisen topologian hyvällä suunnittelulla tilannetta voidaan korjata.

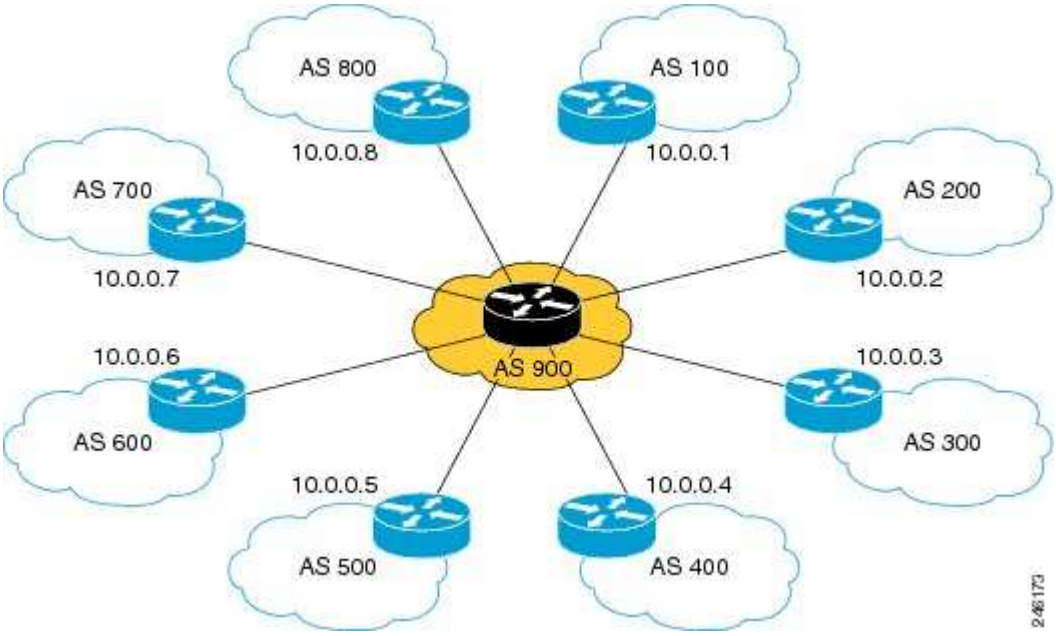
KUVIO 3. Mesh-topologia



(Mitchell 2011, 4 of 5).

Tähti-topologiassa on yksi keskeinen solmu, johon kaikki muut solmut ovat yhteydessä (kts. kuvio 4). Tämä on osittain samanlainen kuin Mesh-topologia, mutta erona Mesh-topologiassa näitä "keskussolmuja" saattaa olla useampia. Tähti -topologiassa siis muodostaa vielä kriittisemmäksi tämä yksittäinen solmu, sillä jos sen toiminta lakkaa, kaikki yhteydet solmujen välillä ovat poikki.

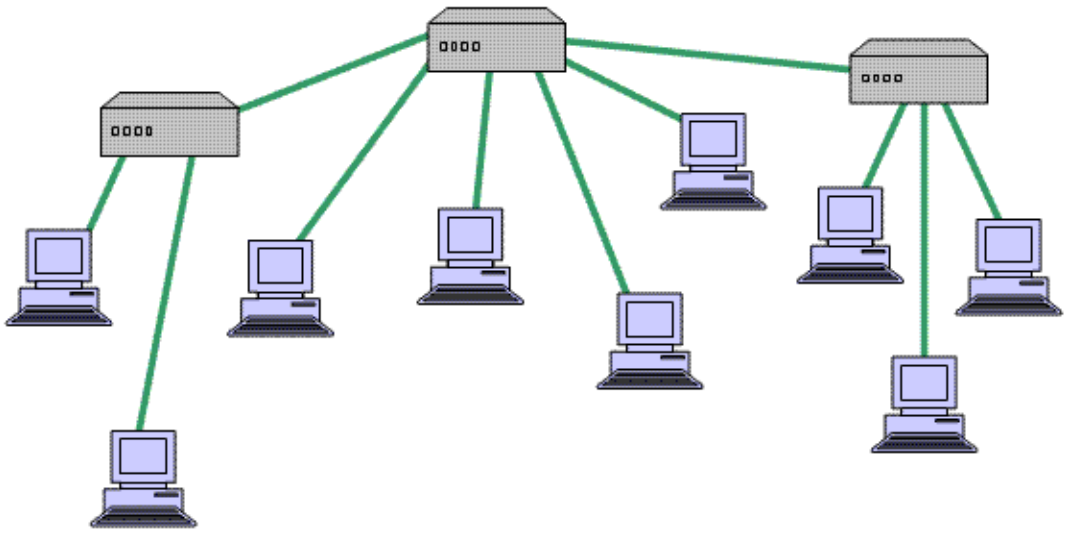
KUVIO 4. Tähti-topologia



(Cisco Systems Inc. 2011).

Puu-topologiassa verkon rakenne on kuten nimikin ilmaisee, puumainen. On olemassa "juuri" solmu, josta lähtee useampia linkkejä toisiin solmuihin (kts. kuvio 5). Näistä solmuista lähtee taas useampia linkkejä eteenpäin jne. Tällainen malli on erityisen tärkeää varsinkin L2-tason laitteiden kanssa, sillä muuten verkkoon saattaa muodostua looppeja, jotka aiheuttavat saman liikenteen kierrätystä yhä uudelleen verkon läpi.

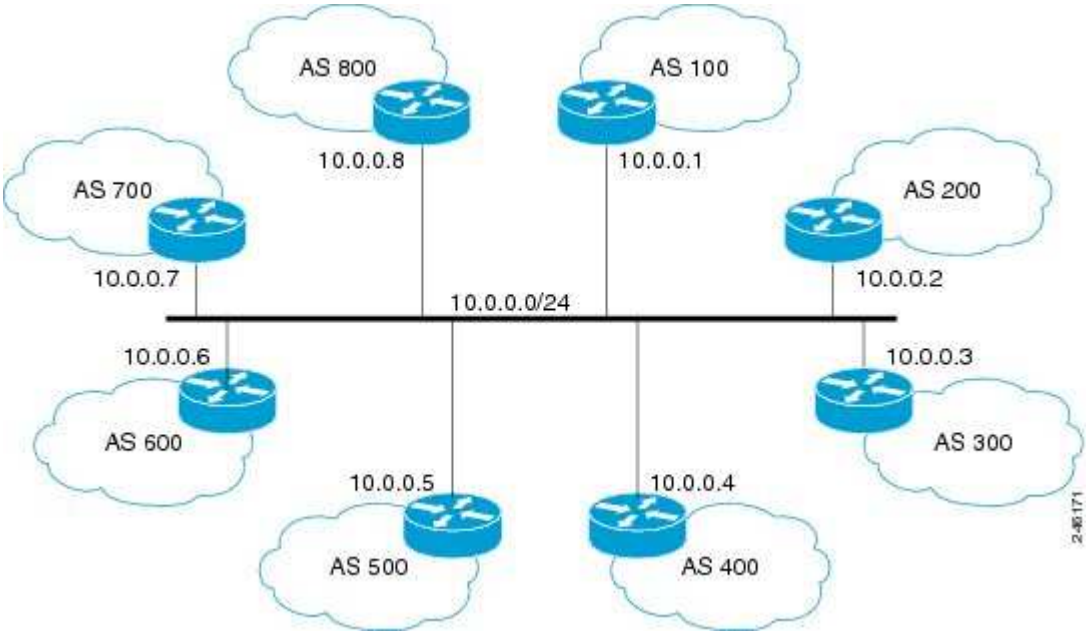
KUVIO 5. Puu-topologia



(Mitchell 2011, 5 of 5).

Bus-topologissa, kaikki solmut ovat yhteydessä samaan fyysiseen mediaan ja jakavat näin ollen saman linkin (kts. kuvio 6). Mikäli linkki katkeaa tai muuten sen toiminta häiriintyy, koko verkko ei ole toimintakyvytön vaan siitä muodostuu yksittäisiä segmenttejä joiden sisällä liikenne yhä toimii.

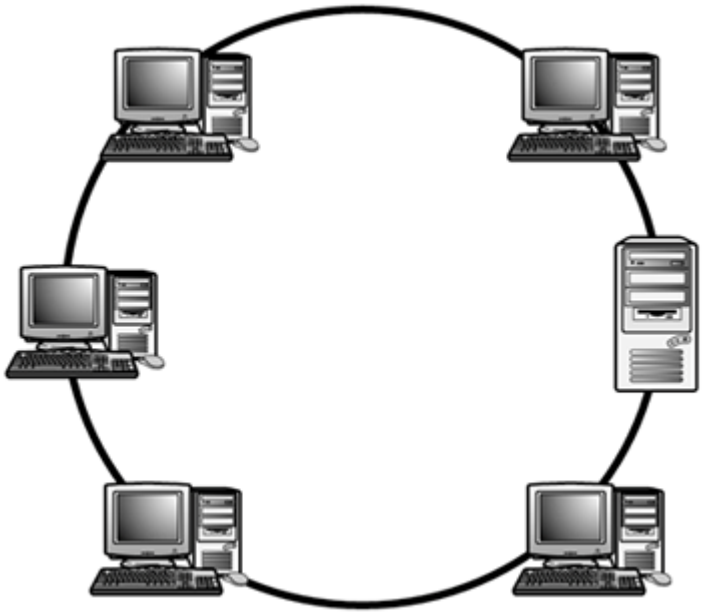
KUVIO 6. Bus-topologia



(Cisco Systems Inc. 2011).

Rengas-topologiassa verkon solmut ovat yhteydessä kahteen solmuun, edelliseen ja seuraavaan. Näin syntyy rengasmainen rakenne verkolle (kts. kuvio 7). Myös tässä toteutuksessa yhden linkkivälin katkeaminen ei johda verkon toiminta kyvyttömyyteen, koska reitti löytyy toisen suunnan kautta kohteeseen. Ongelmana on tässä tapauksessa tarpeettoman monen hopin kautta kulkeminen, mikä generoi verkkoon turhaa kuormitusta. Käsitteellä hop viitataan englanninkieliseen sanaan hop joka tarkoittaa verkkolaitteiden lukumäärää jonka kautta datapaketti joutuu kulkemaan päästäkseen kohteeseensa eli toisin sanoen matkalla olevien "pysähdysten" lukumäärää.

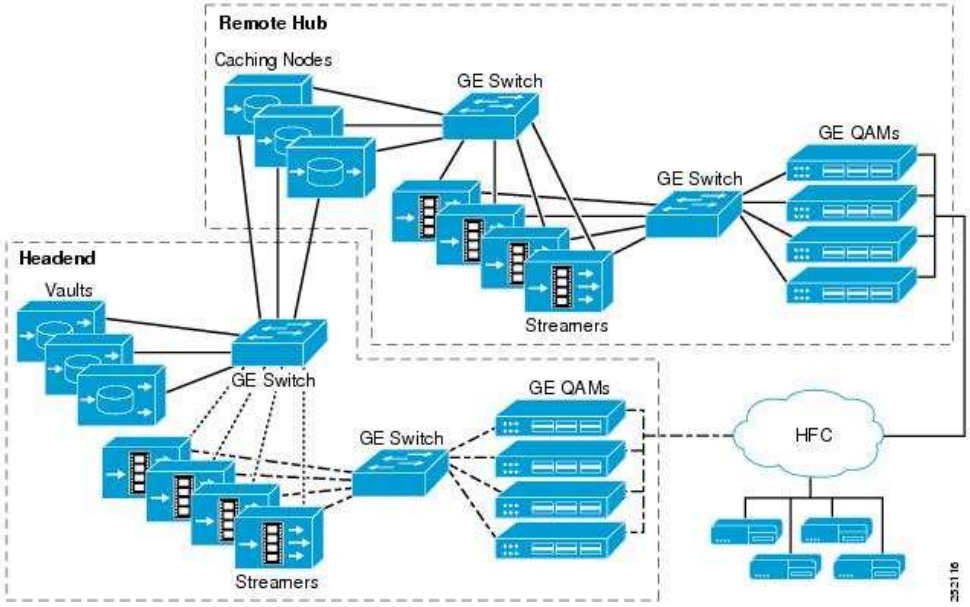
KUVIO 7. Rengas-topologia



(Brainbell.com 2011).

Hybridi-topologia on yhdistelmä muista eri topologia malleista. Hybridiverkot sisältävät siis samankaltaisuuksia kahden tai useamman eri topologia mallin kanssa, mutta tätä verkkoa ei voida kuitenkaan luokitella minkään yksittäisen mukaan (kts. kuvio 8).

KUVIO 8. Hybridi-topologia



(Cisco Systems Inc. 2011).

Kuten jo mainittu, topologisen toteutuksen suunnittelussa tulee ottaa huomioon fyysinen ja looginen topologia. Täytyy pyrkiä suunnittelemaan toimiva ja varma kokonaisuus suhteessa kustannuksiin ja käyttöasteeseen.

4.1.2 Reititys

Reititys tapahtuu verkkokerroksella ja tällä algoritmisella menetelmällä valitaan haluttu reitti lähdeosoitteesta kohteeseen. Se miten reitti valitaan riippuu reititysprotokollasta ja algoritmista mitä kyseinen protokolla hyödyntää. Samoin myös tarkemmat reitin valinnat tapahtuvat eri tavalla protokollasta riippuen. Distance vector -menetelmä ja linkstate -menetelmä ovat yleisellä tasolla useimmin käytetyt menettelyt.

Distance vector -menetelmä, perustuu Bellman-Ford algoritmiin. Kaikille reiteillä määritetään tietty "hinta" ja lasketaan halvin reitti kohteeseen. Tämä kohde laitetaan solmun reititystauluun. Laitteet jakavat myös oman reititystaulunsa naapurilaitteille ja ne ottavat uudet halvemmat reitit tiettyyn kohteeseen omaan reititystauluunsa.
(Cisco Systems Inc. 2006, 2).

Link-state -menetelmä, jokainen verkon solmu lähettää verkkoon paketteja, joilla se tiedustelee mitä laitteita on kytkettynä muihin solmuihin. Tämän jälkeen laitteet muodostavat oman kartan topologiasta kerätyn informaation perusteella. Tämän jälkeen jokainen laite määrittelee reittitaulun mihin lisätään shortest path algoritmilla lyhimmät (halvimmat) reitit kyseisestä solmusta muihin.
(Cisco Systems Inc. 2006, 3).

4.1.3 Reititysprotokollat

Reititys protokollat määrittävät käytännön kuinka verkossa olevat laitteet keskustelevat keskenään ja jakavat reittitietoja kohteisiin. Reititysprotokollia on useita erilaisia, joista tässä käymme läpi olennaisimmat. Keskitymme pääsääntöisesti lähiverkon reititykseen. Käymme myös läpi yleisesti käytössä olevan "de facto" reititys protokollan BGPv4, jolla eri AS:n välinen reititys on toteutettu.

Protokollat voidaan luokitella karkeasti IGP ja EGP protokolliin. IGP eli interior gateway protocol, on protokolla jota käytetään yhden AS:n (autonomous system) sisällä reititykseen. Käytännössä nämä protokollat ovat siis lähiverkkojen protokollia. EGP protokollat, eli exterior gateway protocol, käytetään AS:en väliseen liikennöintiin. Nämä protokollat toimivat siis Internetin reitityksessä välittämällä reittitietoja eri AS:ien välillä.

OSPF reititysprotokolla. Yleisimmin käytössä olevan IGP-protokolla (interior gateway protocol). Nimi tulee termeistä **Open shortest path first**. Kyseinen protokolla käyttää Linkstate -menetelmää toimiakseen. OSPF muodostaa verkkokuvan topologiasta keräämällä linkkien tietoja muilta reitittimiltä. Kun reititin on tällä tapaan keränyt ja muodostanut topologisen kuvan verkosta, valitaan kaikista verkon reitittimistä DR (designated router) ja BDR (backup designated router).
(Cisco Systems Inc. 2006, 2-5).

Kun jokainen verkon laite on muodostanut topologisen kuvan verkosta, nämä kuvat välitetään DR:lle (designated router) ja BDR:lle (backup designated router) ospf multicast osoitteeseen 224.0.0.6. Tämän jälkeen DR laatii parhaan kuvan verkosta ja välittää sen kaikille muille reitittimille. Jatkossa aina kun verkossa havaitaan muutoksia, lähetetään siitä tieto suoraan DR:lle ja BDR:lle, jonka jälkeen DR päivittää verkon topologiakuvan ja lähettää päivityksen muille verkon reitittimille. OSPF reititysprotokollaa käyttävät reitittimet lähettävät säännöllisesti naapuri reitittimille reitityspäivityksiä. Mikäli joltain linkiltä ei tule päivitystä, tämän linkin oletetaan olevan poikki ja topologia muuttuu sen mukaisesti. Reitityspäivityksiä reitittimet jakavat directlyconnected -naapureilleen multicast-osoitteeseen 224.0.0.5. Nämä multicast lähetykset eivät koskaan kulje pitemmälle kuin 1 hopin päässä oleville laitteille. OSPF on yksi yleisimmin käytössä oleva lähiverkon reititysprotokolla. Sen nopea topologian muodostaminen ja muutoksiin reagoiminen ovat sen vahvuuksia. (Cisco Systems Inc. 2006, 5-8).

EIGRP reititysprotokolla. Cisco systemsin kehittämä oma reititysprotokolla, joka on muunnos IGRP reititysprotokollasta. Kyseinen protokolla hyödyntää distance vector menetelmää reititystaulun ja topologian muodostamisessa. EIGRP kykenee välittämään tietoa myös IGRP:tä käyttäville laitteille. Tämä tapahtuu muuttamalla EIGRP metric 32-bittisestä muodosta 24-bittiseen IGRP muotoon. EIGRP kykenee myös pa-

remmin optimoimaan distance vector menetelmän toimintaa käyttämällä DUAL:ia (diffusing update algorithm). Nopeampi verkkokuvan uudelleen muodostus topologian muuttuessa ja kaistan käytön optimointi kuuluvat DUAL:in toiminteisiin. (Cisco Systems Inc. 2006, 1-2, 7).

EIGRP kerää tietoa kolmeen eri tauluun.
1. Naapuritaulu, johon tallennetaan naapurireititinten tiedot, joihin ollaan suoraan yhteydessä.
2. Topologiataulu johon tallennetaan lista kohdeverkoista EIGRP verkossa sekä näiden metric arvot, sekä jokaiselle kohteelle successor ja feasible successor.
3. Reititystaulu, johon tallennetaan tiedot reiteistä kaikkiin kohteisiin. Tämä taulu muodostetaan topologiataulusta seuraavalla tavalla. Jokainen kohde verkko jolle voidaan tunnistaa successor tai feasible successor next hoppina kohdeverkkohin lisätään reititystauluun.
(Cisco Systems Inc. 2006, 7-9).

Successor tiettyyn kohteeseen valitaan laitteesta, josta on kohteeseen lyhin matka sekä voidaan taata, että se ei voi olla osa minkäänlaista reititys looppia. Feasible successor kohteeseen valitaan ainoastaan sen perusteella, että se ei voi olla osa minkäänlaista reitityslooppia. (Cisco Systems Inc. 2006, 7).

Reitittimet jotka käyttävät EIGRP:tä reititysprotokollana vaihtavat hello -viestejä jotka sisältävät tietoja kaistanleveydestä, viiveestä, kuormasta, luotettavuudesta sekä reitin MTU (maximum transmission unit) -arvosta. Mikäli naapuri reitittimiltä ei tule tai ne eivät vastaa lähetettyihin hello –paketteihin, oletetaan yhteyden olevan poikki.
(Cisco Systems Inc. 2006, 9-10).

IGRP reititysprotokolla. Yksi jo vanhemmista classfull –protokollista. Kyseinen protokolla ei tue verkkomaskin käsitettä, joten kaikki osoitteet ovat aina A, B tai C luokasta. Koska nykyään kaikki käytössä olevat reititysprotokollat ovat pääsääntöisesti classless –protokollia, kyseinen protokolla on poistunut pikku hiljaa käytöstä. IP-osoite tilaa hukkuu huomattavasti, koska aliverkon maskin käsitettä ei ole. Protokolla on alun perin Cisco systemsin kehittämä ja se on kehitetty korvaamaan RIP, siinä olevan 15:ta hopin maksimi etäisyyden takia.
(Cisco Systems Inc. 2011)

RIPv1 ja **RIPv2 reititysprotokollat**. Eräs vanhempia classfull –protokollia, ja edelleen käytössä, mutta harvoin ottaen huomioon classfull –protokollien rajoitukset ja heikkoudet. Protokolla hyödyntää Bellman-Ford algoritmia jolla voidaan laskea lyhin reitti kohteeseen. Metric arvona toimii RIP:n tapauksessa hop count. Maksimi etäisyys on 15 hyppyä reitillä. Tämä rajoitus on asetettu reitityslooppien välttämiseksi. Sama rajoitus on koitunut protokollan kuolemaksi, koska monet nykyajan verkon ovat sen verran suuria, jotta kyseistä protokollaa ei yksinkertaisesta voida käyttää. (Hedrick 1988, 1-3).

RIPv2 kehitettiin parantamaan tilanne protokollan osalta. Kyseinen protokolla kykenee käsittelemään aliverkon maski -käsitettä, joten se voidaan luokitella classless protokollaksi. Jotta se olisi yhteensopiva RIPv1:n kanssa, 15 hypyn takaraja säilyi. Reititys päivitykset lähetetään naapurireitittimille multicastina osoitteeseen 224.0.0.9. RIPv1:ssä tämä tapahtui broadcastliikenteenä joka kuormitti verkkoa turhaan. (Malkin 1998, 2-4).

IS-IS reititysprotokolla. Protokolla jota käytetään pakettikytkentäisissä verkoissa. Protokolla kehitettiin alun perin toimimaan CLNS protokollapinon kanssa. Myöhemmin IS-IS protokollaan lisättiin tuki myös IP:lle ja verkkokerroksen liikenteelle. Protokolla käyttää Dijkstran algoritmia määrittämään parhaan reitin verkon läpi. Toiminta on monilta osin samankaltainen OSPF protokollan kanssa. Molemmat tukevat vaihtelevia aliverkon maskeja ja havaitsevat muut laitteet multicast hello paketeilla. IS-IS ei ikinä yleistynyt samalla tavalla kuin OSPF reititysprotokollana. Tämä johtui pääsääntöisesti siitä, että OSPF on rakennettu suoraan reitittämään 3-tason liikennettä IP-osoitteilla ja IS-IS taas on rakennettu OSI:n verkkotason protokollan (CLNS) päälle. (Cisco Systems Inc. 2006, 1-5).

BGPv4 reititysprotokolla. Tämä protokolla on EGP-protokolla joka toimii AS:en välillä. Koko Internet ja yhteydet AS:en välillä rakentuvat BGP:n toimintaan. Sen toiminta eroaa perus IGP-protokollista siinä, että IGP-protokollat käyttävät jonkinlaista metric –arvoa määrittämään suosiollisen reitin tiettyyn kohteeseen, kun taas BGP hoitaa reitityksen määriteltyjen sääntöjen (policies/rules) ja reittien perusteella. BGP:tä ”puhuvat” laitteet, eivät muodosta naapuruus (peer) –suhdetta automaattisesti kuten monet muut IGP-protokollat. Nämä naapuruudet tulee määritellä manuaalisesti. (Cisco Systems Inc. 2006, 2).

BGP voi toimia kahdella tavalla, IBGP:nä ja EBGP:nä. IBGP on reititin joka käyttää bgp:tä reititykseen, mutta toimii yhden AS:n sisällä, eikä ole suoraan yhteydessä toisiin AS:iin. EBGP:tä käyttävä reititin taas toimii AS:en välillä reunareitittimenä. EBGP:n mainostamat reitit ovat aina luotettavampia kuin IBGP:n kun tehdään reitityspäätöksiä. (Cisco Systems Inc. 2006, 7-8, 13).

BGP:n toiminta perustuu Finite State Machinen toimintaan (FSM). BGP toimii kuuden eri tilan mukaan. Nämä kuusi tilaa ovat Idle, Connect, Active, OpenSent, OpenConfirm, Established. Näiden eri tilojen avulla tapahtuu BGP peerien välinen toiminta. Idle –tilassa BGP estää kaikki sisään tulevat yhteydet ja pyrkii neuvottelemaan TCP yhteyden naapurin kanssa. Connect –tilassa BGP odottaa, että TCP yhteyden muodostus saadaan loppuun, tämän jälkeen BGP siirtyy OpenSent tilaan. Mikäli Connect –tilassa yhteyden muodostus epäonnistuu, BGP siirtyy Active tilaan, jossa se resetoi yhteyden ConnectRetry laskurin, ja yrittää muodostaa yhteyttä uudelleen siirtymällä Connect –tilaan. OpenSent –tilassa BGP lähettää Open -viestin naapurille ja odottaa vastausta tähän. Kun vastaus saadaan, BGP siirtyy Established –tilaan. Tässä tilassa BGP kykenee ottamaan vastaan Keepalive-, Update- ja Notification –viestejä naapuriltaan. (Cisco Systems Inc. 2006, 10-12).

4.1.4 Kapasiteetti

Verkkoja suunnitellessa tulee ottaa huomioon useita eri tekijöitä kapasiteetin tarvetta arvioidessa. Käytettävät sovellukset, reititysmainostukset, laitteiden määrät sekä käyttäjien määrät ja ruuhka-ajankohdat vaikuttavat kapasiteetin määrään ja verkon topologiaan. Mahdolliset pullonkaulat tulisi tunnistaa jo etukäteen ja pyrkiä eliminoimaan järkevästi kapasiteettia jakamalla. Kannattaa aina myös pitää mielessä mahdollisen verkon laajentumisen näkökulma, jotta olemassa olevaa topologiaa ja kapasiteettia voidaan tarvittaessa lisätä mahdollisimman helposti. (The Art of Service 2009, 62).

Kapasiteetti voitaisiin jakaa karkeasta kahteen eri luokkaan, Laitteiden suorituskyky (palvelimet, reitittimet, kytkimet, palomuurit) sekä varsinainen media ja sen tyyppi niin sisäverkon kuin WAN yhteyksien osalta (ethernet, gigabit ethernet, kuitu, kupariverkko, kaapeliverkko, mobiiliverkko) eli access-tekniikat jolla saadaan yhteydet ulkomaailmaan.

Käyttäjämäärien ja sovellusten kartoitus. Ensimmäinen vaihe on kartoittaa käyttäjien määrä ja käytössä olevien sovelluksien kaistantarve. Käyttäjämäärä ja sovellukset vaikuttavat suoraan esim. palvelimien tarpeeseen. Mitä palveluita yrityksellä on omilla palvelimillaan, tarvitaanko kuin paljon verkkolevy tilaa ja prossesointitehoa ja muistia? Jos useampia palvelimia käytössä, esim. replikointi voi olla suuri liikenteen generoija. Tulisi arvioida minä ajankohtana mahdolliset ruuhkapiikit muodostuvat ja mistä nämä todennäköisesti johtuvat. (The Art of Service 2009, 15-19).

Verkon monitorointi. Millä työkaluilla verkon käyttöastetta monitoroidaan? Tähänkin löytyy useita eri vaihtoehtoja ja valtaosa niistä ei rasita verkkoa mitenkään dramaattisesti, mutta tämä tulee kuitenkin huomioida kapasiteetin suunnittelussa. Pääsääntöisesti tässä käytetään ohjelmistoja jotka monitoroivat verkon käyttöastetta ja raportoivat siitä kootusti. Tämä yleensä edellyttää yritykseltä omaa palvelinta, mutta esim. pienessä verkossa siihen voidaan käyttää yksittäistä tietokonetta. (The Art of Service 2009, 64-67).

Laitteiden tilaa ja saatavuutta voidaan monitoroida esim. SNMP protokollan avulla. Tällä saadaan jatkuvasti reaaliaikaista tietoja verkon laitteiden tilasta ja huomataan jos jokin laite lakkaa vastaamasta sille lähetettyihin kutsuihin. SNMP protokolla toimii seuraavalla tavalla. Laite jota halutaan tarkkailla pyörittää ohjelmistotasolla (joko erillinen moduuli laitteessa tai ohjelmiston aktivoitava ominaisuus) SNMP agent protokollaa joka kerää tietoa laitteen tilasta ja raportoi siitä eteenpäin. Verkossa on olemassa niin sanottu NMS (network management system) joka kerää tiedon agenttien lähettämistä tilapäivityksistä. NMS laite pyörittää ohjelmistoa jolla tarkkaillaan agenttien tilaa ja hallitaan niitä (vrt. operaattoriverkot ja monitoroidut internet yhteydet suurasiakkailla). Tällä voidaan kootusti antaa käskyjä verkonlaitteilla, ajaa päivityksiä, yms. Samalla saadaan reaaliaikaista tietoja jos laitteet lakkaavat vastaamasta ja voidaan reagoida tilanteen edellyttämällä vakavuudella. (ManageEngine, Zoho Corp. 2011).

SNMP on periaatteessa pohja minkä päälle on rakennettu useita erilaisia verkon käyttöastetta mittaavia ohjelmistoja. Näillä voidaan graafisen käyttöliittymän kautta mitata tietyn laitteen tiettyjä portteja. Samoin voidaan asettaa reunaehtoja joiden täyttyminen aiheuttaa hälytyksen monitoroinnissa (esim. Cacti).

Reititys. Millainen reititys verkossa on käytössä? Reititystaulujen ylläpidosta generoituva liikenne tulee myös huomioida kapasiteetissa sekä muut päivitykset mitä käytössä olevasta protokollasta aiheutuu. Tälle tulee varata tarpeeksi kaistaa, jotta verkko ei ruuhkaudu esim. topologia muutosten seurauksena. Tulee myös huomioida mikä reititysprotokolla kuormituksensa puolesta palvelee parhaiten verkkoa. Osa käyttää reitityspäivitysten lähettämiseen ja reititystaulujen ylläpitoon enemmän kapasiteettiä ja osa taas ruuhkauttaa verkkoa topologia muutosten yhteydessä.

Verkon koko on ratkaisevassa roolissa, samoin myös käytössä olevat laitteet. Mikäli verkossa käytetään useampaa kuin yhtä reititysprotokollaa tulee sekin olla huomioituna kapasiteetissa.

Varmistus. Kaikki data tulisi aina varmistaa, tavalla tai toisella. Mieluiten vielä useammalla eri tavalla. Varsinkin kun kyseessä on yritys. Riippuen käytettävistä sovelluksista, ja toimivatko ne yrityksen omilla palvelimilla vai onko palvelut ulkoistettu. Omien ylläpidettävien palvelinten tapauksessa voidaan lähteä asiaa suunnittelemaan ruohonjuuri tasolta. Itse palvelimien tulee hyödyntää vähintään RAID5-menetelmää käyttäviä kovalevyjä. Näin data saadaan jaetta useiden kovalevyjen välillä, joten vaikka pakasta yksi hajoaisi, data voidaan uudelleen luoda muiden levyjen avulla. Tämä perustuu pariteettidatan hajauttamiseen kaikkien pakan levyjen kesken. Tilaa tässä hukkuu yhden kovalevyn verran suhteessa muihin menetelmiin, mutta tämä on periaatteessa varma tapa säilyttää dataa ongelmatilanteen sattuessa. Samalla tulee huomioida itsensä palvelimen kahdennus. Suotavaa olisi, että yrityksellä olisi esim. useampi eri laitetila jossa on fyysisesti eri palvelin. Tällöin toisen palvelimen data voidaan replikoida myös muille palvelimille ja näin ollen pitää kahdessa tai useammassa fyysisessä sijainnissa ongelmien sattuessa (tulipalo tai muuta vastaavaa). Ainoan rajoituksen tähän asettaa verkon topologia ja kapasiteetti. Kahden eri fyysisen toimipisteen välillä tapahtuva replikointi kuitenkin vie melkoisen määrän varsinaista kapasiteetti runkoyhteydeltä. (The Art of Service 2009, 71-78).

Pullonkaulat ja analysointi. Verkko täytyy analysoida ennen toteuttamista ja tunnistaa mahdolliset ongelmat mitä tulevaisuudessa voi esiintyä kapasiteetin kanssa. Tällä ennaltaehkäisevällä toimenpiteellä voidaan välttää siis selkeitä pullonkauloja verkon toiminnan osalta. Tässä tulee huomioida kaikki seikat josta verkon kokonaisuus muodostuu.

Ongelman tunnistamisen jälkeen suunnitellaan verkko tavalla, jotta todennäköisimpiä ongelmakohtia ei ole mahdollista muodostua ja näin haitata verkon käytettävyyttä kapasiteetin osalta. Tulee huomioida vaihtoehtoisia menetelmiä redundanttisuuden varalta. Jos osa verkosta ei pysty toimimaan (laitevika tai vastaavaa) täytyy olla vaihtoehtoinen väylä datan liikuttamiselle. Tässä tulee toki huomioida kuinka tärkeästä liikenteestä on kyse. Mikäli liikenne ei ole kriittistä ei ole pakko olla redundanttista yhteyttä. Hyviä esimerkkejä missä yhteys on kahdennettu olisi esimerkiksi jonkin säiliön tai reaktorin monitorointi ja hallintaliikenne. Mikäli tällaisessa tilanteessa yhteydet katkeaisivat tai ruuhkautuisivat voisi seuraukset olla merkittävät. Tällöin tulee olla vaihtoehtoinen kanava datan välittämiseen. (The Art of Service 2009, 67-68).

Skaalautuvuus. Verkon ”koon”, käyttäjämäärien ja käyttöasteen kasvaessa, kuinka käy kapasiteetin? Suunnitellessa kokonaisuutta täytyy huomioida tulevaisuuden näkymät ja kehitys. Täytyy pyrkiä arvioimaan kuinka suurta kasvu on ja kuinka paljon siitä aiheutuvaan liikennemäärän kasvuun reagoidaan ennaltaehkäisevästi. Tässä tulee punnita taloudellista näkökulmaa suhteessa verkon käyttöasteen kasvunopeuteen ja tehdä päätös lisäkapasiteetin hankkimisesta sen pohjalta etukäteen. Verkon kokonaisvaltainen suunnittelu täytyy tehdä siltä pohjalta, että toteutusta voidaan nopeasti muuttaa ilman, että siitä seuraa massiivisia verkon topologisia muutoksia (fyysisiä tai loogisia).

Liikenteen luokittelu ja merkkaus , QoS. Riippuen verkon tarjoamista palveluista sen käyttäjille tulee kapasiteetin suunnittelussa huomioida liikenteen luokittelu. Kapasiteetti täytyy suhteuttaa tavalla, jotta tarvittavat liikenneluokat saavat haluamansa nopeudet ja toimintavarmuus voidaan taata. Liiketoiminnan näkökulmasta tärkeimmät sovellukset saavat korkeimman prioriteetin ja kaistanvaraus luokitellaan sen arvioidun käyttöasteen mukaan. Verkon optimaalisen toiminnan kannalta liikenteen luokittelu on melkeinpä pakollinen vaihe. Varsinkin, kun verkon koko kasvaa, asia nousee tärkeämpään rooliin. Liikenteen merkkausta ja luokittelua voidaan suorittaa melkein missä vaiheessa tahansa verkon topologiaa. Yleensä kapasiteetti ei kuitenkaan lähiverkon tai tietyn IP-osoite segmentin sisällä ei ole ongelma koska puhutaan ethernet tekniikasta. Tästä luonnollisesti seuraa se, että yleensä liikenteen luokittelu suoritetaan 3. tason laitteessa josta se lähtee ulospäin. Tämä voi olla ison yrityksen sisällä reitittä-

vä kytkin tai reititin. Luokittelua tehdään mahdollisesti myös useammassa laitteessa. (Cisco Systems Inc. 2011).

Perusperiaate liikenteen luokittelussa on merkata tietyn tyyppinen liikenne lipulla, joka merkitsee mihin luokkaan paketti kuuluu. Luokissa minkä verran kaistaa kyseiselle liikenteelle varataan. Pääsääntöisesti kaikki tärkeät sovellukset kulkevat korkeamman prioriteetin luokassa ja vähemmän tärkeä liikenne menee best effort liikenteenä. (Cisco Systems Inc. 2011).

Verkkolaitteet. Normaalissa verkossa (koosta riippuen) on useita eri verkkotason laitteita. Minimissään verkko koostuu vähintäänkin modeemista, joka toimii alkeellisena reitittimenä. Normaalisti verkossa on vähintäänkin oikea 3. tason reititin, joka tekee tarvittavat reititys ja liikenteenohjaus päätökset (riippuen lähiverkon jaosta tietysti) ja yleensä vähintään yksi kytkin reitittimen takana. (Leino 2009).

Kytkin pitää yllä MAC-taulua jossa on tiedot kaikista siihen liitettyjen laitteiden mac-osoitteet. Näin kytkin osaa suoraan välittää liikenteen saman lähiverkon ja ip-osoiteblokin sisällä toisilla verkkolaitteille ilman, että liikenteen tulee kiertää reitittimen kautta. Kytkimen toiminta tapahtuu OSI-mallin tasolla kaksi. (Leino 2009).

Reititin puolestaan toimii OSI-mallin 3. tasolla. Laite tekee kaikki reititys päätökset eri verkkojen välillä ja pitää yllä reititystaulua jonka mukaan reititys päätökset tehdään. Tämä esim. jos lähiverkosta lähtee liikennettä ulospäin tai jos käytössä on useampi eri aliverkossa toimiva segmentti. Tällöin liikenne segmentistä toiseen kulkee reitittimen kautta. Poikkeuksia tähänkin on, jos käytössä on reitittäviä L2-kytkimiä. Isommat verkot koostuvat mahdollisesti useammista reitittimistä ja useista kytkimistä. Reititystä tarvitaan varsinkin, jos yrityksellä on useita eri toimipisteitä esim. eri paikkakunnilla, mutta loogisesti kaikki kuuluvat samaan yritysverkkoon. (Leino 2009).

Palomuuri laitteet ovat myös yleisiä isommissa verkoissa. Näillä voidaan suoraan tarkkailla liikennettä jota verkon läpi kulkee. Tietysti samaa voidaan jossain määrin toteuttaa suoraan reitittimillä pääsylistojen muodossa. Mutta varsinaiset palomuurilaitteet on suunniteltu tekemään tarvittavat päätökset liikenteen suhteen jo suoraan raudassa, joten liikenteen prosessointinopeus on huomattavan paljon suurempi. Laitteilla voidaan laatia monimutkaisiakin käytäntöjä mitä liikennettä suodatetaan ja mitä salli-

taan läpi. Palomuuri laite tulee yleensä heti reunareitittimen (laite josta lähtevät yhteydet ulkomaailmaan) taakse loogisessa topologiassa. (Leino 2009).

IPS ja IDPS laitteet toimivat hieman samoin tavoin kuin palomuurilaitteet, mutta ne on suunniteltu tunnistamaan hyökkäykset verkkoa vastaan. Ne havaitsevat tiettyjen hyökkäys sormenjälkien perusteelle kuvioita (vrt. "pattern") sisään tulevassa ja ulos-lähtevässä liikenteessä. Näillä voidaan esim. havaita tietomurto yritykset sekä palvelunesto hyökkäykset. Itse lyhenne tulee sanoista Intrusion (Detection) Prevention Systems. (Leino 2009).

Kokonaisuudessaan tietoverkot voivat pitää sisällään paljon muitakin verkkolaitteita, mutta oleellisimmat ovat juuri verkon normaalitoimintaan liittyvät laitteet ja sen tietoturvasta ja liikenteen ohjaamisesta vastaavat laitteet.

Suojaus ja tietoturva. Kuten jo edellä mainittiin verkon laitteista, suojaus ja tietoturva on hoidettu monessa verkossa palomuuri ja IPS/IDS laitteilla. Tämä ei ole kuitenkaan ainoa vaihtoehto. Varsinkin pienemmissä verkoissa missä kyseisten laitteiden ylläpito ja hankkimiskustannukset olisivat liian suuret, voidaan turvautua muihin menetelmiin. Jokainen tietokone tulisi olla suojattuna sovelluspohjaisella palomuurilla ja virustorjuntaohjelmistolla. Liikennettä voidaan rajoittaa pelkällä reitittimelläkin tai jopa modeemilla luomalla näihin pääsylistoja tai porttiohjauksia. (Leino 2009).

Erittäin hyvä yleissääntö tietoturvan kannalta on "Estä oletuksena kaikki liikenne, ja salli läpi ainoastaan tarvitsemasi" (Leino 2009.). Monet lähtevät rakentamaan verkkoa ja sen suojausta vääristä lähtökohdista sallimalla ensin kaiken liikenteen ja sitten estämällä sitä tarpeen vaatiessa. Tämä tekee verkon alttiiksi hyökkäyksille ja haittaliikenteelle. Heti alusta pitäen, kontrolloidusti tietoturvaa rakentaen, voidaan verkko myös pitää turvallisena. Mikäli käytössä ei ole esim. reititintä tai modeemia jolla voitaisiin jonkinlaisia sääntöjä liikenteelle tehdä, voidaan asia toteuttaa ylimääräisellä tietokoneellakin. Kyseiseen koneeseen asennetaan jokin vakaa alusta (UNIX/LINUX) jonka päällä ajetaan jotain palomuuriohjelmistoa (esim. Shorewall). Kaikki ulos- ja sisäänpäin menevä liikenne ohjataan kyseisen koneen kautta, joka sitten tekee tarvittavat päätökset kuinka liikennettä ohjataan tai suodatetaan. Ongelmana tässä voi olla, että sisäänpäin tulee tarpeetonta liikennettä jos reunareitittimessä ei tehdä mitään lii-

kenteen suodatusta. Tällöin kaistaa menee hukkaan kun sisään lasketaan liikennettä joka kuitenkin suodatetaan muurilla heti pois. (Leino 2009).

Pääsylistoilla voidaan erittäin tehokkaasti rajata pois ei haluttua liikennettä esim. IP-osoitteiden perusteella, käytetyn protokollan perusteella, kohde portin perusteella jne. Reitittimissä tavanomaisesti rajoitetaan liikennettä suoraan IP-osoitteiden, protokollan ja portin perusteella. Pääsylistoja voi melko vapaasti muokata ja soveltaa tarpeisiinsa sopiviksi. Täytyy kuitenkin muistaa, että pääsylistat on helppoa luoda väärin. Rajoitetaan esim. turhaan tiettyä liikennettä tai päästetään suoraan sellaista läpi palomuurille asti minkä voisi suodattaa jo reitittimessä pois. Verkon tietoturvan suunnittelijan tulee huomioida nämä seikat tietoturvaa ja sen tehoa silmälläpitäen. (Leino 2009).

Suorituskyky. Kuten jo edellä mainittu laitteiden suorituskyky tulee myös huomioida. Riippuen verkon topologiasta ja missä vaiheessa liikennettä seulotaan, tulee hankkia oikeanlaiset laitteet joissa riittää tarpeeksi suorituskykyä tarvittavan toimintatason ylläpitämiseen. Esimerkiksi reunareititin on tärkeässä asemassa. Jos laitteella ajetaan mitään raskaampaa reititysprotokollaa, (BGP) tai mahdollisesti useampia eri reititysprotokollia, tulee laitteella olla tarpeeksi suorituskykyä, jotta se voi ylläpitää suuria reititystauluja sekä tehdä tarvittavat reitityspäätökset tarvittavan nopeasti. Sama pätee käytössä oleviin palomuuri ja IPS/IDS laitteisiin. Nämä laitteet on pääsääntöisesti suunniteltu tekemään raskaammat päätökset jo suoraan "raudassa" sovelluspuolen sijaan. Tällöin saavutetaan suuremmat tehokkuudet päätösten tekemisessä. Jos käytetään muita kuin erillisiä palomuurilaitteita (kuten edellä mainittu esim. palvelin kone jossa sovelluspohjainen palomuuri) tulee huomioida tässä erityisesti laitteen kuormitus ja mitoittaa käytettävä laitteisto sen mukaan. (The Art of Service 2009, 64-65).

4.1.5 Access-tekniikat

Kun tarkastellaan mahdollisia yhteysvaihtoehtoja täytyy tarvittavan kokonaiskapasiteetin olla jo selvillä. Kun tämä tarve on tiedossa niin voidaan suunnitella kustannustehokkain vaihtoehto runkoyhteydeksi ulkomaailmaan. Kaikkia tekniikoita ei varsinkaan suomen sisällä ole joka paikkakunnalla saatavilla, mutta vaihtoehdot tulee kartoittaa mahdollisimman tarkasti ennen päätöksen tekemistä. Varsinkin jos kyseessä on yritys jolla on useampia toimipisteitä eri paikkakunnilla.

Yleensä kustannusten kannalta paras vaihtoehto on valita operaattori joka voi tarjota yhteydet kaikille paikkakunnille. Jos valitaan eri paikkakunnilla sijaitseville toimipisteille eri palvelun tarjoajat tulee kokonaisuuden rakentamisesta vaikeampaa mikäli halutaan rakentaa yhtenäinen yritysverkko. Tällöin saadaan myös keskitettyä viankorjausprosessi yhden operaattorin vastuulle. Voitaisiin tähän todeta, että mitä useampi kokki on samassa sopassa, sitä "byrokraattisemmaksi" viankorjaus muodostuu.

ADSL-yhteydet ovat ehkä yleisimpiä käytössä olevia yhteysmuotoja suomessa tällä hetkellä. Kyseisessä tiedonsiirto menetelmässä käytetään hyväksi vanhoja lankapuhelin (kuparikaapeli) linjoja. Nopeudet vaihtelevat tekniikassa nykyään yleisimmin välillä 512k - 24M. Myös 256k nopeus on saatavilla, mutta sitä ei operaattoreiden toimesta aktiivisesti tarjota. ADSL oli ensimmäinen askel pois hitaammista soittosarjan modeemeista jotka pystyivät maksimissaan 56kt nopeuteen. Tämän jälkeen tuli ISDN tekniikka jossa suurin nopeus oli 128kt. ADSL on edelleen erittäin laajasti käytössä alueilla missä ei ole mahdollisuutta saada yhteyksiä kaapeliverkon kautta tai kuitu/ethernet yhteydellä. Nopeuteen vaikuttaa asiakkaan päätelaitteen etäisyys palveluntarjoajan puhelinkeskuksesta eli siis kuparikaapelin pituus. Yleisesti ottaen alle 3km linjapituuksilla päästään nopeusluokkiin 8M-24M ja mitä pitemmäksi kuparikaapelin pituus kasvaa, nopeudet pienenevät. Pitkästi yli 4km linjalla yhteys ei välttämättä toimi kuin 256k - 4M nopeudella. (Siltala 2008).

Yhteydet rakentuvat asiakkaan päätelaitteesta, josta yhteys lähtee RJ11-liitännällä varustettua puhelinkaapelia pitkin puhelinpistokkeeseen. Täältä kuparipari menee talojakamolle josta yhteys lähtee edelleen kuparikaapelia pitkin välijakamoiden kautta palveluntarjoajan puhelinkeskukselle. Täällä yhteys kytkeytyy DSLAM laitteeseen, josta se ohjautuu operaattorin IP-verkkoon. ADSL muodostui kuluttaja ystävälliseksi sen suuren latausnopeuden (suhteessa upload nopeuteen) ansiosta. Upload kaistan nopeus vaihtelee yleisesti ottaen 512k - 2M välillä normaali yhteyksissä. Tämä johtuu siitä, että DSLAMin päässä kuparilangat ovat monesti isona "vyyhtinä" jonka seurauksena keskuksen päässä on enemmän ylikuulumista linjojen välillä. Tämän takia upload puolen signaali on heikoin ja siksi päästään vain matalampiin nopeuksiin. Asiakaspäässä tilanne on toinen, sillä siellä ei vastaavaa ylikuulumista tapahdu samassa mittakaavassa. Tämän vuoksi päästään suurempiin nopeuksiin. Normaalissa kuluttaja käytössä ei upload kaistanopeutta juurikaan tarvita jos ei ole käytössä esim. omaa

palvelinta tai vastaava joka tarvitsee upload kaistaa datansiirron kannalta. ADSL-toimii myös yrityksen käytössä, mutta tässä tulee huomioida myös upload kaistan nopeus suhteessa yrityksen tarpeisiin. Mikäli tarve ei ole suuri, adsl soveltuu oikein hyvin myös yritysten käyttöön. (Siltala 2008).

Nykyään ADSL tekniikka perustuu DMT-modulointiin, joka otettiin yleiseksi standardiksi 1996 vuoden jälkeen. Tätä ennen käytössä oli CAP. Upstream (yläkaista) -taajuudet ADSL yhteyksissä ovat väliltä 26,000 kHz - 137,825 kHz. Downstream (alakaista) -taajuudet ovat väliltä 138 kHz - 1104 kHz. DMT-moduulaatiolla nämä taajuusvälit jaetaan vielä pienempiin taajuuskanaviin. Yhteyttä muodostaessa jokainen näistä pienemmistä taajuuskanavista neuvottelee vastapuolen kanssa sopivan SNR (signal to noise ratio, signaalikohina -suhde) arvon. Tähän vaikuttaa suoraan linjan pituus ja kuparikaapeleiden laatu, ylikuuluminen ja laitteiden tuottamat sähköiset häiriöt. Mitä parempi SNR arvo linjalle neuvotellaan, sitä suurempiin nopeuksiin voidaan päästä. Luvattuun nopeuteen ei aina päästä sillä osa kaistasta varataan aina kehysrakenteiden (prokolla ja synkronointi) siirtämiselle (protocol overhead). Tämän seuraksena varsinaiseen datansiirtoon jää yleensä 80-90% varsinaisesta nopeudesta. Operaattorit käyttävät normaalisti sellaisia ADSL linjaprofiileja missä tuo overhead on huomioitu jo suoraan. Esim. 12M nopeudella myydyssä liittymässä on yleisimmin käytössä 14M nopeusprofiili juuri tästä syystä. Profiilit ovat yleensä joko fastpath tai interleaved profiileja. Fast -profiilissa lähetetään yksi paketti kerrallaan. Tämä johtaa siihen, että paketteja saadaan lähetettyä suuremmalla nopeudella ja pienemmällä vasteella, mutta tällainen yhteys on virheille alttiimpi. Mikäli linja virheilee saattaa vasteet nopeasti nousta korkeammaksi uudelleen lähetyksien takia. Interleaved -profiilissa paketit lähetetään 8-64 paketin ryppäissä jolloin niihin voidaan hyödyntää paremmin Reed-Solomon virheenkorjausta. Tämä tekee pakettiryppäästä vastustuskykyisemmän virheille, koska paketteihin lisätään ylimääräinen kehys, jonka pohjalta voidaan virheellinen paketti havaita ja korjata tehokkaammin. Tämä kuitenkin aiheuttaa suuremman viiveen, koska joudutaan odottamaan suurempi aika ennen pakettinipun lähettämistä. Fastpath on yleisemmin käytössä normaaleissa ADSL yhteyksissä ja Interleaved profiilia käytetään enemmän esim. IP-tv lähetyksen yhteydessä koska kuva on herkempi virheille. (Siltala 2008).

VDSL on ADSL yhteyksien tapaan tekniikka jolla siirretään dataa kuparikaapeleiden yli. Datan siirto tapahtuu taajuusalueella 25kHz - 12MHz. Koska dataa siirretään suuremmilla taajuuksilla, päästään suurempiin teoreettisiin nopeuksiin kuin ADSL-yhteyksillä. Nopeudet ovat maksimissaan luokkaa 52Mbit/s (downstream) ja 16Mbit/s (upstream). Korkeammista taajuuksista johtuen kuparikaapelit ovat suuremmassa roolissa datansiirron kannalta. Huonolaatuiset kuparikaapelit aiheuttavat nopeasti tilanteen jossa VDSL yhteys ei toimi kunnolla. **VDSL2** on uudempi standardi jossa taajuudet nousevat aina 30 MHz:iin asti. Tämän tekniikan teoreettinen maksimi on 100Mbit/s. Jos kuparikaapeleiden etäisyydet kasvavat yli 300 metrin mittaisiksi alkaa signaali vaimentua nopeasti. VDSL2-yhteydet on monesti yhdistetty ethernetkaapelointiin tai kuituyhteyksiin suomessa. (Telecommunication standardization sector of ITU 2006, 11, 15-22, 25-26).

HDSL on tekniikka joka ei ole suomessa käytössä. Tätä hyödynnetään Amerikassa ja Japanissa. Kyseessä on aikajanalla mitattuna ensimmäinen nopeampi xDSL-tekniikka. Tekniikka voitaisiin jaotella karkeasti T1- ja E1-standardiin. T1 mahdollistaa nopeuden 1,544 Mbit/s asti. E1 nostaa ylärajaa ja mahdollistaa nopeuden 2 Mbit/s asti. Kyseisessä tekniikassa käytetään edelleen hyväksi kuparikaapeleita. Käytetyistä taajuuksista johtuen joudutaan linjalla käyttämään toistimia 1-2 kilometrin välein jotta signaali ei vaimennu liikaa. Tämä tekee tekniikasta melko virhealttiin, koska toistimia on monesti paljon. HDSL:n ansiosta kehitettiin HDSL2 ja S(H)DSL tekniikat. (Telecommunication standardization sector of ITU 2006, 1-13).

SHDSL-tekniikassa käytetään hyväksi myös olemassa olevaa puhelinverkkoa. Esimerkiksi ADSL-tekniikasta poiketen tiedon siirto on symmetristä (upload ja download -kaistaa saman verran). Tämä johtuu vanhan POTS (puhelinverkkojärjestelmän) ominaisuuksista. Käytössä oleva modulaatio ja taajuudet ovat samat joita käytettään POTS-verkossa. Tästä seuraa myös se, että asiakas ei voi käyttää analogisuodatinta asiakaspäässä. Eli lankapuhelinta ei ole mahdollista käyttää samassa osoitteessa niinkuin ADSL-yhteyden kanssa. Kuitenkin, koska downstream ja upstream kaistat ovat yhtä suuria, tämä tekniikka on varteenotettava vaihtoehto varsinkin monelle yritykselle. (Telecommunication standardization sector of ITU 2004, 1, 6-7).

SHDSL-yhteys on mahdollista rakentaa joko yhdellä kupariparilla tai kahdella. Erona tässä on tietenkin nopeus. Kun on käytössä yksi kuparipari niin nopeus voi olla väliltä

192 kbit/s - 2304 kbit/s. Jos käytössä on kaksi kupariparia niin nopeus on tuplasti tämä, eli 384 kbit/s - 4608 kbit/s. Samat lainalaisuudet pätevät SHDSL-tekniikkaan kuin ADSL-tekniikkaankin. Kuparikaapelin pituus rajoittaa toimintaa, mitä pitempi kaapeli sitä suurempi vaimennus linjalla on.
(Telecommunication standardization sector of ITU 2004, 6-9, 61-64).

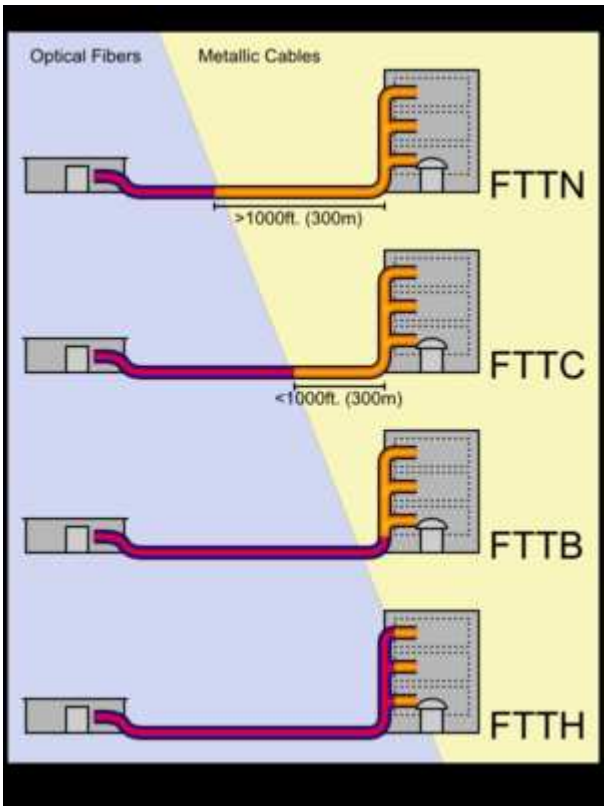
Operaattorin runkoverkon puolella käytössä on samat laitteet kuin ADSL-yhteyksienkin kanssa. DSLAM:lta on varattu kaksi (yleensä vierekkäistä) porttia SHDSL yhteyksille. Ainoa ero ADSL:ään nähden on, että DSLAM:ssä on erillinen SHDSL moduulikortti johon yhteydet päätetään. Nämä kaksi liitäntää paritetaan (bondataan) toisiinsa, jolloin saadaan aikaan kaksiparinen SHDSL-yhteys. Mikäli asiakkaalla on käytössään vain yksiparinen yhteys ei bondausta tarvitse tehdä. Tämä on varsin hyvä ratkaisu yrityksille jotka tarvitsevat suuremman upstream-kaistan esim. palveluidensa tarjoamiseen.

Kaapelimodeemi yhteydet ovat yleisiä suurempien kaupunkien alueilla. Yhteys tarjotaan olemassa olevaa tv-kaapeliverkkoa pitkin. Toiminnallisuudeltaan tekniikka eroaa xDSL-yhteyksistä. Tämä on toinen yleisimmin käytössä oleva "langallinen" yhteys tapa suomessa. Operaattorit käyttävät olemassa olevaa kaapeli-tv verkkoa hyväkseen datan siirrossa. Kyseiset liittymät käyttävät erityisiä kaapelimodeemeja asiakkaan päätelaitteina. Laite kytketään koaksiaalikaapelilla tv-antennipistokkeeseen josta yhteys menee operaattorin verkkoon. Operaattorin keskuksella on CMTS (cable modem termination system) joka on toiminnallisesti verrattavissa xDSL yhteyksissä käytettäviin DSLAM:eihin. CMTS:stä lähtee ethernet yhteydet operaattorin runkoverkon suuntaan ja kuluttajan suuntaan laitteesta löytyy koaksiaaliliitännät. Eri CMTS:ät voivat palvella tiettyä määrää kaapelimodeemeja laitteesta riippuen. Kaapeliverkko onkin näin jaettu eri segmentteihin. Näin ollen varsinainen kapasiteetti jaetaan tietyn käyttäjämäärän kesken. Asiakkaan päätelaitteet tunnistetaan verkkoon laitteen MAC-osoitteen perusteella. Tämä tulee olla tiedossa operaattorin päässä jotta yhteys voidaan muodostaa. Tämän jälkeen kyseinen modeemi toimii missä tahansa kyseisen operaattorin kaapeli-tv verkossa (osalla operaattoreista). Kapasiteettia rajoittaa CMTS-yksiköiden down- ja upstream porttien määrä. Pääosin nopeudet voivat yltää asiakkaalle downstreamin osalta 100Mbit/s asti ja upload 20Mbit/s asti, mutta jaetun kapasiteetin vuoksi tämä ei aina toteudu, varsinkaan ruuhka-aikoina.

CMTS:ät käsittelevät tavallisesti vain IP-liikennettä. Asiakkaalta päin tulevien IP-pakettien siirtämisessä käytetään QAM64 ja QAM256 modulaatiota. (Siltala 2008).

Kuituyhteydet yleistyvät suomessa jatkuvasti. Tämä onkin tällä hetkellä nopein tiedonsiirto tapa mikä voidaan hankkia. Samalla se on operaattoreiden näkökulmasta myös paikoitellen halvempaa ylläpitää kuin vanha kuparikaapeli. Kuitukaapeli itsessään on kalliimpaa ja vaurioituu herkästi, joten sen vetäminen ei ole halpaa ja tästä syystä kaikki operaattorit eivät ole laajentaneet kuituverkkoon kovinkaan agressiivisesti. Olemassa olevan kaapelin ylläpito sen sijaan on halvempaa kuin vanhojen kuparikaapeleiden.

KUVIO 9. FTTx-mallit



(Wikipedia 2011).

Kuituyhteydet kuten kuparikaapeliyhteydetkin kärsivät vaimennuksesta pitkillä matkoilla. Vaimennus on kuitenkin huomattavasti vähemmän kuituyhteyksissä. Yleisesti ottaen kuituyhteydet on toteutettu neljällä eri tavalla. Englannin kielinen termi mitä näistä käytettään on Fiber-to-the-x eli FTTx.

Ensimmäinen tapa on kuituyhteys, missä osa yhteydestä on toteutettu vanhoilla kuparikaapeleilla. Koska tällä saadaan kuparikaapelin matkaa lyhyemmäksi saadaan yleensä paremmat nopeudet kuin perus adsl-liittymien kanssa. Käytössä voi olla tämän kanssa myös VDSL (ja yleensä onkin) jolloin päästään olemassa olevalla kupariosuudella vielä suurempiin nopeuksiin. Tätä vaihtoehtoa kutsutaan lyhenteellä FTTN (fiber-to-the-node or neighborhood). Kuituyhteys tulee siis periaatteessa jollekin välijakamolle tai useammin keskukselle, mutta kuitenkin vielä pitemmän matkan päähän asiakkaasta. Tätä termiä käytetään jos kuparikaapelin pituus on kuitenkin useita kilometrejä. Nyrkkisääntönä voitaisiin puhua, että jos kuparikaapelia on yli 300 metriä voidaan käyttää FTTN termiä. (PennWell Corporation 2011).

Seuraavana tulee FTTC (fiber-to-the-cabinet or curb). Tässä toteutuksessa kuitu yltää lähemmäs asiakkaan tiloja. Tavallisesti kuitu tulee jollekin välijakamolle, joka sijaitsee 300 metrin säteellä asiakkaan tiloista. Varsinkin tällaisissa tapauksissa VDSL2-yhteydet ovat yleisiä. Kun kuparikaapelin pituus lyhenee, nopeudet paranevat käytetystä tekniikasta riippuen huomattavasti. (PennWell Corporation 2011).

Seuraavana on FTTB (fiber-to-the-building or basement). Kuten nimikin kertoo, tässä vaihtoehdossa kuitu tulee suoraan kiinteistöön asti. Asiakkaan laitetilassa on kuitumuunnin ja operaattorin hallitsema kytkin. Kuitu tulee kiinni kuitumuuntimeen josta se jatkaa ethernet kaapelilla kytkimelle ja yleensä Gigabit ethernet porttiin. Tämä runkokapasiteetti on sitten rajoitettu porttikohtaisesti. Vapaista 100M porteista vedetään ethernet kaapelointi asuntoihin joissa on yleensä oma kotijakamo, jolla yhteys voidaan jakaa halutulla tavalla asunnon sisällä. (FTTH Council 2006, 1-2).

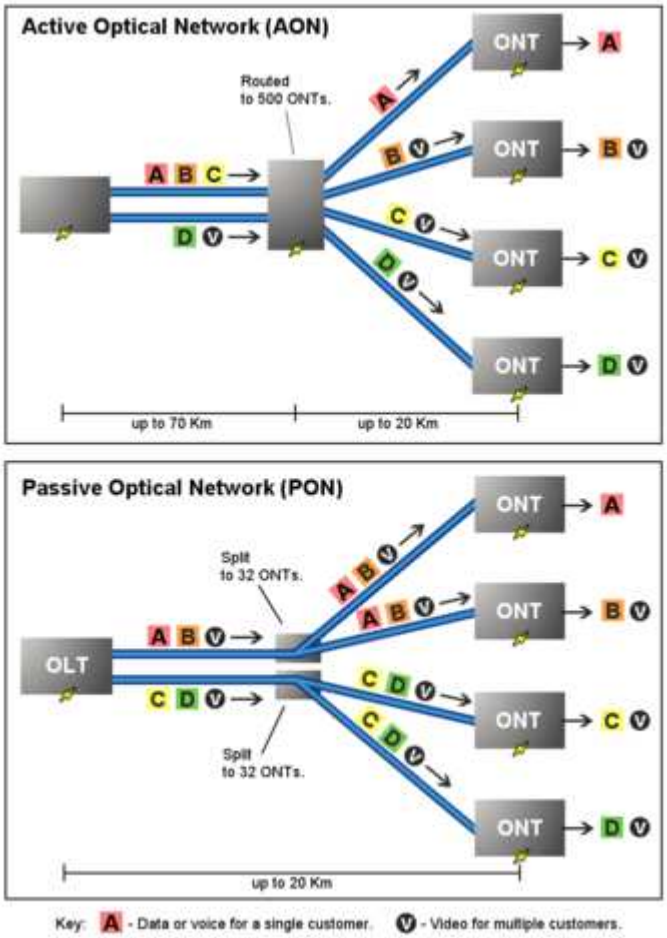
Viimeisenä on FTTH (fiber-to-the-home). Kuten nimi kertoo, tässä kuituyhteys tulee suoraan asiakkaan tiloihin ja asiakkaalla täytyy olla kuitumuunnin josta hän itse jakaa yhteytensä haluamallaan tavalla. (FTTH Council 2006, 1-2).

Näissä edellä mainituissakin vaihtoehdoissa on erilaisia toteutuksia. Pääsääntöisesti toteutus on tämä, mutta kapasiteetti saattaa olla jaettu useammassa vaiheessa. Vaihtoehtoisesti löytyy yhteyksiä joissa kapasiteetti ei ole jaettu kenenkään kanssa. Näistä voitaisiin käyttää termejä Direct cable (ei jaettua kapasiteettiä) ja Shared cable (kapasiteetti jaetaan suuremman käyttäjämäärän kesken). Shared cable on näistä yleisimmin

käytössä oleva menetelmä. Direct cable on operaattoreiden itsensä käyttävä menetelmä sekä suurempien yritysten käytössä.

Varsinkin Shared Cable -tekniikan kanssa käytettään kahta toteutustapaa, AON (Active Optical Network) ja PON (Passive Optical Network).

KUVIO 10. AON-verkko ja PON-verkko



(Wikipedia 2011).

AON -tekniikkasta (P2P, point-to-point) puhuttaessa tarkoitetaan pakettikytkentäistä ethernet verkkoa johon runkoyhteys tuodaan kuidulla. Nämä liittymät ovat yleensä EFM (ethernet in the first mile) verkkoja. Operaattorilta tulee kuitu tiettyyn pisteeseen verkkoa, josta se jaetaan ethernet kaapeloinnin ja kytkinten avulla asiakkaille. Kokonaisuus muodostaa yhden pakettikytkentäisen verkon. Tällainen kuituyhteys saattaa

käsittää esimerkiksi satoja kuluttajaliittymiä. Liikenne voidaan suoraan ohjata oikealla asiakkaalle ja sitä ei tarvise lähettää broadcast liikenteenä kaikkille laitteille vaan unicastina / multicastina. (FTTH Council 2006, 2-5).

PON -tekniikassa (P2MP, point-to-multipoint) operaattorilta tuleva kuitu jaetaan asiakkaille splittereiden ja kuitumuuntimien avulla. Periaatteessa kyseessä on point-to-multipoint -yhteys. Itse verkko tässä tapauksessa ei ole täysin ethernet verkko kuten AON tapauksissa. Splitterin avulla voidaan verkkoa segmentoida paremmin. Tässä toteutuksessa liikenne lähtee yleensä broadcastina splitterin suuntaan joka levittää sen eteenpäin myös broadcastina. (Da Silva 2005, 11-23).

Mobiili-access tekniikat ovat yleistyneet suomessa kovasti. Tekniikat voidaan jaotella selkeästi käytettyjen menetelmien ja tiedonsiirron nopeuden mukaan. Harva niistä soveltuu kuitenkaan varsinaisesti pienenkään yrityksen pääyhteydeksi, mutta tietyissä tilanteissa niitä voidaan myös käyttää ja hyödyntää.

GPRS-tekniikka oli ensimmäisiä pakettidatan siirtomuotoja mobiiliverkossa. Se on edelleenkin käytössä nykyään, mutta pienemmissä määrin. Kun puhutaan GPRS-verkosta, voitaisiin yhtä hyvin käyttää termiä 2G (2.5G) verkko. GPRS-verkko on käytännössä jatke vanhalle GSM verkolle joka tarjoaa perus puhepalvelut. GRPS-verkon puolella voidaan siirtää suurempia määriä dataa, mutta nykymittapuulla puhutaan erittäin matalista tiedonsiirtonopeuksista. Samat ongelma kuin muissakin mobiilitekniikkaa hyväksikäyttävissä tiedonsiirtomenetelmissä ovat läsnä. Koska GPRS-verkossa siirtyvä data on best-effort liikennettä ovat latenssit vaihtelut suuret sekä matalat nopeudet normaalia. Itse datansiirtonopeus vaihtelee välillä 56-114kbit/s. Tekniikka on siis edelleen suomessa käytössä alueilla joilla ei ole kattavampaa kuuluvuutta kuin 2G verkoilla. (Telecom Forum 2011).

EDGE-tekniikka on kehittyneempi menetelmä datansiirrolle normaalissa GSM-verkossa. Se voidaan toteuttaa olemassa olevan GPRS-tekniikan päälle ja tällöin päästään suurempiin datanopeuksiin pakettidatan siirrossa. Suomessa kyseinen tekniikka on varsin laajasti käytössä. Yleisesti sitä voidaan luonnehtia 2.5G:ksi. Koska Edgen tekniikka on käytännössä sama kuin GPRS:n (lukuun ottamatta edge-yhteensopivia vastaanotinyksiköitä) suuremmat nopeudet saadaan sovelluspohjaisesti. Kasvaneet nopeudet johtuvat edgen käyttämästä modulaatiosta ja signaalin koodauksesta. Edge

käyttää signaalin siirrossa GMSK ja 8PSK modulaatiota signaalin koodauksessa ja siirrossa. Tämä johtaa siihen, että nopeus verrattuna normaaliin GPRS-verkkoon kolminkertaistuu. Edge-tekniikalla päästään nopeuksiin 236,8kbit/s jos käytössä on neljä timeslottia. Teoreettinen maksimi on 473,6kbit/s jos käytössä on kahdeksan timeslottia. Varsinaiseen signaalin ja koodauksen EDGE käyttää yhdeksää modulaatio ja koodaus menetelmää verrattuna GPRS:n neljään. (Ericsson 2009, 3-15).

Edgestä on olemassa nopeampi version nimeltä Evolved EDGE. Tämä mahdollistaa vielä normaalistakin Edge-tekniikasta korkeammat latausnopeudet ja pienentää latenssiä. Latenssin pieneminen perustuu lähetysajan intervalleihin. Normaalisti aika lähetysten välillä on 20ms luokkaa mutta Evolded Edgen kanssa se on 10ms. Samoin signaalin modulointiin ja koodaukseen käytetään 32QAM- ja 16QAM-modulointia 8PSK:n sijaan. Tällä mahdollistetaan nopeudet jopa 1Mbit/s asti. Samoin latenssi tällaisilla nopeuksilla pienenee 80ms:iin (kahdeksan timeslottia). Tämäkin muutos voidaan tehdä sovellustason päivityksillä operaattoriverkkoon, joten se on yleisesti käytössä. (Ericsson 2009, 3-15).

UMTS-tekniikka oli periaatteessa ensimmäinen 3G-tekniikka joka omaksuttiin käyttöön suomessa. Tekniikka on erittäin laajasti edelleen käytössä GSM-verkoissa. Itse pakettidatan siirto perustuu W-CDMA tekniikkaan (Wideband code division multiple access) jolla mahdollistetaan suuremmat nopeudet. UMTS-tekniikka poikkeaa EDGE-tekniikasta, joten se tarvitsee omat laitteet toimiakseen ja olemassa olevaa tekniikka ei voida sellaisenaan käyttää hyväksi. Tekniikalla päästään jopa 45Mbit/s teoreettisiin nopeuksiin kun sitä käytetään yhdessä HSPA+ tekniikan kanssa. Käytännössä nopeudet ovat yleensä maksimissaan 7.2Mbit/s luokkaa käyttäjille, mutta kuten aina, latenssi saattaa olla ajoittain ongelma kuten myös itse nopeus. Itse UMTS on pohja jonka päälle 3.5G ja 4G tullaan rakentamaan. 3.5G onkin jo pitkällä käytössä Suomessa, mutta 4G on vasta tuloillaan valtaosalle alueista. Varsinainen liityntä menetelmä (vrt. Air Interface) jota käytetään kun yhteys avataan UMTS-verkkoon on W-CDMA. Tämä on myös suomessa yleisesti käytössä oleva menetelmä yhteyksien muodostamiseen mobiiliverkossa. W-CDMA:lla avataan pari 5MHz leveitä kaistoja. Alunperin UMTS-verkoissa määritellyt taajuusalueet ovat 1885-2025 MHz (uplink) ja 2110-2200 MHz (downlink). UMTS2100 on yleisimmin käytössä oleva taajuus, mutta myös

UMTS900 on suomessa yleinen varsinkin haja-asutus alueiden vuoksi.
(Poole 2011).

HSPA koostuu HSPDA ja HSUPA tekniikoista. Tai tarkemmin sanottuna, on näiden tekniikoiden fuusio. Nopeudet HSPA:lla vaihtelevat teoreettisessa maksimissaan 14Mbit/s downlink ja 5,76Mbit/s uplink. Myös latenssit ovat pienemmät kuin muissa tekniikoissa. Tekniikalla voidaan lähettää yhtäaikaisesti useammilla kanavilla jaettua dataa, joten se pystyy hyödyntämään WCDMA:ta paremmin. Myös datan lähetyksellä on pienempi TTI (Transmission Time Interval) joten näin saadaan pienemmät latenssit datan siirrolle. Datan siirrossa käytettään 16QAM ja 64QAM modulointia. Nopeudet ovat samaa luokkaa WIMAX-verkkojen kanssa, mutta näiden käyttöönotto on kustannuksiltaan halvempi prosessi kuin rakentaa WIMAX-verkko joka vaatii aivan oman tekniikkansa. Tästä syystä WIMAX ei ole ikinä saavuttanut suosiota Suomalaisten operaattoreiden keskuudessa. Olemassa olevaa verkkoa on huomattavasti helpompi lähteä kehittämään kuin lähteä rakentamaan uutta verkkoa vanhan toimivan päälle. (3GPP 2011).

HSPA+ on 3GPP:n kehittämä parannus olemassa olevaan HSPA verkkoon. Tätä kutsutaan myös nimellä Evolved HSPA. Tällä tekniikalla ylletään jo 84Mbit/s (downlink) ja 22Mbit/s (uplink) nopeuksiin. (3GPP 2011).

Suomessa muihin tekniikoihin ei ole juurikaan mahdollisuutta ja sijainti rajoittaa sitä mitä on saatavilla. Suurten asutuskeskusten ja kaupunkien yhteydessä yleensä valinnan vara on suurempi. Pienempien kuntien kohdalla mahdollisuudet rajoittuvat yleensä yhden operaattorin tarjoamiin palveluihin. Esim. WIMAX ei ole koskaan kehittynyt suomessa kattavaksi verkoksi. Tämä oikeastaan siitä syystä, että operaattoreiden on ollut helpompi päivittää olemassa olevat verkkonsa kuin lähteä rakentamaan uutta WIMAX-verkkoa ruohonjuuritasolta.

4.2 Palvelunhallinta

Palvelunhallinta on yksi tietoverkkojen monimuotoisimmista käsitteistä. Tähän löytyy useita eri malleja ja standardeja mitä voidaan käyttää sen toteuttamisessa hyväksi. Palvelunhallinnalla tarkoitetaan verkon kokonaisuuden hallintaa. Kuinka verkkolait-

teiden monitorointi on toteutettu? Kuinka muut verkonpalvelut on toteutettu? Miten toimitaan vikatilanteissa? Kuinka menetellään verkkoa päivittäessä? Kuinka verkon ylläpito on toteutettu? Millaiset SLA:t ovat operaattorin kanssa? Palvelunhallintaan liittyy erittäin monia kysymyksiä. Tässä luvussa käydään läpi palvelunhallinnan perusteita ja teoriaa.

Kokonaisvaltaisesti voitaisiin palvelunhallinta summata seuraavien alueiden kokonaisuudeksi, palvelun tuottaminen, sovellusten hallinta, palvelun tukitoiminnot, ylläpito ja verkkojen sekä palvelinten ylläpito ja kehittäminen. Pyritään pitämään palvelun laatu ja palvelutaso korkealla hallitsemalla kokonaisuutta järjestelmällisesti, proaktiivisesti, laadukkaasti ja kustannustehokkaasti. Näin varmistetaan tietty taso tuotetuille palveluille ja myös niiden korkean tason säilyminen. (Hautamäki 2009).

Nykyään kovasti yleistynyt on ITIL, joka käsittää kokoelman hyviksi havaituista metodeista ja menetelmistä IT-palvelun hallinnassa. ITIL ei suinkaan ole ainoa käytössä olevan palvelunhallintamalli. TOM ja eTOM olivat pitkään käytössä monilla suomalaisilla operaattoreilla ja samaa mallia hyödynnetään varmasti myös isoissakin yrityksissä. TOM ja eTOM olivat kehitetty juuri operaattoritason palveluidenhallintaan joten siitä syystä ne olivat erittäin yleisesti käytössä sillä tasolla. Monet ovat kuitenkin siirtyneet pikkuhiljaa ITIL:n tarjoamaan malliin. ITIL poikkeaa siinä muista palvelunhallintamalleista, että sitä ei ole suunniteltu suoraan operaattoritason palvelunhallintaan. ITIL kuitenkin on kokoelma parhaita käytäntöjä palvelunhallinnasta, joten se on helpommin sovellettavissa yrityksienkin palvelunhallinnan toteuttamiseen. (Hautamäki 2009).

Myös BS 15000 on yleinen käytössä oleva standardi. Ilmestyessään tämä oli ehkä kokonaisvaltaisempi ja kuvaili spesifisti kuinka palvelunhallinnan prosessit olisi tehokasta toteuttaa. (Hautamäki 2009).

Valtaosa palvelunhallinta malleista ja standardeista rakentuu "samojen" perusosien varaan. Jokaisen niistä tulee kuitenkin ottaa kantaa samoihin peruskysymyksiin. Näitä voitaisiin jaotella esim. seuraaviin osa-alueisiin:

- Palvelut
- Kapasiteetti

- Käytettävyys ja jatkuvuus
- Monitorointi ja raportointi
- Kustannusten ja taloudenhallinta
- Muutoshallinta
- Käyttöönoton hallinta
- Poikkeamien hallinta
- Laitteiden hallinta ja konfiguraatiot
- Ongelmien hallinta
- Organisaation hallinta
- Tietoturvanhallinta

(Hautamäki 2009).

Samat teemat toistuvat jokaisessa standardissa tavalla tai toisella. ITIL:ssä ja BS 15000 standardeissa ne on tuotu selvimmin esille. Kustannus ja talouden hallinta käsitteenä ei ole jokaisessa standardissa kuitenkaan. Tätä ei ole aina mielletty varsinaiseksi osaksi IT-palveluidenhallintaa, mutta todellisuudessa tämä myös on olennainen osa kokonaisuutta. (Hautamäki 2009).

Riippumatta yrityksen koosta, toimivan palvelunhallintamallin käyttö on suositeltavaa. Tämän pohjalta voidaan kuitenkin laatia selkeät toimintamallit jokaiseen tilanteeseen. Tämä taas nopeuttaa ongelman ratkeamista kun sellainen esiintyy. On aina helpompaa noudattaa edeltäkäsin laadittua mallia kuin soveltaa tilanteen mukaan. Varsinkin suuressa mittakaavassa tästä saadaan suuri hyöty.

Käydään esimerkkinä läpi pääpiirteittäin yleisimmin käytössä olevat palvelunhallinta mallit, ITIL ja ISO/IEC20000 sekä BS 15000.

4.2.1 ITIL v3

ITIL ei suoranaisesti oli varsinainen standardi mitä palvelunhallintaan tulee vaan enemmänkin kokoelma parhaita käytäntöjä hyvän palvelunhallinnan saavuttamiseksi. Menetelmä on jalostunut pikkuhiljaa ja se alkaa nykyään olemaan kuitenkin de facto jonka mukaan yritykset rakentavat palvelunsa. Tehokkaaksi ja toimivaksi sen tekee siihen kerättyjen menetelmien määrä ja pitkä aikajana jonka perusteella toimivimmat

prosessit on siihen valittu. ITIL pitää sisällään parhaita prosesseja useiden vuosikymmenten ajalta.

Erona moneen muuhun standardiin, ITIL on periaatteessa kaikkien käytössä oleva työkalu. Sitä ei omista mikään yksittäinen taho kuten esim. BS 15000 (British Standards Institute). Näin ollen kuka tahansa voi kehittää, soveltaa, kouluttaa ITIL:iin liittyviä asioita. Ainoana edellytyksenä on, että ITIL:iä käyttävä yritys rekisteröityy ITIL:in käyttäjäfoorumeille ja sertifioituvat ITIL:n käyttöön. ITSMF käyttäjäfoorumin kautta ITIL:iä kehitetään kollektiivisesti eteenpäin. Varsinkin pienet ja keskisuuret yritykset joutuvat monesti soveltamaan ITIL:n käytäntöjä, koska se on pääosin laadittu suurten yritysten näkökulmasta. (Hautamäki 2009).

Koska ITIL on melko universaalisti tavalla tai toisella yritysten käytössä, onnistuu järjestelmien sulauttaminen ja yhteistyökin helpommin. Tietysti tällaisissa tilanteissa on monia muita ongelmakohtia jotka tulee ratkaista, mutta itse palvelunhallinnan näkökulmasta yrityksiltä löytyy monesti samankaltaiset prosessit juuri tämän yhteisen "standardin" seurauksena.

ITIL koostuu siis parhaista IT-palvelunhallinnan käytänteistä joita on usean vuosikymmenen ajalta kerätty yhdeksi kokonaisuudeksi ja muokattu universaaliksi "standardiksi" yritysten ja muiden tahojen käyttöön.

ITIL V3 koostuu seuraavasta viidestä osasta.

- Palvelustrategia (Service strategy)
    - Strategian hallinta IT-palveluille
    - Palveluportfolion(-salkun) hallinta
    - IT-palveluiden taloudellinen hallinta
    - Kysynnänhallinta
    - Liikesuhteiden hallinta

(The Art of Service 2009, 25-43).

- Palvelun suunnittelu (Service Design)
    - Suunnittelun koordinointi
    - Palveluluettelon hallinta
    - Palvelutason hallinta
    - Käytettävyyden hallinta
    - Kapasiteetin hallinta
    - IT-palveluiden jatkuvuuden hallinta (ITSCM)
    - Tietoturvanhallintajärjestelmä
    - Toimittajan/yhteistyötahon hallinta

(The Art of Service 2009, 47-81).

- Palvelutransitio (Service Transition)
    - Transition suunnittelu ja tuki
    - Muutoshallinta
    - Palveluomaisuuden- ja konfiguraationhallinta
    - Jakelun/julkaisun ja käyttöönotonhallinta
    - Palvelun validointi ja testaus
    - Muutosten arviointi
    - Tietämyksenhallinta

(The Art of Service 2009, 85-110).

- Palvelutuotanto (Service Operation)
    - Tapahtumien hallinta
    - Poikkeamien hallinta
    - Pyyntöjen toimittaminen (Request fulfillment)
    - Ongelmien hallinta

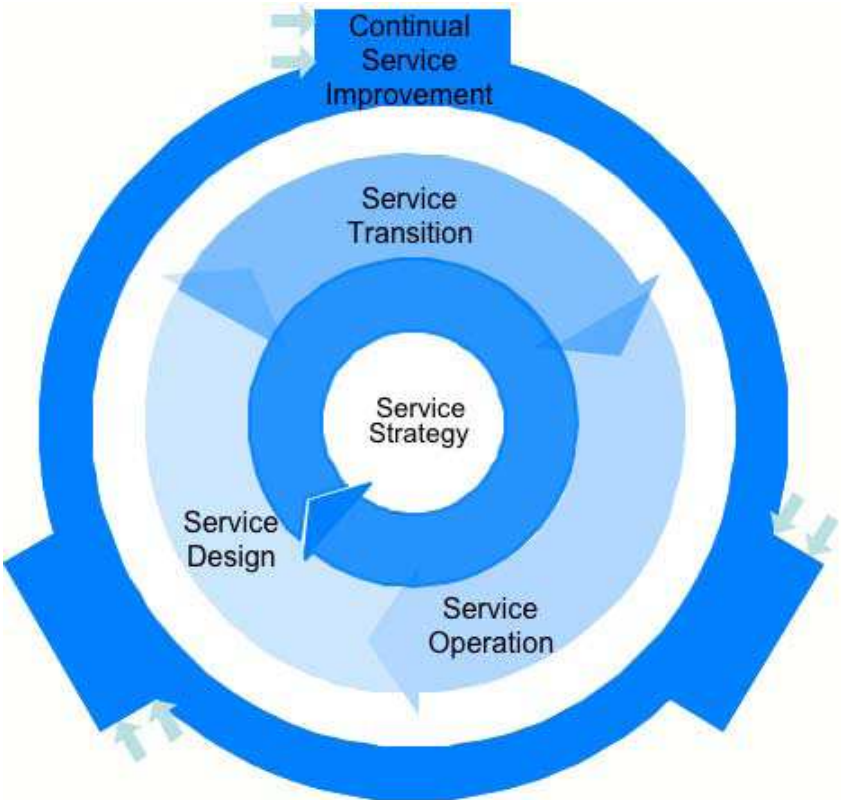
- Pääsyn hallinta

(The Art of Service 2009, 114-143).

- Jatkuva palvelun parantaminen (Continual Service Improvement)
  - Seitsemän portainen kehitys/parannus prosessi
  1. Tunnistaa strategia kehittämiselle
  2. Mitattavien kohteiden määrittely
  3. Datan keräys
  4. Datan käsittely
  5. Datan ja informaation analysointi
  6. Informaation esittäminen ja hyödyntäminen
  7. Parannuksen implementointi

(The Art of Service 2009, 147-157).

KUVIO 11. ITIL v3 elinsykli.



(The Art of Service 2009, 20).

ITIL v3 on ITIL:n seuraava kehitysaskel ITIL v2:sta. Aikaisemmin versio 2 otti pääasiallisesti kantaa vain palveluiden toimittamiseen ja niiden tukeen, mutta uudemmassa ITIL v3:ssa otetaan kantaa laajamittaisemmin itse palveluiden elinkaareen. ITIL v3:ssa ei pelkästään oteta kantaa oman yrityksen toimintamalleihin ja käytäntöihin vaan myöskin yhteistyökumppaneiden ja tahojen suhteen sekä kuinka yhteistyö tulisi hoitaa. Samoin kantaa otetaan myös taloudellisiin näkökulmiin. Luonnollisesti suurella osalla yrityksistä on tänä päivänä ITIL tai sen kaltainen menetelmä käytössä palvelunhallintaa ajatellen, joten yhtymäkohtia löytyy paljon. Tästä syystä ITIL onkin myös niin joustava. Koska kyseessä ei ole tiukka standardi, voidaan omaksua ITIL:n parhaita puolia tarpeen mukaan mikäli ei olla muokkaamassa kaikkia palveluita sen kaltaiseksi. (The Art of Service 2009, 9-11).

Uudempi versio ITIL:stä ottaa laajemmin kantaa kokonaisuuden hallintaan, eikä keskity niin suppeasti palvelun jakeluun ja tukeen. Sama periaate kuitenkin palvelunhallinnan kehittämisessä pätee, oli ITIL:n versio mikä hyvänsä: valitaan yrityksen jo olemassa olevasta toimintamallista paras prosessi, josta lähdetään rakentamaan uutta. Kun pohjalla on toimiva osa, voidaan sen ympärille lähteä laajentamaan ITIL:n viitoittamaa kokonaisuutta. Siirtyminen uuteen standardiin ei yleensä ole nopea tai kivuton prosessi. Organisaation luonne ja koko vaikuttavat merkittävästi se nopeuteen uuden standardin käyttöönotossa. Valtaosa prosesseista täytyy räätälöidä yrityksen tarpeisiin sopivaksi. Pelkästään jo verkon ja palveluiden monitoroimiseksi, ylläpitämiseksi ja toteuttamiseksi on olemassa useita valmiita ratkaisuja. Nämäkin yleensä harvoin toimivat suoraan sellaisenaan. Yrityksen pitäisikin pyrkiä muokkaamaan ne omiin tarpeisiinsa sopiviksi, eikä lähteä rakentamaan omaa toimintaansa jonkin helposti käyttöönotettavan järjestelmän ympärille. (Hautamäki 2009).

Käytettävien työkalujen merkitys on erittäin olennainen. Tämä koskee jokaisen eri prosessin/tahon tarvitsemia järjestelmiä ja työkaluja. Kuten aikaisemminkin mainittiin, jos yrityksellä on jo ennestään hyvä järjestelmä käytössä, kannattaa tämä ottaa kiintopisteeksi koko kehittämiselle ja lähteä siitä. Itse prosessit eivät monestikaan rajoitu pelkästään omaan lähimpään organisaatioon. Tästä lähtökohdasta pitäisi lähteä myös niitä suunniteltaessa.

Palvelustrategia muodostaa ensimmäisen osan uudesta ITIL:stä. Sen tarkoituksena on määritellä palvelunhallinta, suunnittelu/kehittäminen ja käyttöönotto strategisena vah-

vuutena yrityksen kasvun kannalta. Samoin palvelustrategian suunnittelu tähtää myös kulujen ja riskien hallintaan mahdollisimman tehokkaalla tavalla. Selkeät strategiset päämäärät tulisi asettaa palveluille ja prosesseille. (The Art of Service 2009, 25).

"KEY ROLE: To stop and think about WHY something has to be done, before thinking HOW." (The Art of Service 2009, 25).

Palvelun suunnittelu muodostaa toisen ITIL:n pääkohdan. Päätavoitteet palvelunsuunnittelulle ovat aikaisemmin asetettujen strategioiden kehittäminen ja jalostaminen toimiviksi palveluiksi ja toimintamalleiksi. Tähän tulisi pyrkiä soveltamaan käytännönläheisiä ja kokonaisvaltaisia lähestymistapoja, jotta päästään mahdollisimman korkealaatuiseen lopputulokseen ja laatuun palveluiden osalta. Palvelun suunnittelussa tulisi myös asettaa standardi tulevaisuuden suunnittelulle, jotta taataan sama laatu kaikissa tulevaisuuden prosesseissa ja palveluissakin. (The Art of Service 2009, 47-48).

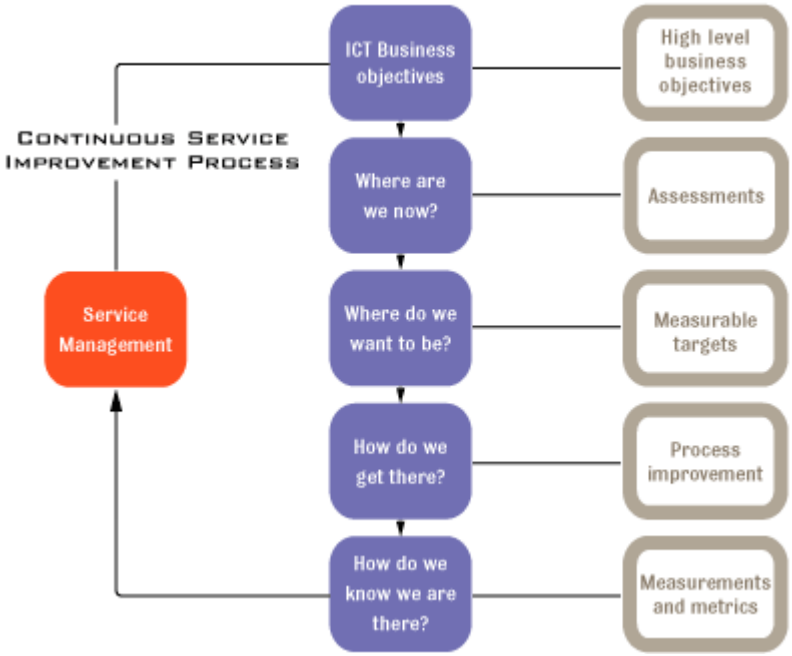
Palvelutransitio muodostaa kolmannen kokonaisuuden ITIL:ssä. Päätavoite on uusien ja paranneltujen palveluiden käyttöönotton helppous. Kaikki pyritään hiomaan jatkuvasti paremmaksi ja toimivammaksi uuden palveluiden käyttöönoton kannalta. Tämä johtaa automaattisesti siihen, että kaikkien uusien palveluiden täytyy täyttää asiakkaan vaatimukset ja näillä muutoksilla ei saa olla negatiivista vaikutusta IT-kokonaisuuden toimintaan tai liiketoimintapuoleen. Kun palvelutransitio on kokonaisuutena hyvin totetutettu saadaan realistinen arvio arvioiduista kustannuksista sekä todellisista kustannuksista. Sama pätee aikatauluihin, riskeihin ja muutoksen kohderyhmään. Näiden todelliset kustannukset voidaan realistisemmin verrata teoreettisiin tuloksiin ja näin saadaan paljon tarkempi arvio tarvittavista ja käytettävistä resursseista. Kaikki tämä tähtää siis mahdollisimman tehokkaaseen palveluiden rakentamiseen, konfiguroimiseen, testaamiseen ja käyttöönottoon ja samalla näiden muutosten vaikutusten minimointiin yrityksen toiminnalle ja asiakkaille. (The Art of Service 2009, 85).

Palvelutuotanto on neljäs pääteema ITIL:ssä. Sen avain käsite on palveluiden tehokkuus sekä tehokas tuotanto, toimitus ja tuki kyseisille palveluille. Aikaisemmin säädetyt strategiset tavoitteet konkretisoituvat palveluntuotannon kautta. Oleellisia pääkohtia ovat myös kuinka taataan sulavat muutokset palveluiden toimintamalleihin, laajuuteen ja palvelutasoihin. Kaikki tämä täytyy onnistua mahdollisimman kivuttomasti muun toiminnan kannalta. Tätä varten prosessit ja työkalut tulisi jaotella reaktiivisiin

ja proaktiivisiin. Näin voidaan paremmin hallita palveluita, kehittää niitä, ja ehkäistä sekä korjata ongelmia. (The Art of Service 2009, 114).

Viides pääteema on jatkuva palveluiden parantaminen ja kehittäminen. Mikään palvelu ei ole valmis uunituoreena vaan palvelu jalostuu ja kehittyy elinkaarensa aikana. Tähän tähtää myös ITIL:n CSI (Continual Service Improvement) kokonaisuus. Palveluita tulisi toistuvasti tarkkailla ja toimintaa pyrkiä kehittämään. Tämä toimintamalli toistuu läpi koko palvelun elinkaareen. Se on prosessi jota ei koskaan voida periaatteessa saada valmiiksi vaan se on jatkuvaa muutosta ja oppimista.
(The Art of Service 2009, 148).

KUVIO 12. Continual Service Improvement model.



(NextireOne 2011).

4.2.2 ISO/IEC 20000 ja BS 15000 standardi

BS 15000 pohjautuu paljon ITIL:iin, mutta pitää sisällään muita lähestymistapoja palvelunhallintaan eikä vain orjallisesti noudata samaa kaavaa kuin ITIL (lähinnä ITIL v2). Moduulijaottelussa on eriäväisyyksiä, sekä osa ITIL:in puutteista on "korjattu". Tämä pätee enemmän tietoturvan hallinnan ja liiketoimintaprosessin hallinnan suh-

teen. Tosin uudempi ITIL:n versio ottaa jo paljon laajemmin kantaa näihin puutteisiin ja ainoastaan ITIL v2 kärsii näistä vajaavaisuuksista. BS 15000 innoittamana ja sitä sekä ITIL:iä hyväksi käyttäen laadittiin uudempi ISO/IEC 20000 standardi joka ottaa kantaa nimenomaan IT-palveluiden hallintaan paremmin kuin vanhempi BS 15000 standardi. (Hautamäki 2009).

ISO/IEC 20000 pohjaa erittäin paljon vanhempaan BS 15000 standardiin. Kyseinen standardi jaetaan kahteen osaan. Osa 1 (pakolliset vaatimukset - Specification) käsittelee prosessien integrointia ja lähestymistapaa/toimittamista tavalla, joka täyttää yrityksen sekä asiakkaan vaatimukset. Tarkemmin kyseinen kokonaisuus koostuu seuraavista käsitteistä:

1. Laajuus (Scope)
2. Termit ja määritelmät (Terms and Definitions)
3. IT-palveluiden hallinan suunnittelu ja käyttöönotto (Planning and Impelenting Service Management)
4. Vaatimukset johtamisjärjestelmälle (Requirements for Management System)
5. Muutosten sekä uusien palveluiden suunnittelu ja käyttöönotto (Planning & Implementing new or changed services)
6. Palveluiden toimittamisen prosessi (Service Delivery Process)
7. Asiakas-ja toimittajasuhteiden hallinta (Relationship Processes)
8. Kontrolliprosessit (Control Processes)
9. Ylläpitoprosessit (Resolution Processes)
10. Versionhallintaprosessit (Release Management Processes)
(ITSMF.fi 2011).

ISO/IEC 20000 toinen osakokonaisuus (osa 2., code of practice - Ohjeet toiminnalle) koostuu yhdeksästä osasta.

1. Laajuus (Scope)
2. Termit ja määritelmät (Terms and Definitions)
3. IT-palveluiden hallinnan suunnittelu ja käyttöönotto (Planning and Impelenting Service Management)
4. Muutosten sekä uusien palveluiden suunnittelu ja käyttöönotto (Planning & Implementing new or changed services)

5. Palveluiden toimittamisen prosessi (Service Delivery Process)
6. Asiakas-ja toimittajasuhteiden hallinta (Relationship Processes)
7. Kontrolliprosessit (Control Processes)
8. Ylläpitoprosessit (Resolution Processes)
9. Versionhallintaprosessit (Release Management Processes)
(ITSMF.fi 2011).

Vanhemman BS 15000 standardin jaottelussa on osittain samankaltaisuuksia ja sitä on myös hyvä tarkastella, jotta ymmärretään ISO/IEC 20000 taustalla oleva historia. Pääpiirteittäin BS 15000:n moduulijaottelu näyttää seuraavalta:

- Palvelun tuotantotoiminnot
    - Kapasiteetinhallinta
    - Jatkuvuuden ja käytettävyyden hallinta
    - Palvelutasonhallinta
    - Palvelun raportointi
    - Tietoturvan hallinta
    - Liiketalouden hallinta
- Hallintatoiminnot
    - Konfiguraatioiden hallinta
    - Muutosten hallinta
- Käytöönottotoiminnot
    -Käyttöönoton hallinta
- Käsittelytoiminnot
    - Poikkeamien hallinta
    - Ongelmien hallinta
- Suhdetoiminnot
    - Liiketoimintasuhteiden hallinta
    - Tukiorganisaatioiden hallinta

(Hautamäki 2009).

Kuten jaottelusta nähdään molemmat standardit kattavat varsin laajan skaalan palvelunhallinnasta ja ei rajoitu pelkästään IT-toiminteisiin vaan myös yrityksen liiketoimintasuhteiden hallintaan. (Hautamäki 2009).

Palvelun tuotantotoiminnoilla käsitetään, kuten jo edellä mainittu, useampia eri kohtia palveluiden hallinnasta, suunnittelusta, ylläpidosta ja tietoturvasta lähtien. Ensimmäiseksi tulee sopia palveluntasonhallinnasta. Asetettuihin tavoitteisiin pääsemiseksi laaditaan SLA:t (service level agreement) yhteiskumppaneiden kanssa sekä tarvittaessa jokaiselle yrityksen sisäiselle palvelulle myös. Näissä määritellään kaikki yrityksen erinäiset palvelut, joiden toimivuus halutaan varmistaa pysyvän tavoitetasolla. Kyseessä on virallinen dokumentti, joten palvelutasoja asetettaessa kannattaa olla mahdollisimman yksityiskohtainen halutusta palvelusta. Sopimukset laaditaan yrityksen ja asiakkaan kesken. SLA:n käyttö ei ole mikään BS15000 keksimä menettely vaan se on ollut käytössä jo pitkään varsinkin operaattoreilla. Sopimuksia ja niiden täyttymistä sekä niiden palvelemaa tarkoitusta tulee seurata jatkuvasti. Mikäli uudelleen tarkastelun yhteydessä havaitaan puutteita sopimuksissa tai tarvetta muutokselle voidaan niitä lähteä muokkaamaan sopijaosapuolten kesken. (Hautamäki 2009).

Kun SLA:n ehdot on määritelty täytyy pystyä luomaan järjestelmä joka ylläpitää realistista kuvaa toiminnasta ja ehtojen täyttymisestä. Tähän tarvitaan toimiva raportointi kyseisestä palvelusta, jotta sen toimintaa voidaan seurata ja dokumentoida tulevaa varten.

Myös palveluiden käytettävyys täytyy saada pysymään tavoitetasolla kustannustehokkaasti kuin myös niiden jatkuvuus. Tätä varten palveluiden toimintaa korjataan ja optimoidaan jatkuvasti ja varsinkin kun ongelmia tai poikkeamia niiden toiminnassa ilmenee. Yrityksellä tulee myös olla laadittuna jatkuvuuden hallintasuunnitelma sekä riskianalyysit siitä kuinka tavoitteisiin päästään kaikissa olosuhteissa.
(Hautamäki 2009).

Liiketalouden hallinta on osio jossa otetaan palvelunhallintaan enemmän kantaa kuin esim. ITIL v2:n kanssa. BS 15000 standardissa liiketalouden hallinnan keskeiseksi tehtäväksi määritellään liiketaloudelliset resurssit palvelun laadulle ja jatkuvuudelle, sekä sen kehittämiselle. IT:n kustannukset pilkotaan osakokonaisuuksiin ja niille kaikille osioille määritellään toimintaohjeet. Tällaisia ovat esimerkiksi liiketalouden valvonta, kustannusten jakaminen eri palveluiden kesken, kirjanpito, ostopalvelut, henkilöstökulut, vakuutuskulut ja ohjelmistolisenssit. Koska tilanne on jatkuvasti elävä, tulee tätäkin osa-aluetta monitoroida ja reagoida muutoksiin niiden edellyttämällä vakavuudella. (Hautamäki 2009).

Kapasiteetinhallinnan tehtävä on kuten monessa muussakin standardissa, varmistaa riittävä kapasiteetti kaikelle toiminnalle niin normaalitilanteissa kuin poikkeustoimintamalleissakin. Tarkkaillaan aktiivisesti tämän hetken tilaa ja varaudutaan tulevaisuuden tarpeisiin hyvissä ajoin etukäteen, jotta kapasiteetti ei muodostu ongelmaksi missään vaiheessa. Parhaat tulokset saavutetaan kun kapasiteetin käyttöastetta monitoroidaan aktiivisesti. (Hautamäki 2009).

Tietoturvan hallinta pyrkii takaamaan turvallisen ympäristön yrityksen palveluiden toiminnalle kuin myös käyttäjille. Yritys laatii tietoturvapolitiikan joka pohjautuu vahvasti myös riskianalyysiin. Hyvä kokonaisuus saadaan aikaiseksi kun määritellään aktiiviset valvontakohteet. Samoin tulee määritellä tietoturvavaatimukset yhteistyökumppaneiden kanssa. Aktiivista valvontaa suoritetaan jatkuvasti ja poikkeamista raportoidaan eteenpäin, jotta tarvittaviin hälytyksiin voidaan reagoida nopeasti. (Hautamäki 2009).

Palvelun suhdetoiminnoilla kuvataan suhdetta asiakkaisiin sekä tuki organisaatioihin tai palveluntarjoajiin. Palveluntarjoajilla ei tässä tapauksessa välttämättä viitata ulkopuoliseen operaattoriin vaan myös sisäiseen tahoon joka tarjoaa palveluita muun yrityksen käyttöön. Suhdetoiminnoissa kuvataan myös koko tuotantoketju, alihankkijat ja yhteistyökumppanit mukaan lukien myös loppuasiakas. Suhdetoiminnoissa on tärkeä määritellä asiat mahdollisimman eksaktisti jotta kaikki osapuolet ymmärtävät asetetut liiketoiminnan vaatimukset, mahdollisuudet, rajoitukset, vastuut ja velvollisuudet. Koska kyseessä on kuitenkin suhdetoiminta tulee aina pitää asiakastyytyväisyys korkealla tasolla. (Hautamäki 2009).

Liiketoimintasuhteiden hallinnalla pyritään pitämään hyvät suhteet asiakkaisiin ja yhteistyökumppaneihin. Kokonaiskuvassa pitää myös huomioida tilanne asiakkaiden liiketoiminnan näkökulmasta, eikä ainoastaan omasta perspektiivistään. Liiketoimintasuhteiden avulla tulee myös tunnistaa ja dokumentoida sidosryhmät ja asiakkaat. Tarpeen mukaan tulee palvelut myös arvioida uudelleen ja tehdä niiden vaatimat muutokset. Tämä tehdään totta kai yhteistyössä sidosryhmien ja asiakkaiden kanssa. Myös asiakkaiden ja sidosryhmien mahdollinen tyytymättömyys ja valitukset tulee huomioida. Nämä käsitellään samoin tavoin kuin muutkin poikkeamat. Valitukset kirjataan ylös, raportoidaan eteenpäin, käsitellään tapauskohtaisesta, etsitään ratkaisu ja kuitataan pois. Jotta saadaan realistinen kuva palveluiden laadusta ja asiakastyytyväisyy-

destä, tulisi säännöllisin väliajoin tehdä myös tyytyväisyys kyselyjä. Kaikki palaute tulee myös käsitellä ja kehittää toimintaa sen perusteella. (Hautamäki 2009).

Tukiorganisaatioiden hallinta BS 15000 standardissa tarkoittaa suhteiden ylläpitoa alihankkijoiden ja yhteistyökumppanien suuntaan sekä varmistaa sovittujen SLA-sopimusten ehtojen täyttyminen. Tukiorganisaatioille ja yhteistyökumppaneille tulee myös määritellä hallintaprosessit, sekä nimetä henkilöt jotka vastaavat sopimusten toteutumisesta. Sopimuksissa tulee määritellä vaatimukset, tavoitteet, palvelutasot ja kommunikointiprosessit johon kaikki osapuolet sitoutuvat. Nämä sopimukset tulee suunnitella SLA:n pohjalta, jotta niissä säädetyt palveluntasot ja vaatimukset toteutuvat ja täyttävät samat kriteerit. Eri prosessien väliset rajapinnat tulee myös olla dokumentoituna sekä sovittuna. Tukiorganisaatioiden hallinnalla ei tarkoiteta pelkästään yrityksen ja ulkoisen yhteistyökumppanin välistä toimintaa vaan myös yrityksen sisäisiä eri tahoja. Yhteistyörajapinnan ulkopuolella myös yrityksen ylempien tahojen tulee voida testata sovittuja tuotantoprosesseja ennen niiden käyttöönottoa. Samoin prosesseja tulee voida tarpeen ilmetessä muuttaa, jotta ne palvelevat kaikkia osapuolia parhaalla mahdollisella tavalla. Kuten muissakin osioissa, toimintaa tulee monitoroida ja kehittää jatkuvasti. (Hautamäki 2009).

Käsittelytoiminnot koostuvat standardissa ongelmien ja poikkeamien hallinnasta. Vaikka itse käsitteet ovat lähellä toisiaan, kyseessä on kuitenkin kaksi erilaista prosessia. Poikkeamien hallinnalla viitataan palvelutason pitämiseen oikealla tasolla, tai sen palauttamiseen oikealle tasolla, yllättävien tilanteiden ilmetessä. Ongelmien hallinnalla puhutaan enemmän proaktiivisesta ongelman havaitsemisesta. Ongelma paikallistetaan ja poistetaan. Poikkeamienhallinta voitaisiin summata seuraavasti: sen tehtävänä on reagoida vikailmoitukseen ja palauttaa sovittu palvelutaso mahdollisimman nopeasti. Kaikki poikkeamat kirjataan ylös tietokantaan, raportoidaan, dokumentoidaan sekä priorisoidaan. Jatkossa saman poikkeaman ilmenemistiheyttä voidaan seurata ja näihin tilanteisiin löytyy olemassa oleva korjausmenetelmä/ratkaisumalli. Ongelmien hallinnassa vastaavasti pyritään kokonaisvaltaisempaan ongelmien eliminointiin. Siinä analysoidaan koottujen poikkeamien juurisyitä ja kehitetään menetelmät niiden ratkaisemiseksi. Joskus ratkaisu voi olla yleinen toimintamalli tai ohje kuinka tietty poikkeama korjataan, joskus ratkaisu voi olla poikkeaman aiheuttajan juurisyyn eliminoiminen. Joka tapauksessa tärkein tavoite on minimoida poikkeamista aiheutuneet haitat

niin asiakkaalle kuin itse palvelullekin. Kun saadaan tarpeeksi suuri tietokanta koottua ilmenneistä ongelmista on juurisyyn paikallistaminen ja korjaaminen helpompi tehtävä. (Hautamäki 2009).

Palvelun hallintatoiminnot koostuvat konfiguraation hallinnasta sekä muutosten hallinnasta. Nämä kaksi seikkaa kulkevat pitkälle käsikädessä ja tukevat toistensa toimintaa. Ne vastaavat osaltaan yrityksen palveluiden, laitteiston ja ohjelmistojen konfiguraatioista sekä niiden testauksesta. Samoin näiden hallinta ja käyttöönotto sekä muutospyynnöt käsitellään hallitulla tavalla. (Hautamäki 2009).

Konfiguraatioiden hallinnalla pidetään yllä ajantasaista tietokantaa olemassa olevista verkonlaitteista ja komponenteista, sekä käytetyistä ohjelmistoista ja tuotetuista palveluista. Kaikki konfiguraatiot kerätään kollektiivisesti yhteiseen konfiguraatiotietokantaan. Myös kaikkien näiden eri konfiguraatioiden suhteet toisiinsa tulee määritellä, jotta voidaan taata toimiva ympäristö ja se hallinta helpottaa myös samalla. Versionhallintaa ei myöskään sovi sivuuttaa, vaan sille tulee olla omat toiminnot. Kaikista konfiguraatioista sekä muusta dokumentaatiosta tulee löytyä varmuuskopiot. Näin kaikki konfiguraatioihin tehtävät muutokset tulee myös dokumentoitua ja niiden vaikutuksia voidaan seurata paremmin kun aikaisemmat konfiguraatiot ovat myös tallessa. Jokaiselle eri konfiguraatiolle (laitekohtaisesti) tulee löytyä versiohistoria konfiguraatioineen sekä dokumentaatio versiomuutoksista ja mahdollisista ongelmista. Yhtenäisyys ja eheys ovat avaintermejä. (Hautamäki 2009).

Muutosten hallinnan tehtävänä on taata organisoitu tapa muutosten tekemiselle palveluihin. Tehtävien muutosten vaikutukset tulee arvioida, jonka jälkeen ne hyväksytään ja otetaan käyttöön. Saapuvat muutospyynnöt tarkastellaan ja luokitellaan eri kiireellisyysluokkiin. Näin kriittisemmät muutokset saadaan suoritettua nopeammin. Joka muutoksen yhteydessä arvioidaan sen riskit itse palvelulle ja asiakkaille. Myös muutoksen kumoaminen tulee olla mahdollista mikäli siitä aiheutuu odottamattomia ongelmia. Tätä varten tulee myös laatia oma suunnitelma. Muutoksien vaikutuksia tulee analysoida jotta voidaan päätellä muutoksen tehokkuusaste. Tätä tietoa voidaan myös käyttää jatkossa hyväksi palvelua kehitettäessä. (Hautamäki 2009).

Käyttöönottotoiminnot BS 15000 standardissa hallitsee ja ohjaa käyttöönoton suunnittelua ja jakelua palvelussa. Pohjana tälle käytetään suoritettavan toiminteen vaikutusta asiakkaisiin sekä palveluntarjoajan toimintaan sekä IT-palveluihin. (Hautamäki 2009).

Käyttöönoton hallinnalla pyritään BS 15000 standardissa kokoamaan muutokset yhdeksi kokonaisvaltaiseksi release -paketiksi. Nämä valmiit paketit koostuvat yleensä konfiguraatioista tai ohjelmistoversioista jotka on testattu ja valmiita käyttöönotettavaksi. Käyttöönoton hallinta määrittelee ja dokumentoi jakeluversiot sekä arvioi niiden negatiiviset vaikutukset asiakkaille ja itse palvelulle. Tällä pyritään minimoimaan muutoksesta aiheutunut haitta. Suunnitelmien tulee olla myös kokonaisvaltaisia, joten niissä määritellään kunkin eri tahon toiminta. Jokaiselle jakeluversiolle tulee myös olla palautussuunnitelma, jolla voidaan palauttaa järjestelmät aikaisempaan tilaan mikäli käyttöönotto epäonnistuu. Jokainen release -paketti testataan ennen käyttöönottoa testiympäristössä yhteistyössä konfiguraation- ja muutoshallinnan kanssa. (Hautamäki 2009).

Jatkuva kehittäminen on iso osa mitä tahansa standardia. Se on läsnä myös BS 15000 standardissa. Kun olemassa olevaa kokonaisuutta monitoroidaan tarpeeksi tarkasti voidaan sen perusteella kehittää toimintaa kokoajan eteenpäin. BS 15000 standardissa tätä menetelmää nimitetään PDCA -lyhenteellä (Plan-Do-Check-Act). Menetelmä on periaatteessa vuokaavio, minkä mukaan jatkuva kehittäminen suoritetaan ja toteutetaan. Ensimmäinen vaihe on aina suunnitella kuinka palvelunhallinta toteutetaan kyseisessä palvelussa. Toisessa vaiheessa otetaan suunnitelma käyttöön hallitusti. Kolmannessa vaiheessa monitoroidaan ja kerätään dataa palvelun toiminnasta. Neljännessä vaiheessa tehdään tarvittavia muutoksia järjestelmään. Tämän jälkeen prosessi alkaa uudelleen vaiheesta yksi. Näin saadaan jatkuva sykli kehittämiselle ja palvelut jalostuvat. (Hautamäki 2009).

4.3 Tietoturva

Tietoturva on nykyään kasvavassa määrin oleva trendi tietoverkkojen suunnittelussa. Kun Internetin kautta tehtävä liiketoiminta ja palveluiden tarjoaminen kasvaa, tarvi-

taan myös tietoturvaa turvaamaan palveluiden toimivuutta ja turvallista ympäristöä jossa voidaan toimia. Kehittymisen ja verkostoitumisen seurauksena on tullut väistämättä kuvaan mukaan erilaiset haittaohjelmat, virukset, troijalaiset sekä hakkerit. Myöskin yritysvakoilu on seikka jota ei sovi lukea pois. Tästä kaikesta seuraa kuitenkin kasvavissa määrin ajan tasalla olevan tietoturvan tärkeys.
(Stoneburner, Hayden, Feringa 2004, 3).

Perinteisesti tietoturva voitaisiin luokitella defensiiviseksi eli puolustavaksi. Tämä on kuitenkin jo vanhentunut ajatusmalli, sillä pelkästään puolustava tietoturva on suhteellisen passiivista. Sillä pyritään suojaamaan käyttäjät, palvelut ja laitteet. Voitaisiin verrata tätä suuren muurin rakentamiseen. Jotta saadaan aikaan oikeasti turvallinen järjestelmä on otettava aggressiivisempi ote tietoturvan suunnitteluun. Pelkkä muuri ei riitä, vaan tarvitaan tälle muurille myös sotilaita aktiivisesti valvomaan tilannetta. Offensiivisempaa näkökulmaa pyritään tuomaan yhä kasvavissa määrin esiin tietoturvaa suunniteltaessa. Sen sijaan, että keskityttäisiin rakentamaan pelkästään suljettu ympäristö otetaan voidaan pyrkiä kehittelemään menetelmiä millä voidaan yrittää rajata hyökkääjä tehokkaasti ulos ja estää proaktiivisesti hyökkäykset jatkossakin. Pyritään tunnistamaan hyökkääjä ja jäljittämään mistä hyökkäys tulee.
(Hautamäki 2009).

Suurimmat uhat tietoverkoille koostuvat useiden eri asioiden summasta. Perinteiset seikat kuten virukset ja haittaohjelmat ovat vain pieni osa kokonaisuutta. Toinen iso osa on itse käyttäjien huolehtiminen omalla kohdallaan yhteisistä tietoturvan pelisäännöistä. Ei esimerkiksi kirjoiteta salasanoja ylös ja hukata niitä, ei jätetä tärkeitä sovelluksia päälle mikäli niitä ei käytetä. Mahdollisten standardien (vrt. yhteiset pelisäännöt) puuttuminen tietoturvatoiminnassa. Internet on nykyään tietoa pullollaan ja tämäkin osaltaan vaikuttaa siihen, että tietoturvan tärkeys korostuu entisestään. Koska tietoa on yleisesti saatavilla on myös ihmisten tietotaso korkeammalla. Yrityksellä tärkeää on laatia selkeät verkonhallinnan ohjeet ja toipumissuunnitelma juuri tällaisten tilanteiden varalta. Suotavaa olisi välttää jo etukäteen tiedossa olevia turvattomia protokollia ja tulisi kehittää menetelmiä havaitsemaan verkon liikenteen analysointi heti, jotta ulkopuolinen ei voi analysoida verkon liikennettä. Mahdolliset hyökkäykset suoraan yritystä vastaan ovat myös suuri uhka, tämä sitä suuremmissa määrin mitä isommasta yrityksestä on kyse. Pois ei voida myöskään sulkea selkeitä fyysisiä uhkia. Lait-

teiston rikkoontuminen, kaapeli-, laite-, ohjelmisto- ja sähköviat tulee myös huomioida. Samoin mahdollinen ilkivalta tai tiloihin murtautuminen sekä varkaudet. Kuten tästä voidaan jo havaita, tietoturva kokonaisuutena on useiden muuttujien summa. (Hautamäki 2009).

Itse tietoturvaa kuvataan monesti ns. "sipulimallina", eli kasataan suojauksia kerroksittain toistensa päälle. Tämä pitää paikkansa kaikilla eri tietoturvan osa-alueille. Ei tule ainoastaan luottaa yhteen tasoon vaan kokonaisrakenteen tulee olla kerroksittain rakennettu. Jaetaan tietoturva seuraaviin osa-alueisiin ja tarkastellaan niitä tarkemmin. (Stoneburner, Hayden, Feringa 2004, 4).

4.3.1 Hallinnollinen ja organisatorinen tietoturvallisuus

Tällä kuvastetaan yrityksen johdon vastuuta sekä sen velvollisuutta laatia hyvä tietoturvapolitiikka jonka päälle voidaan toimintaan kehittää tietoturvan näkökulmasta. Myös tietoturvasuunnitelmien laatiminen kuuluu tähän vaiheeseen. Kun on laadittu yrityksen toimintaa vastaava tietoturvapolitiikka sekä tietoturvasuunnitelma voidaan lähteä analysoimaan mahdolliset riskit ja uhat. Laaditaan riski/uhka -analyysi ja muokataan suunnitelmia näissä havaittavien asioiden perusteella. Ne ongelmat mitä ei voida ennalta ehkäistä, suunnitellaan niin, että näiden tilanteiden vahinko rajoittuu mahdollisimman pieneksi ja laaditaan vaihtoehtoinen toimintasuunnitelma tällaisen tilanteen ilmetessä. (Hautamäki 2009).

Myös tarvittavan tietoturvaohjeistuksen laatiminen on olennainen osa tätä vaihetta tietoturvan suunnittelussa. Koko tämän vaiheen tarkoitus on laatia kokonaisvaltainen suunnitelma jonka pohjalta tietoturva voidaan toteuttaa. Välttämättä ei oteta vielä kantaa kaikkiin yksityiskohtiin vaan ne katsotaan myöhemmässä vaiheessa. Suotavaa olisi kuitenkin laatia niin yksityiskohtaiset suunnitelmat kuin mahdollista, jotta niiden perusteelta käyttöönotto on mahdollisimman vaivaton ja helppo prosessi.
(Hautamäki 2009).

4.3.2 Henkilöstöturvallisuus

Tällä kuvataan, yrityksen ja organisaation työntekijöiden velvollisuuksia. Jokaisen henkilökohtainen velvollisuus on huolehtia omalta kohdaltaan tietoturvasta. Salasanojen pitäminen tallessa, tietokoneen lukitseminen, vaitiolovelvollisuus, kaikki nämä ovat osa tietoturvaa ja näitä voitaisiin luonnehtia henkilöstöstä aiheutuviksi uhiksi. Myös tarkoitushakuinen pahanteko henkilöstöntoimesta tulee huomioida. Henkilöstöturvallisuus käsittää myös henkilöstöön kohdistuvat uhat. Jokaiselle tulee taata turvalliset palvelut ja turvallinen työympäristö sekä työkalut. Myöskin työntekijöiden taustojen tarkistus sekä tarkoin määritelty työnkuva on osa henkilöstöturvallisuutta. Näiden sopimusten avulla asetetaan selkeät rajat työntekijän toiminnalle.
(Hautamäki 2009).

4.3.3 Fyysinen tietoturvallisuus

Tällä käsitetään mm. rakennuksen ja toimitilojen turvallisuus. Onko itse rakenteet kunnossa? Kuinka ukonilman aiheuttamat vauriot estetään ja suojataan työympäristö? Entä vesivahingon sattuessa? Tulipalo on myöskin aina mahdollisuus kun käytössä on suuria määriä elektroniikka ja mahdollisesti palvelinfarmeja yms. Kuinka tilojen kulunvalvonta on toteutettu? Käytetäänkö kulkukortteja? Onko kiinteistössä valvontakamerat tai jopa vartijat. Nämä ovat seikkoja jotka kuuluvat fyysisen tietoturvallisuuden piiriin ja ne tulee myös suunnitella palvelemaan yrityksen toimintaa ja sen henkilöstöä ja palveluita mahdollisimman kustannustehokkaasti. Arvioidaan jokaisen riskin todennäköisyys, ja suunnataan tarvittava määrä varoja näiden riskien ehkäisemiseen/vahingon minimoimiseen. Myös työntekijöille tulee olla selkeät pelisäännöt salasanojen suhteen sekä tietokoneen lukitsemisen suhteen. (Hautamäki 2009).

4.3.4 Tietoliikenteen turvallisuus

Tietoliikenteen turvallisuudella käsitetään menetelmiä joilla kaikki salassa pidettävä tieto voidaan suojata ulkopuolisilta tahoilta. Käytännössä tämä tarkoittaa, että kaikkien verkkoa käyttävien laitteiden oikeudet on rajattu ehdottomaan minimi ehtoihin, jotta toiminnallisuus yhä säilyy. Tällä viitataan laitteiden reititykseen, access-listoihin, työasemien ja käyttäjien oikeuksiin. Mikäli jokin verkonlaite joutuisi ulkopuolisin tahon hallintaan hän ei pysty tekemään paljoa haittaa verkolla tai urkkimaan tietoja

laitteen avulla. Ainoastaan järjestelmää ylläpitävillä tahoilla on oikeudet tehdä sellaisia toimenpiteitä verkossa, joilla jotain voitaisiin saada selville ja myöskin nämä toiminteet olisi suotavaa olla jonkinlaisen vaihtuvan salausavaimen takana (esim. RSA). Verkon liikennettä voidaan kontrolloida VLAN konfiguraatioilla ja oikein segmentoimalla aliverkko sopiviin kokonaisuuksiin. Kaikki verkkoliikenne tulee myös salata. Tämä on erittäin tärkeää kun puhutaan varsinkin langattoman verkkoliikenteen salauksesta. Selkokielisenä menevä data on helppoa kaapata ja sisältö purkaa. Puhutaan esim. SSL-, SSH-, HTTPS-, AES-, IPsec-, TKIP-, WEP-, WPA-, WPA2-protokollista muun muassa. Tarvittaessa verkon sisäinen liikennekin voidaan toteuttaa VPN:n kautta jolloin liikenne pysyy varmasti suojattuna. (Kotikoski 2009).

4.3.5 Laitteistoturvallisuus

Kuinka laitteiden turvallisuus sitten taataan? Loogisin vastaus on tietysti käyttämällä hyväksi itse laitteiden tarjoamia turvaominaisuuksia. Käytetään salasanoja, kättelymenettelyjä, pääsylistoja, reititystä. Koska laitehallinta voidaan suorittaa etänä verkon yli sekä fyysisesti itse laitteelta, tulee myös molemmat seikat huomioida. Laitteiden hallinnasta vastaavalla taholla täytyy olla mahdollisuus ottaa yhteys laitteisiin fyysisesti esim. verkkokaapelilla tai konsolikaapelilla sekä myös verkon kautta. Fyysinen turvallisuus on myös osa laitteisto turvallisuutta. Kaikki eri tietoturvan kokonaisuudet tukevat toisiaan. Laitteet tulee sijoittaa tiloihin joissa niihin ei ole asiattomilla pääsyä. Tilat tulee olla suojattu tulipalojen, varkauden, vesivahingon ja luonnonmullistusten varalta. Myös yhteydet olisi suotavaa olla kahdennettu. Varsinkin palvelimet ja niiden yhteydet tulisi olla kahdennettu, koska sisältö on monesti kriittinen yrityksen toiminnalle ja samoin sen salassapito. Tämä tulee myös huomioida mikäli jokin uhkakuva toteutuu. Miten datan kahdennus toimii yleensä ja miten se toteutetaan poikkeaman sattuessa. Tässä vaiheessakaan laitteiden tai tiedon turvallisuus ei saa vaarantua.
(Leino 2009).

4.3.6 Ohjelmistoturvallisuus

Jotta käytössä olevien ohjelmistojen turvallisuus voitaisiin varmistaa tulee huolehtia, että itse ohjelmistot ovat aina ajan tasalla. Virheet ohjelman toiminnassa korjataan mahdollisimman tehokkaasti ja nopeasti ja päivitykset voidaan ottaa verkossa käyttöön joka laitteella nopeaan tahtiin. Yritysten toiminnassa on myös olennaisen tärkeää,

että käytössä olevien ohjelmistojen lisenssit ovat voimassa mikäli sovellukset ovat kaupallisia. Mikäli käytetyt sovellukset ovat avoimen lähdekoodin ohjelmia ei tästä tarvitse huolehtia. Samoin myös jos yritys itse tuottaa kyseistä ohjelmaa. Uusien ohjelmistojen käyttöönotto, päivitys, sulauttaminen, kaikkien näiden tapahtumien tulee kulkea aina testausvaiheen kautta. Asennusten toteuttaminen erinäisille verkonlaitteille voidaan toteuttaa yrityksen koosta riippuen usealla eri tavalla. Mikäli kyseessä on pienempi yritys missä ei ole keskitettyä hallintaa verkossa voidaan asennukset tarvittaessa tehdä manuaalisesti jokaiselle verkonlaitteelle. Suositeltavampaa on kuitenkin ajaa ohjelmistopäivitykset työasemille suoraan verkon kautta sekä automatisoida työasemien toiminta mahdollisimman pitkälle. (Rantonen 2009).

4.3.7 Käyttöturvallisuus

Tietoverkon käyttöturvallisuus periaatteessa käyttäjän oikeellisuuden varmistamista ja tämän mukaan heidän käyttöoikeuksiensa rajoittamista. Tästä syystä on tärkeää, että yrityksellä on jonkinlainen keskitetty käyttäjähallinta tietokanta. Tähän tarkoitukseen voidaan usein soveltaa esim. Windows pohjaisen järjestelmän Active directory -ominaisuutta. Näin voidaan jokaiselle käyttäjälle helposti määritellä oikeudet tarpeen mukaan. Sama periaate kuin muunkin tietoturvan suhteen toimii, eli sallitaan ainoastaan ne palvelut, joita tarvitaan normaalissa toiminnassa. Kaikki muu oletuksena estetään. Näin ei pääse syntymään tilanteita jossa oikeuksia poistetaan sen jälkeen kun vahinko on jo tapahtunut. Käyttäjä tunnistautuu kirjautuessaan järjestelmään ja syöttämällä oikean käyttäjätunnuksen ja salasanan. Tällöin itse tunnuksista ja varsinkin salasanan vaihtamisesta kannattaa pitää huoli. Salasana kannattaa säätää tietyin väliajoin vaihtuvaksi turvallisuus syistä. Salasanoille tulisi myös määritellä minimi vaatimukset, jotta ne eivät ole liian helposti arvattavissa. (Rantonen 2009).

4.3.8 Tietoaineistoturvallisuus

Tietosisällön autenttisuus tulee pystyä varmistamaan joka tilanteessa. Parhaiten tämä saavutetaan kun itse tietosisällöllä on luokitukset sen tärkeydestä. Samoin voidaan oikeudet kyseiseen aineistoon rajata käyttäjien luokituksen tai esimerkiksi käyttäjäryhmän mukaan. Vastaavat säännöt ja luokitukset olisi parasta laatia kaikkiin eri osaalueisiin. Tiedon säilytys, kuljetus, kopiointi, hävittäminen, jakelu, käyttö ja varmuuskopiointi niin digitaalisessa muodossa kuin kirjallisenakin tulee määritellä. Nämä

säännöt määräävät samalla kuin tarkasti kyseistä tietoa ja dokumentteja käsitellään (turvaluokituksen mukaan). Kun luokitukset ja niiden mukaiset säännöt on tiedoille laadittu tulee näiden noudattamista myös valvoa ja tarkastella säännöllisesti. Myös digitaalisen ja kirjallisen materiaalin suojaaminen tulee suunnitella, koska luonnollisesti, nämä kaksi eri menetelmää eroavat toisistaan suuresti.
(Hautamäki 2009).

4.3.9 Uhat

Kuten jo aikaisemmassa vaiheessa mainittiin tietoturva on useiden osien summa. Varsinaiset uhkakuvat muodostuvat useista eri skenaarioista. Valtaosassa on mukana inhimillinen elementti, ihminen. Ainoastaan tekniset-, ohjelmisto- ja laiteviat voidaan katsoa olevan vikoja joille ei mahdeta suoranaisesti mitään, koska ne liittyvät monesti itse laitteiden komponentteihin ja elinkaareen. Kaikkeen mihin voidaan vaikuttaa, näin tehdään ja ne seikat mihin ei voida, varaudutaan reagoimaan muilla toimenpiteillä (esim. laitevaihdot).

Inhimillisistä tekijöistä johtuvat uhat koostuvat pääosin työntekijöiden toimintaan liittyvistä seikoista, väärät toimintamallit, asioiden unohtaminen tai välinpitämättömyys voivat kaikki aiheuttaa tietoturvariskin. Salasanat ja lukitsemattomat tietokoneet ovat hyvä esimerkki inhimillisistä tietoturva aukoista. Osa näistä tietoturvan ongelmista on tahallisia, osa taas tahattomia. Tällaisia tilanteita voidaan ehkäistä helposti kouluttamalla työntekijöitä sekä rajoittamalla heidän käyttöoikeuksiaan erinäisiin järjestelmiin. Mikäli työntekijä haluaa tahallisesti tehdä vahinkoa, tämänkin voidaan minimoida oikeanlaisilla käyttöoikeuksilla. (Hautamäki 2009).

Yksi suuri tekijä on myös haittaohjelmat ja virukset. Tämä on kuitenkin hallittavissa oleva ongelma joka voidaan hoitaa ajan tasalla olevalla viruksentorjuntaohjelmistoilla. Suotavaa olisi rajoittaa jokaisessa eri verkon vaiheessa. Itse palomuurit sekä proxypalvelimet seulovat ja poistavat haittaliikennettä verkosta ja itse tietokoneetkin on sovelluspohjaisilla tietoturvaohjelmistoilla suojattu. Kaikki tulee myös olla aina ajan tasalla.

Laiteviat muodostavat suuren kokonaisuuden, mutta tähänkin on olemassa useampia varautumistapoja. Mikäli laitteita rikkoutuu, voidaan valmiiksi hankkia varalaite tilal-

le. Ohjelmistovirheet tulee korjata päivityksillä mahdollisimman nopeasti. Kaikki data tulee olla varmuuskopioituna sekä sähkönsyöttö turvata laitteille myös sähkökatkosten aikana.

Ei tule myöskään unohtaa tarkoitushakuista vahingontekoa vaikkakin se on hieman harvinaisempaa. Puhutaan tahallisesta hyökkäyksestä verkkoa vastaan. Tämä voi olla palvelunesto hyökkäys jolla pyritään estämään hyökkäyksen kohteena olevan tahon tarjoamien palveluiden toiminta. Hyökkäävä taho voi yrittää harhaanjohtamalla saada pääsyä verkkoon ja järjestelmiin. Tämä voidaan tehdä teknisesti erinäisillä hyökkäyksillä/haittaohjelmilla tai sitten sosiaalisen hyökkäyksen kautta. Social engineering -termillä kulkeva metodi on halpa ja helppo tapa saada tietoa käsiinsä petkuttamalla ja harhaanjohtamalla esim. yrityksen työntekijöitä. Myös yritysvakoilu on mahdollista, joten siitä syystä onkin erityisen tärkeää olla selkeät menettelytavat ja suojaukset tällaista vastaan.

5 TOTEUTUSEHDOTUS

Yrityksen lähtökohtainen tilanne huomioidessa havaitaan, että useita asioita voitaisiin toteuttaa toisin. Yrityksen pieni koko ja taloudelliset rajoitukset kuitenkin karsivat suoraan osan muutosehdotuksista pois. Käydään systemaattisesti läpi mitä yritys tarvitsee/haluaa, mitä suositellaan ja mikä on mahdollista toteuttaa kohtuullisin kustannuksin.

Konsultoidaan ehdotuksista yrityksen henkilöstöä ja päätetään sen mukaan millä tavalla edetään jokaisen kehitysehdotuksen pohjalta.

5.1 Verkkosuunnitelma

Kun huomioidaan yrityksen erittäin pienen verkon koko ei voida varsinaisesti kattavasta verkkosuunnitelmasta puhua. Itse verkon topologiset muutokset eivät ole varsinaisesti mahdollisia eivätkä tarpeen koosta johtuen tällä hetkellä.

5.1.1 Verkkolaitteet

Tällä hetkellä yrityksellä on käytössä kaksi työasemaa joilta kaikki tarvittava tietotekninen työskentely suoritetaan. Heillä on myös käytössään myös maksupääte korttimaksuja varten, samoin monitoimi kopiokone/tulostin sekä Telewellin valmistama modeemi/reititin.

Varsinaista lähiverkkokaapelointia ei ole myöskään vedetty kiinteistössä vaan kaikki laitteet sijaitsevat toimistohuoneessa. Kyseisessä kiinteistössä on useampia terapiahuoneita, mutta niissä ei ole erillisiä tietokoneita, josta voitaisiin suoraan asiakkaan käsittely hoitaa. Tämä suoritetaan toimistossa olevilta tietokoneilta. Terapiahuoneisiin olisi mahdollista vetää kaapelointi tarvittaessa. Tämä ei todennäköisesti tule ajankohtaiseksi ellei yritys päätä lisätä työasemiensa määrä sekä työntekijöiden määrä kasva.

5.1.2 LAN ja WLAN

Koska nykyaikana WLAN-yhteyksiä hyväksi käyttävät laitteet ovat voimakkaasti yleistyneet olisi myös mahdollista suunnitella jonkinlainen asiakkaiden käytössä oleva WLAN-verkko toimimaan varsinaisten yhteyksien rinnalla. Tämä edellyttäisi liikenteen luokittelua, jotta asiakasverkon liikenteelle voitaisiin varata osa yhteyden kokonaiskapasiteetista ja näin kuitenkin varmistaa yrityksen toiminnalle oleellisten palveluiden toiminnallisuus ja tarvittava kapasiteetin saaminen. Tämä edellyttäisi minimissäänkin modeemin vaihtamista toiseen. Kyseisellä laitteella ei ole ensinnäkään mahdollista toteuttaa WLAN-yhteyksiä eikä minkäänlaista liikenteen luokittelua.

Jotta tämä toteutus olisi mahdollinen on sen toteuttamiseen kaksi vaihtoehto riippuen halutaanko myös asiakkaille tarjota WLAN mahdollisuus. Mikäli ei, niin voidaan hankkia vanhan Telewell modeemin tilalle toinen josta löytyy antenni ja WLAN tuki kaikille uusimmille 802.11x standardeille. Näin voidaan toimitiloihin jakaa WLAN verkko joka suojataan vähintään WPA-PSK salauksella jotta sitä ei pysty luvattomasti käyttämään.

Itse modeemiksi voidaan harkita myös oikeaa reititintä. PPO (paikallinen operaattori) käyttää edelleen PPOE tekniikka adsl-yhteyksien muodostamisessa, joten laitteessa pitää olla tuki tälle. Tarvittaessa tähän käy esimerkiksi Ciscon reititin (827 tai uudem-

pi), tai esim. Intenon modeemi. Modeemeja/reitittimiä on sen verran paljon, että tarvittaessa valtaosalla voidaan kyseinen toteutus saada aikaiseksi ainakin WLAN yhteyden osalta. Mikäli modeemin konfiguroidaan CoS ja QoS sääntöjä liikenteen luokkitelua varten suosittelisin suosiolla Ciscon laitetta.

5.1.3 Access-tekniikka ja operaattori

Yrityksellä on tällä hetkellä internet-yhteys hankittuna paikallisen operaattorin kautta. PPO eli Pohjanmaan Puhelin tarjoaa heille ADSL yhteyden. Liittymä itsessään on vakiona 512kbit/s nopeudeltaan molempiin upstream ja downstream suuntaan. Myös sähköpostipalvelut ovat PPO:n kautta. Yrityksellä on kuitenkin oma domain käytössä, mutta liikennöintiin käytetään operaattorin hallitsemia palvelimia. Domain on kannuksenfysikaalinen.fi.

PPO:lta löytyy muitakin vaihtoehtoja liittymä tyypeiksi tässä tapauksessa, mutta toiselle operaattorille siirtyminen on hankalaa, koska kyseisellä alueella ei ole toimintaa tai kuparikaapeleita/kuitua muiden tahojen toimesta. Vaihtoehdoiksi jäisi tässä tapauksessa langattomat yhteydet. Ainoana vaihtoehtona tässä on siis mobiililaajakaista liittymät. Oman kokemukseni ja tietämykseni perusteella en kuitenkaan tätä vaihtoehtoa voi suositella sen arvaamattomuuden takia. Latenssit ovat liikenteellä välillä erittäin suuret sekä käytännön nopeus jää liikennemääristä riippuen ajoittain erittäin alhaiseksi.

Tällä hetkellä voimassa oleva sopimus on PPO:n Baana liittymä. Hinta on suhteessa korkeampi nykyisiin standardeihin, koska sopimus on vanha. Yrityksellä on myöskin käytössään ainoastaan kuluttajaliittymä. Tulevaisuudessa vanhasta Fysio32-ohjelmistosta joudutaan luopumaan ja sama yritys joka sen tuottamisesta vastaa hoitaa asiakastietojen ylläpidon internetin välityksellä. Uudempi versio ohjelmistosta on siis selainpohjainen. Tällöin internet -yhteyksien luotettavuus korostuu entisestään. Mikäli yhteydet eivät toimi, ei pystytä mitään tarvittavia kirjauksia, laskutusta tai terapian raportointia tehdä. Näin ollen olisi suotavaa harkita tilalle yritysliittymää johon saadaan jonkinlainen SLA sopimus sovittua tietyn palvelutason ja käytettävyyden aikaansaamiseksi, koska toiminta on kuitenkin internet -yhteyksistä täysin riippuvainen mikäli yritys siirtyy uuteen fysio -ohjelmistoon.

Tarvittaessa on myös hankkia kuituliittymä mikäli tulevaisuudessa tarvetta ilmenee, mutta toistaiseksi ADSL-liittymä riittää yrityksen tarpeisiin.

PPO:n kautta on tarvittaessa mahdollista siirtyä kaiken kattavaan palvelupakettiin joka voidaan räätälöidä asiakkaan tarpeiden mukaan. Palvelupakettiin voidaan hankkia leasatut tietokoneet ja ylläpito kaikille yrityksen ICT-palveluille sekä internet-yhteys ja tätä kautta sopia SLA –sopimus.

”PPo Pakki - tehokas ratkaisu yrityksen ict-tarpeisiin

PPO Pakki -palveluja voi hyödyntää tehokkaasti yrityksen viestintäyhteyksissä, toiminnanohjauksessa, tietoturvakysymyksissä sekä laitteistojen asennuksissa, ylläpidossa ja huollossa. Pakki paketoi kaiken tämän yhteen pakettiin. Se voi olla laaja ja vaativa tietotekniikkaratkaisu tai yhden tietokoneen ja yhteyden paketti.

Yritys voi valita erilaisista vaihtoehdoista sopivan ratkaisun tai rakentaa Pakki-ratkaisun tarpeiden mukaisesti. OmaPakki-ratkaisu voi sisältää tämänhetkiset yrityksen tietokoneet ja ohjelmat sekä lisäksi uusia laitteita ja palveluja yrityksen tarpeiden mukaisesti.

Ylläpito- ja huoltopalvelut

Huoltopalvelut takaavat ict-järjestelmän sujuvan toiminnan ja nopean avun mahdollisissa ongelmatilanteissa. Ict-asiantuntijamme ovat yrityksen käytettävissä palvelutasosopimuksen mukaisesti. Ict-huoltopalvelu hyödyntää verkkoyhteyksiä ja etähallintaohjelmistoja.

Tarvittaessa asiantuntija tulee paikan päälle hoitamaan ennakoivat huollot, ohjelmistopäivitykset, laiteasennukset ja korjaukset.” (PPO 2011).

Tarvittaessa tähän ratkaisuun on siis mahdollista siirtyä. Sopimuksen ja siihen sisältyvien toiminteiden hinta on tällä hetkellä vielä auki. Yrityksen verkko ja ylläpito ei vaadi suurta työtä, mutta henkilökunnalla ei ole välttämättä osaamista hoitaa yksinkertaisiakaan tehtäviä verkon ylläpitoon liittyen. Tästä syystä mahdollisimman kattava palvelupaketti olisi hyvä ratkaisu. Ongelmana tähän on seikka, että varsinainen fysio-

ohjelma on toisen alihankkijan hallinnassa ja sitä ei pystyttäisi integroimaan PPO:n pakettiin. Samoin yrityksen olemassa olevat tietokoneet kattavat jo tämän hetkiset tarpeet joten uusia koneita ei ole tarpeen leasata ja vanhojen koneiden hylkääminen ei tule kysymykseen tässä vaiheessa.

5.1.4 Kapasiteetti

Yrityksen toiminnan ja lähiverkon toiminnan kannalta kapasiteetti ei astu kovinkaan suureen rooliin. Ottaen huomioon työasemien määrän ja verkkolaitteiden määrän, ei tarvitse lähteä suorittamaan erityisiä toimenpiteitä kapasiteetin säätelyksi. Lähiverkon kaapelointiin soveltuu normaalit Cat5e tai Cat6 kaapelit. Valtaosa liikenteestä on internetin suuntaan menevää, joten access-tekniikalla on aavistuksen suurempi merkitys. Nykyinen nopeus joka on 512k/512k riittää kyllä teoriassa, mutta vanhaa sopimusta olisi tarpeen tarkastella joka tapauksessa, joten samalla nopeuden nostoa tulee harkita mikäli siitä ei aiheudu yritykselle suuria kuluja.

Myös sähköposti palvelut muodostavat osansa kokonaisliikenne määrästä, mutta tämäkin käyttö on sen verran vähäistä, että sitä ei erityisesti tule huomioida kapasiteetin suunnittelussa.

Poikkeuksena kapasiteetin suunniteluun tulee WLAN-verkko mikäli yritys haluaa tarjota asiakkaille mahdollisuuden WLAN-yhteyksiin toimitiloistaan. Tällöin kapasiteetia tulee hallita säätämällä liikenneluokkia ja varata prosentuaaliset osat kapasiteetista ensisijaisen liikenteen käyttöön. Mikäli tähän vaihtoehtoon päätytään, olisi access-yhteyden nopeutta syytä myös nostaa nykystandardien mukaiselle tasolle. 1-2M nopeus riittäisi varmasti yrityksen tarpeisiin vaikka asiakasverkko toteutettaisiin.

5.2 Palvelunhallinta

Koska yrityksellä ei ole omaa IT-henkilöä joka voisi vastata toiminnasta ja varsinkin tarjota tukea ongelmien esiintyessä paras vaihtoehto yrityksen kannalta olisi laatia sopiva sopimus paikallisen operaattorin kanssa jolloin saataisiin sieltä kuitenkin kaiken kattava palvelukokonaisuus. Ongelmana tässä on tietenkin siitä aiheutuvat kus-

tannukset. Ja välttämättä ei ole tässä vaiheessa varaa lähteä niin suurta investointia tekemään ottaen huomioon kuitenkin yrityksen ICT-kokonaisuuden pienen koon.

5.2.1 Palveluluettelo

Listataan yrityksen toiminnassa mukana olevat palvelut. Jaotellaan nämä tällä hetkellä sisäisesti toteutettuihin sekä ulkoisesti alihankkijan tai nimeltä mainitsemattoman free-lance tahon toimesta toteutettavat. Osa näistä ulkoisista palveluista ei ole aktiivisesti millään tavalla hallittuna, vaan ongelmien esiintyessä, yrityksestä kontaktoidaan tahoa joka pystyy heitä auttamaan kyseisessä ongelmassa. Suositus onkin, että kaikki palvelut, jota ei sisäisesti voida itse toteuttaa ulkoistetaan.

Sisäiset palvelut:

- Käyttäjätunnusten hallinnointi
- Ohjelmistojen asennus ja ylläpito
- Tietoturvallisuus
- Asiakastietokannan ylläpito ja varmuuskopiointi (tällä hetkellä, jatkossa AcuteFDS)

Ulkoiset palvelut:

- Sähköpostipalvelut
- Internet-yhteys
- Kotisivujen suunnittelu, teko ja ylläpito
- Viankorjaus (fyysinen- kuin sovelluspohjainen)
- Käyttötuki
- Domainin ylläpito
- Työ ohjelmistot (Acute Fysio)
- Verkkolaitteet

KUVIO 13. Palveluluettelo -ehdotus

Palvelu	Käyttäjät	Tukipalveluiden saatavuus	Vasteaika	Korjausaika	Käytettävyys /kk	Palveluntuottaja
Käyttötuki Laitevaihto	Henkilökunta	8-16, ma-pe 7-20, ma-pe	2h 2h	24h	90% 26h käyttökatkoa /kk	PPO PPO
Ohjelmistot	Henkilökunta	7:30-20, ma-pe	30min	1h	99,3% 1h 20min käyttökatkoa /kk	AcuteFDS
Kotisivut		8-16, ma-pe	1d	3d		KaPeKe
Internet yhteys Domain ylläpito Sähköposti Työasemat Verkkolaitteet viankorjaus	Henkilökunta	8-17, ma-pe	30min	1h	98 % 3h 36min käyttökatkoa /kk	PPO
Laskutus	Henkilökunta					AcuteFDS
Tietoturvallisuus Ohjelmisto asennus Tunnusten hallinta						Kannuksen Fysikaalinen Hoitolaitos

5.2.2 Työkalut ja sovellukset

Käydään läpi tarkemmin yrityksen toiminnan kannalta kriittiset ohjelmistot ja työkalut.

Fysio32 ja Acute Fysioterapia

Tärkein osa koko yrityksen toimintaa tällä hetkellä on heidän käyttämänsä sovellus joka hallitsee kaikki asiakastiedot, laskutuksen ja kirjaukset terapiasta ja muista toimitteista. Tästä syystä kyseinen ohjelmisto on syytä ottaa kiintopisteeksi heti alusta alkaen ja sen pohjalta tarkastellaan muuta ympäröivää kokonaisuutta. Vanha versio

mitä tällä hetkellä käytettään on edelleen Windows XP pohjainen ja ei toimi uudemmissa käyttöjärjestelmissä. Fysio32 on käytössä oleva ohjelmisto. Tämä ei ole suinkaan ainoa ongelma kyseisen sovelluksen kanssa. Useilta työasemilta ei myöskään voida käyttää ohjelmistoa samanaikaisesti. Ainoa tapa on jakaa "pääkoneelta" Fysion hakemisto muille koneille lähiverkossa, mutta tällöinkään ei samanaikaisesti voida tietokantaan kirjoittaa kuin yhdeltä koneelta. Näin ollen katsoisin tarpeelliseksi harkita uudemman version käyttöönottoa.

Uudemmassa versiossa käyttöliittymä on web-pohjainen ja kaikki asiakastiedot sijaitsevat kyseisen ohjelmiston valmistajan palvelimilla. Tämä toisi samalla turvaa niiden säilymiseen ja poistaisi yrityksen tarpeen jatkuvasti ottaa varmuuskopioita tietokannastaan. Uuden ohjelmiston lisenssi ei kuitenkaan ole aivan halpa. Vanhan tietokannan siirtäminen uuteen järjestelmään onnistuu kyllä toimittamalla se ohjelmiston valmistajalle.

Ollessani yhteydessä ohjelmiston valmistajaan Fysio32 -ohjelmiston tiimoilta minulle kerrottiin, että ohjelmiston aktiivinen kehittäminen on lopetettu tuolla vanhalla alustalla. Tuota vanhempaa ohjelmistoversiota ei ole odotettavissa missään vaiheessa esim. Windows 7 koneille tai edes Windows vista x64 -koneille. Ohjelmisto toimii luotettavasti ainoastaan Windows XP koneella sekä mahdollisesti Windows Vista x32 -koneilla. Tästä syystä ohjelmistonvaihto tulevaisuudessa uuteen koneeseen on mahdoton. Ohjelmistovalmistajan edustaja informoi uudemmasta versiosta joka toimii täysin selainpohjaisesti. Kaikki data tallennetaan suoraan ohjelmistovalmistajan palvelimille käyttämällä heidän web-käyttöliittymäänsä. Tämä keskittää kaikki tarvittavat työkalut samaan sijaintiin. Samalla tämä poistaisi yrityksen tarpeen tehdä manuaalisesti varmuuskopioita asiakastietokannastaan toistuvasti päivittäin, sekä mahdollistaisi usealta koneelta yhtäaikaisen asiakastietokannan käsittelyn. Alustavaa kustannusarviota ei pyydetty, mutta todelliset kustannukset olisivat useamman tuhannen euron luokkaa alustavasti. Ylläpito katetaan säännöllisillä kuukausimaksuilla.

Mikäli tähän uuteen ohjelmistoon siirryttäisiin tulisi ohjelmiston valmistajan (AcuteFDS) tulisi laatia samalla sopimus, missä sovitaan heidän osaltaan tietystä palvelutasosta jonka tulee täyttyä esim. kvartaaleittain tai kuukausittain. Normaali käytettävyys huomioon ottaen kyseisen sovelluksen tärkeyden voisi olla esim. 99,8% 7:00 - 21:00 välisenä aikana. Ongelmat jotka johtuvat muista kuin AcuteFDS:n toiminnasta

eivät tietysti tätä heidän käytettävyyttään laske. Mikäli kyseinen ehto ei täyty, voitaisiin sopia taloudellinen korvaus/hyvitys jonka tässä tapauksessa AcuteFDS maksaa yritykselle joko rahan muodossa tai esim. hyvityksenä tulevista maksuista tiettyyn rajaan asti.

Uudempi ohjelmisto kulkee Acute Fysioterapia -nimellä. Ohessa valmistajan esittely.

"Acute Fysioterapia - tulosta fysioterapiaan ja kuntoutukseen

Acute Fysioterapia on nykyaikaisen kuntoutusyksikön ja fysioterapialaitoksen päivittäisen työn kirjaamis- ja kehittämisväline. Tietojärjestelmä ohjaa käyttäjiä tehostamaan työtään ja ajankäyttöään.

Monipuoliset taustarekisterit helpottavat kirjaamista ja vähentävät virheiden mahdollisuutta. Laskutuksessa, raportoinnissa ja tilastoinnissa on huomioitu fysioterapian erityistarpeet ja sidosryhmien vaatimukset.

Järjestelmä perustuu selaintekniikan hyödyntämiseen. Palvelinyhteys muodostetaan tietoturvallisesti SSL-yhteydellä (verkkopankit käyttävät samanlaista yhteyttä).

Käytön aloittaminen ei vaadi suuria alkuinvestointeja. Riittää, että käytössä on toimiva Internet-yhteys ja Internet Explorer-selain.

Järjestelmä toimitetaan sovellusvuokrauksella (SaaS-palvelu). Edullinen kuukausimaksu sisältää:

- asiakastuen pääkäyttäjille – arkisin 8-16, tarvittaessa suora yhteys palvelimeen
- palvelimeen liittyvät kustannukset: hankinta, ylläpito, suojaus
- päivitykset
- varmuuskopiot
- palvelimen käyttöjärjestelmän ja varusohjelmat
- liitedokumenttien tallentamiseen tarvittavan levytilan"

(AcuteFDS 2011).

Sähköpostipalvelut

Tällä hetkellä sähköpostipalvelut on hankittu operaattorin kautta olevan internet liittymän ohessa. Palveluista ei makseta erillisiä maksuja internet yhteydestä aiheutuvien kustannusten lisäksi. Asiakkaan käytössä on domain nimi kannuksenfysikaalinen.fi josta on luovutettu valtuutusavain paikalliselle operaattorille joka ylläpitää domainia sähköpostipalveluiden osalta.

Erillisen sähköpostisopimuksen laatiminen ei ole suositteltavaa vaan sähköposti on hyvä pitää saman operaattorin kautta mistä muutkin yhteydet on hankittu. Mikäli yritys haluaa siirtyä yritysliittymään PPO pakki, niin tällöin tulee tarkastella sähköpostipuoltakin tarkemmin samassa yhteydessä ja onko nykyiseen ratkaisuun tarpeen tehdä muutoksia.

Kotisivut

Kotisivut ovat tällä hetkellä (KaPeKe) Raumakarinmainos -yrityksen ylläpidossa. He vastaavat sivujen suunnittelusta ja tekevät tarvittavat muutokset asiakkaan pyynnöstä. http://www.raumankarinmainos.fi/

Tässä olisi selkä mahdollisuus kilpailuttaa ylläpitäjän taho ja näin saataisiin kokonaiskustannuksia alemmas.

5.2.3 Tietokoneet ja muut laitteet

Tietokoneet ovat tällä hetkellä yrityksen omistuksessa, mutta tarvittaessa uudet koneet on mahdollista leasata esim. PPO:lta. Jotta vastuu eri ongelmista ei jakautuisi kovin monelle eri taholle, suositus vaihtoehdoksi on edelleen PPO:n tarjoamaa pakki -ratkaisu. Kyseiseen ratkaisuun liittyy myös koneiden leasaus. Tällöin laitteiden huolto ja ylläpito saataisiin myös operaattorin suuntaan. Tämä tulee paremmin ajankohtaiseksi kun muutkin yrityksen järjestelmät tullaan uudistamaan. Samoin, myös muut lähiverkonlaitteet olisi mahdollista varmasti sopia saman ylläpidon piiriin (tulostimet yms.). Maksupääte on käytännössä pankin vastuulla, mutta Internet-yhteyteen liittyvät ongelmat voitaisiin integroida PPO:n sopimukseen.

5.2.4 Käytettävyys ja SLA:t

Tällä hetkellä varsinkin toiminnan kannalta kriittisten palveluiden toteutus on epävarmalla pohjalla. Ei ole selkeää ylläpitoa tämän hetkisille palveluille ja yrityksen tulee ongelmien ilmetessä toimia parhaaksi katsomalla tavallaan. Suositus olisi ulkoistaa valtaosa palveluista tahoille joiden kanssa voidaan laatia erilliset sopimukset palveluiden käytettävyyksien ja rajojen suhteen.

5.2.4.1 PPO-pakki SLA

Operaattori jolla yritys on asiakkaana tarjoaa palvelua, jonka kautta saataisiin kaikki heidän IT-tarpeidensa ylläpito siirrettyä mainitulle operaattorille. Samalla voitaisiin laatia SLA-sopimus, missä sovitaan laitteiden ylläpidosta (mitä laitteita koskee), tietokoneiden leasauksesta (uudet koneet), viankorjauksen vasteajasta, käytettävästä Internet yhteydestä (päivitetään nykyinen), tietoturvapalvelut, sähköpostipalvelut, domain ylläpito, lähiverkonhallinta ja tuki. Tähän sopimukseen tulisi laatia myös SLA-ehdot jokaiselle eri tehtävälle sekä sopia palvelun käytettävyydestä kuukauden tai kvartaalin mittaisissa sykleissä.

Käytettävyydellä tarkoitetaan sitä prosentuaalista osuutta tiettynä aikana minä sovittu palvelu tulee olla yrityksen henkilöstön käytettävissä. Esimerkiksi lähitukipalveluiden (työasemat, tulostimet yms.) käytettävyys voisi olla 98% 08:00 - 17:00 välisenä aikana arkipäivisin. Mikäli tiettynä tarkastelujaksona PPO ei pysty ilmoitettuna aikavälinä ongelmaa korjaamaan, kerääntyy kuluvasta ajasta luonnollista negatiivista käytettävyyttä. Kuukaudessa lasketaan siis 20 työpäivää, jolloin 2% osuus 08-17 välisenä aikana olisi 3 tunti ja 36 minuuttia. Näin saadaan esimerkki toteutumisesta. Mikäli kuukauden aikana 08:00 - 17:00 välisenä aikana arkisin työasemat tai muut lähiverkonpalvelut ovat yhteensä yli 3h 36min poissa käytöstä eivät SLA-sopimuksen ehdot täyty. Tällöin PPO maksaa sopimukseen kirjattujen sanktioiden pohjalta tietyn korvauksen yritykselle joka tulee myös erikseen määritellä tietysti. Lähiverkonlaitteille kuten tietokoneet, tulostimet yms. korjausajaksi voitaisiin sopia esim. 2 vuorokautta. Tässä ajassa PPO:n tulee toimittaa uusi laite vioittuneen tilalle mikäli lähituki ei sitä pysty korjaaman erikseen säädetyn viankorjaus aikarajan puitteissa. Tällöin korjausaika käytännössä tarkoittaa 13h / päivä 7-20 välisenä aikana, 2h vasteaika ongelmaan.

SLA-sopimuksen tiukkuus vaikuttaa suoraan sen kuukausi hintaan joka tulee maksaa operaattorille ylläpidosta. Sanktioiksi voitaisiin sopia esimerkiksi, että operaattori maksaa kuukausimaksun tuplana takaisin yritykselle jokaisesta kuukaudesta jona kyseinen käytettävyys ei toteudu. Samaan SLA-sopimukseen voidaan sopia erikseen näin internet-yhteyden käytettävyys, lähituki sekä muut palvelut. Tällä tavoin operaattori voisi tarvittaessa hyvittää sanktiot esimerkiksi seuraavien kuukausimaksujen osalta. Voidaan myös osapuolten halutessa sopia kiinteät rahasummat mitkä maksetaan jos ehdot eivät täyty.

5.2.4.2 Acute Fysioterapia SLA

Acute Fysioterapia (uudempi versio siis Fysio32 -ohjelmistosta) on toiminnan kannalta keskeisin työkalu. Kun vanha sopimus puretaan ja siirrytään uudempaan tulisi siinä myös laatia SLA-sopimus palvelua tarjoavan tahon kanssa, jossa sovitaan palvelulle käytettävyys prosentti.

Esimerkkinä voisi toimi esimerkiksi 99,3% käytettävyys arkisin 07:30 - 17:00 välisenä aikana. Tämä käytettävyys prosentti on riippumaton Internet-yhteyden ja PPO:n SLA:n prosenteista, koska kyseessä ovat kuitenkin kaksi eri kokonaisuutta. Mikäli Internet-yhteyden käytettävyys on kuitenkin alle tuon 99,3% ei Acute Fysioterapian käytettävyyttä voida efektiivisesti mitata yrityksen toimesta vaan joudutaan luottamaan AcuteFDS:n sanaan palvelun toimivuudesta. Vastaavalla käytettävyydellä palvelu saisi olla kuukauden jaksossa 1 tunti ja 20 minuuttia poissa käytössä yrityksestä riippumattomista syistä. Mikäli kyseiset ehdot eivät täyty kuukauden jaksoissa AcuteFDS:n maksamina sanktioina pitää esim. kahden tai yhden kuukauden kuukausimaksut jotka voidaan suoraan hyvittää yrityksen maksamista kuukausimaksuista.

5.3 Tietoturva

Yrityksen koosta riippumatta tietoturva on erityisen tärkeässä roolissa kaikessa toiminnassa. Varsinkin asiakastietojen salassapito on erittäin tärkeässä roolissa sekä myös oman toiminnan kannalta tärkeät kohteet. Tietoturvapolitiikan ja strategian kautta pyritään laatimaan selkeät rajat yrityksen tietoturvalle. Tietoturvapolitiikassa katselmoidaan yleisemmällä tasolla yrityksen tietoturvaa liiketoiminnan kannalta ja näin

laaditaan suurpiirteiset toimintamallit joita pitää noudattaa. Tietoturvapolitiikan suunnittelussa katselmoidaan tyypillisesti tiedon luottamuksellisuutta, eheyttä sekä käytettävyyttä.

Toisena suurena kohtana on tietoturvastrategian valinta ja suunnittelu. Strategialla laaditaan tarkempi ohjeistus tietoturvan eri aspekteihin, kuten tietoturvan kehittämiseen, ylläpitämiseen, suojattavat kohteet. Myös alustavien tietoriskien havaitseminen ja tunnistaminen sekä hallitseminen kuuluu tietoturvastrategiaan. Pääsääntöisesti laaditaan keskeinen tavoite ja suuntaviivat mihin yrityksen tietoturvamenettelyillä pyritään ja millä tavalla.

Tietoturvaa syventää entisestään tietoturvasuunnitelma sekä riskianalyysi. Näissä vaiheissa pureudutaan konkreettisemmin suojattaviin kohteisiin, menetelmiin, sekä riskitekijöihin. Pyritään ennalta ehkäisemään kaikki mahdolliset riskit ja laaditaan toipumissuunnitelmat mikäli riski jostain syystä kuitenkin toteutuu. Samoin tietoturvasuunnitelmassa määritellään tarkemmin velvollisuudet ja vastuut ja toimintaohjeet yrityksen eri tahoille.

5.3.1 Tietoturvapolitiikka

Yrityksellä on velvollisuus pitää asiakkaidensa tiedot salassa sekä vaitiolovelvollisuus kaikkeen niihin liittyvään työympäristön sisällä- ja ulkopuolella. Ainoastaan työn suorittamisen kannalta tärkeää informaatiota voidaan vaihtaa terapeuttien ja heidän esimiestensä välillä sekä kyseessä olevan asiakkaan kanssa. Samoin yrityksellä on velvollisuus suojata kaikki tiedostat ja asiakirjat joissa käsitellään edellä mainittuja seikkoja. Laaditaan selkeät ohjeet ja menettelyt oikeaoppiselle tietojenkäsittelylle joita noudatetaan jokaisen työntekijän toimesta. Yrityksen johto vastaa aina viimekädessä yrityksen tietoturvallisuudesta. Yrityksen tietoturva käytännöistä tiedotetaan yrityksen sisällä ja/tai tehdään tarvittava dokumentaatio saataviksi kaikille yrityksen työntekijöille sekä velvoitetaan kaikkia työntekijöitä tutustumaan siihen, niin uusia kuin vanhojakin. Perustetaan tietoturvapolitiikka yleiseen tietoturvan periaatteeseen CIA (Confidentiality, Integrity, Availability) eli tiedon ja asiasisällön luottamuksellisuus, eheys sekä käytettävyys.

Luottamuksellisuudella varmistetaan, että ainoastaan henkilöillä kenellä on oikeus kyseiseen tietoon, taataan pääsy siihen. Heille annetaan selkeät rajat joita noudattamalla lainsäädännölliset ehdot eivät vaarannu.

Eheydellä varmistetaan tiedon autenttisuus. Tietosisältö ei saa missään vaiheessa vaarantua tai muuttua. Tämä varmistetaan myös antamalla ainoastaan asianmukaisille henkilöille pääsy kyseiseen tietoon.

Käytettävyydellä varmistetaan, että kyseiset toiminnan kannalta kriittiset tiedot ovat käytettävissä kun niitä tarvitaan. Yrityksen laatimilla palvelusopimuksilla ulkopuolisten tahojen suuntaan tuetaan käytettävyyttä tälle informaatiolla sekä oikeaa vasteaikaa viankorjaukselle mikäli palvelussa jossa tieto sijaitsee, on ongelmia. Näin käytettävyydellä saavutetaan korkea varmuus ja se ei vaaranna yrityksen tietoturvaa eikä taloudellista toimintaa.

5.3.2 Tietoturvastrategia

Jotta yrityksen tietoturvapolitiikka ja tietoturvallisuutta voidaan harjoittaa lain säätämällä tavalla, sitoutuu yrityksen johto ottamaan vastuun tietoturvan kehittämisestä ja ylläpitämisestä sekä sen eteenpäin viemisestä. Yrityksen toiminnan jatkumisen kannalta on elintärkeää, että tietoturva ei vaarannu missään muodossa. Tämä pätee kaikkiin yrityksen työntekijöihin, omistajiin, sekä esimiehiin. Yrityksen johdon velvollisuutena on taata myös työntekijöille turvallinen työympäristö.

Jokainen yrityksen osa, niin sisäiset kuin ulkoisetkin -tahot kantavat oman vastuunsa tietoturvasta yrityksen ohjeistamalla tavalla. Kyseinen ohjeistus koskee kaikkia yrityksen vanhoja, nykyisiä sekä uusia työntekijöitä. Ohjeistus koskee myös yrityksen johtoa, yhteistyökumppaneita, alihankkijoita ja palveluntarjoajia.

Kaikki yrityksen toimintaa käsittelevät tiedot tulee pitää salaisena kaikkien yrityksen palveluksessa olevien henkilöiden toimesta, sekä yhteistyötahojen toimesta. Mitään yrityksen ja muiden tahojen välisessä kanssakäymisessä esiin tulevaa tietoa ei saa eteenpäin luovuttaa ilman yrityksen johdon erikseen myöntämää lupaa. Asiakastiedot pidetään aina salaisina kaikkien toiminnassa mukana olevien tahojen osalta.

Yrityksen johdon tehtävänä on huolehtia lainsäädännöllisten vakuutusten voimassaolosta sekä toiminnan kannalta tärkeiden vakuuksien voimassaolosta. Tähän sisältyy kiinteistön, laitteiston ja työntekijöiden vakuutukset.

Suojattava aineisto käsittää yrityksen käyttämien sovellusten asiakastietokannan (pitää sisällään asiakaskertomukset, laskutukset, henkilökohtaiset tiedot, kaikki kanssakäyminen asiakkaan ja yrityksen välillä), kirjallisen dokumentaation joka liittyy asiakkaisiin tai yrityksen liiketoimintaan tai yrityssalaisuuksiin. Jokaisen tahon tulee tiedostaa henkilökohtaiset vastuunsa suojatun aineiston käsittelystä ja toimia ohjeistuksen mukaan joka tilanteessa.

Mikäli epäillään, että tietoturva ja tietosuoja on jotenkin vaarantunut, otetaan yhteyttä paikalliseen esimieheen joka kontaktoi yrityksen johtoa sekä tarvittaessa ulkoista yhteistyötahoa asian selvittämiseksi. Samalla pyritään tunnistamaan kuinka kyseinen tilanne on päässyt syntymään ja kehitetään tietoturvallisuutta tämän pohjalta. Laaditaan riskianalyysi ja tietoturvasuunnitelma.

Jos viranomaiset tarvitsevat jotain suojattavan aineiston tietoja tulee pyynnön tulla yrityksen johdolle suoraan viranomaisten taholta tai paikallisen esimiehen kautta. Yrityksen tulee ensin selvittää tietoja pyytävän henkilön henkilöllisyys ja oikea tarve tietoihin. Tällöinkin sovelletaan valtion lainsäädäntöä ja toimitaan vain sen puitteissa.

Tietoturvastrategian määrittelemiä henkilöitä tai tahoja koulutetaan ja valistetaan tietoturvakäytäntöön liittyvistä muutoksista ja tarvittaessa koulutetaan jos siihen tarvetta ilmenee.

5.3.3 Tietoturva-uhat

Yrityksen toimintaan vaikuttavia uhkatekijöitä on useita ja paras menetelmä niiden ehkäisemiseen on proaktiivinen toiminta. Puututaan uhkatekijöihin ennen kuin kyseinen riski toteutuu. Analysoidaan mitkä seikat muodostavat uhkia yrityksen toiminnan kannalta.

Luonnonmullistukset tai katastrofit.
Mahdolliset myrskyt, trombit, tulvat tai muut vastaavat luonnonmullistukset saattavat

aiheuttaa suurtakin vahinkoa yritykselle. Erityisesti toiminnan kannalta tärkeät laitteistot ja työvälineet saattavat rikkoontua tai mahdollisesti voidaan kärsiä jopa henkilövahingoista. Tämä tekee työskentelyn pahimmassa tapauksessa mahdottomaksi ennen kuin tilanne on ratkaistu.

Skenaario 1 : Alueelle tulee trombi, joka vaurioittaa kiinteistöä repimällä katon irti. Kosteutta pääsee sisälle toimitiloihin ja sekä kuntoutuslaitteistoa, että tietokoneita vioittuu kosteuden seurauksena.

Skenaario 2 : Mannerlaattojen liikkumisesta johtuen alueella tapahtuu maanjäristys ja työntekijä loukkaantuu kiinteistön kärsiessä vahinkoja ja joutuu olemaan pitkäkestoisesti poissa töistä tai mahdollisesti jäämään kokonaan pois.

Tulipalo, vesivahinko, sähköviat tai muu vastaava.
Mahdollinen kiinteistöä vahingoittava onnettomuus tai turma kuten tulipalo, vesivahinko tai vastaava. Tämä koskee kaikkia yrityksen toimintaa kyseisissä tiloissa ja näihin riskeihin tulee olla varauduttu oikeaoppisilla tavoilla. Myös henkilövahinkojen mahdollisuus on kyseisten uhkien kanssa kuin myös laitteiston vioittuminen.

Skenaario 1 : Naapuri kiinteistössä sattuu tulipalo joka leviää myös yrityksen toimitiloihin ja tekee ne kelvottomiksi kunnes vauriot on korjattu. Toiminta joudutaan siirtämään toisiin toimitiloihin tai keskeyttämään kokonaan tämän seurauksena.

Skenaario 2 : Yrityksen kuntosalin yhteydessä olevissa peseytymistiloissa on vesivahinko joka on levinnyt sähkökaapeleihin ja aiheuttaa oikosulun kiinteistön sähköverkossa joka rikkoo tietokoneen sekä tulostimen. Ennen kuin tilanne on korjattu ei voida kiinteistön sähköverkkoa käyttää turvallisesti.

Virukset, hakkerit ja haittaohjelmat.
Yksi suurimmista uhkatekijöistä yritykselle ovat erinäiset haittaohjelmat sekä virukset. Tämä on varsin yleinen ongelma nykypäivänä ja sitä varten tulee ehdottomasti toimia ennaltaehkäisevästi. Tiedostonsiirron välityksellä (Internet, ulkoinen laite kuten muistitikku, sähköposti yms.) haittaohjelmistot ja virukset pääsevät siirtymään yrityksen verkkoon. Myös hakkerit ovat riski. Joku saattaa halutessaan pyrkiä vahingoitta-

maan yritystä murtautumalla heidän verkkoonsa tai muutoin vahingoittamalla tai estämällä yrityksen palveluita.

Skenaario 1 : Yrityksen työntekijä lukee tietokoneella sähköposti viestin mikä sisältää liitetiedoston. Työntekijä suorittaa liitetiedostossa olevan ohjelmiston jonka seurauksena koneelle pääsee mato. Kyseinen mato alkaa työntekijän sekä kaikkien saman työaseman käyttäjien sähköpostitilejä käyttäen lähettää roskapostia (joka sisältää saman haittaohjelman liitetiedostona) kaikkiin muistissa oleviin sähköpostiosoitteisiin. Huonossa tapauksessa yrityksen verkon muut laitteet saastuvat myös ja alkavat toimia samoin. Tietokone joudutaan eristämään ja tartunta poistamaan. Operaattori saattaa myös katkaista Internet-yhteyksien toimivuuden kunnes tilanne on selvitetty näin estäen pääsyn työskentelyssä tarvittavaan ohjelmistoon. Yhteistyötahot joille kyseinen saastunut sähköpostiviesti on mennyt saavat pahimmassa tapauksessa tartunnan myös omiin järjestelmiinsä tai mahdollisesti estävät yrityksen domain -osoitteesta tulevan sähköpostiliikenteen. Tämän selvittäminen tahon kanssa aiheuttaa lisää rasitetta yritykselle.

Skenaario 2 : Työntekijä käy tauolla kyseenalaisilla Internet sivuilla jota kautta pääsee virustartunta evästeiden kautta koneelle. Virus leviää salakavalasti myös lähiverkon muille laitteille aiheuttaen toimintahäiriön laitteiden käynnistyksessä. Kaikki laitteet joudutaan puhdistamaan tai formatoimaan ja pahimmassa tapauksessa vaihtamaan uusiin riippuen virustartunnan vakavuudesta.

Työntekijät, asiakkaat ja yhteistyökumppanit.

Myös työntekijät, asiakkaat ja yhteistyökumppanit muodostavat riskiryhmän. Varsinkin tyytymättömät työntekijät voivat halutessaan aiheuttaa vahinkoa yrityksen toiminnalle ja järjestelmille. Samoin tyytymättömät asiakkaat ja yhteistyökumppanit. Uhka ei rajoita ainoastaan tyytymättömiin henkilöihin vaan ulottuu myös vahingossa tapahtuviin tilanteisiin. Huolimattomuus tai tietämättömyys muodostaa suuren riskin myös. Proaktiivinen ehkäisy kyseistein riskien kohdalla toimii jälleen parhaiten. Valistamalla henkilökuntaa ja kontrolloimalla asiakkaiden pääsyä tiloihin jossa vahinkoa voisi syntyä, voidaan rajoittaa tätä riskiä huomattavalla tavalla.

Skenaario 1 : Työntekijä kirjoittaa käyttäjätunnuksensa sekä salasanan paperille joka unohtuu työaseman viereen. Asiakas huomaa tilanteen ja kirjautuu yrityksen järjes-

telmään sekä peukaloi mahdollisesti omaa laskutustaan tai aiheuttaa muuta haittaa yrityksen järjestelmissä tai saa jotain salassa pidettävää tietoa muista asiakkaista mitä hän levittää eteenpäin.

Skenaario 2: Irtisanottu ex-työntekijä päättää livahtaa yrityksen tiloihin ja testata toimiiko hänen vanhat tunnuksensa järjestelmiin vielä. Tunnukset ovat edelleen toiminnassa ja työntekijä vääristelee terapia istuntojen kirjauksia sekä laskutusta tai tuhoaa koko asiakastietokannan.

Ilkivalta, murtautuminen, varkaus.

Riskin muodostaa myös mahdollinen ilkivalta jonka kohteena yritys on. Kyseessä voi olla ennalta harkittu rikos juuri yritystä vastaan tai satunnainen vandalismi. Myös murto on suuri riski koska yrityksellä on paljon fysioterapiassa ja kuntoutuksessa käytettävää laitteistoa joka on toiminnan kannalta kriittistä. Samoin tietokoneet ja työasemat voivat joutua anastuksen kohteeksi.

Skenaario 1 : Paikallinen nuoriso saa perjantai iltana idean töhriä kiinteistöjen seiniä ja ikkunoita spraymaalilla. Yrityksen tiloja tärvellään myös. Syyllistä ei saada kiinni koska käytössä ei ollut minkäänlaista kameravalvontaa ulkona.

Skenaario 2 : Yrityksen entinen asiakas on pistänyt merkille, että yrityksessä on paljon terapiassa käytettävää kallista laitteistoa. Entisenä asiakkaana hän tuntee yrityksen tilat ja osaa livahtaa huomaamatta sisään kiinteistöön. Hän varastaa osan yrityksen kalliista laitteistosta myyntitarkoituksessa.

Internet -yhteyksien puuttuminen/katkeaminen.

Pienemmän, mutta todennäköisemmän riskin muodostaa Internet yhteyksien katkeaminen. Tämä estää yrityksen asiakassovellusten käytön efektiivisesti, koska ne toimivat Internetin yli. Yhteyksien katkeaminen on melko todennäköistä, mutta voi johtua useista eri syistä. Nämä tulee huomioida tehtäessä SLA-sopimusta operaattorin kanssa, jotta palveluiden käytettävyys kärsii mahdollisimman vähän. Tietoturva on uhan kohteena tällaisissa tapauksissa siten, että kun asiakassovelluksia ei voida käyttää, joudutaan asiakastietoja dokumentoimaan muilla tavoilla. Tällöin tieto on riskialttiimmassa tilassa joutua vääriin käsiin.

Skenaario 1 : Iltapäivän aikana yrityksen Internet yhteydet katkeavat yllättäen juuri kun asiakaslaskutusta tai terapian seurantaa tehdään. Asiasta tehdään vikailmoitus, mutta yhteyksien korjaantuminen viivästyy. Yrityksen toiminta seisoo ja työt kasaantuvat, koska työkaluihin ei ole pääsyä.

Laiteviat.

Laiteviat muodostavat erittäin suuren riskiryhmän. Useimmiten laitteistoja tai ohjelmistoja tulee vaihtaa niiden elinkaaren aikana ja näin ollen se yleensä on jossain vaiheessa edessä jokaisen laitteen kohdalla. Ainoa tapa proaktiivisesti ehkäistä tätä on varautua kyseiseen tilanteeseen ennalta käsin. Varsinaista täydellistä ehkäisyä ei ole vaan ainoastaan tarpeeksi selkeä ja hyvä ohjeistus kuinka toimitaan kun kyseinen tilanne toteutuu.

Skenaario 1 : Modeemi/reititin lakkaa toimimasta. Yrityksen työkaluihin pääsy katkeaa kunnes tilalle saadaan uusi modeemi/reititin. Joudutaan hankkimaan itse uusi laitetilalle tai mahdollisesti hoitamaan se operaattorin kautta.

5.3.4 Riskianalyysi

Jotta tärkeitä resursseja pystyttäisiin suojaamaan ulkoisilta uhilta tulee yrityksellä olla selkeä riskianalyysi malli. Tarkastellaan mitkä uhat ovat todennäköisimpiä ja millaiset kulut niistä voi yritykselle aiheutua. Pyritään etsimään mahdolliset heikkoudet menettelyssä jo itse etukäteen ja näin ennalta ehkäistään riskiskenaarioita.

Uhkien vakavuutta voimme kuvata parhaiten riskianalyysi taulukolla. Luokitellaan erinäiset uhkatekijät todennäköisyyden ja vakavuuden mukaan. Emme lähde analysoimaan riskeistä aiheutuvia kuluja niiden toteutuessa rahamäärällisesti, koska tälle hetkellä ei ole täyttä varmuutta millä tavalla osa yrityksen palveluista toteutetaan. Olettamus on kuitenkin, että paikallinen operaattori PPO tulee vastaamaan laitehuollosta sekä vastaavista seikoista, joten kuluja ei aiheudu normaalia enempää kuin mitä SLA-sopimuksesta ja ylläpidosta jo maksetaan.

Käytetään luokitteluun siis todennäköisyyttä sekä vakavuutta parametreinä. Kokonaisriski muodostuu näistä arvoista. Molemmat kohdat pisteytetään asteikolla 1-4. Arvo 1 on todennäköisyyden osalta erittäin pieni ja vakavuuden osalta triviaali. Kokonaisriski selviää riskianalyysi taulukosta jossa riskit sijoitetaan oikeisiin ruutuihin mikä vastaa kyseisen tapahtuman todennäköisyyttä sekä vakavuutta. Vihreä kuvaa uhan pieneksi, keltainen vakavaksi, punainen kriittiseksi. Samalla saadaan myös selkeät prioriteetit eri riskeille, joten yhtäaikaisten sattuessa pystytään priorisoimaan toimintaa sekä kohdistamaan resursseja tehokkaammin. Kun riskien vakavuus on selvillä, laaditaan tietoturvasuunnitelma jossa pyritään ennaltaehkäisemään kyseiset riskit. Tämän jälkeen laaditaan jatkuvuus- ja toipumissuunnitelma sekä toimintaohjeet kyseisten riskien varalle.

Listataan eri uhkatekijät tarkemmin.

1. Luonnonmullistukset (myrsky, tulva, maanjäristys, trombi, yms.)
2. Tulipalo, vesivahinko, sähkövika.
3. Haittaohjelmat ja virukset.
4. Hakkerit.
5. Vandalismi
6. Murto, varkaus
7. Laiteviat
8. Ohjelmistoviat
9. Internet yhteyksien katkeaminen
10. Luvattomien henkilöiden pääsy järjestelmiin
11. Salassa pidettävän materiaalin pääsy väärin käsiin
12. Digitaalisen tai kirjallisen datan tuhoutuminen

KUVIO 14. Riskinhallinta analyysi -taulukko

TODENNÄKÖISYYS					
	Erittäin suuri		7	9	
	Suuri		10	8	
	Keskisuuri		3	12	2, 11
	Pieni	5	4	6	1
		Pieni	Keskisuuri	Suuri	Erittäin suuri
		VAKAVUUS			

Kun riskiluokitukset on näin määritelty, voidaan edetä suunnittelemaan tarkempaa tietoturvasuunnitelmaa jokaisin uhkanäkymän ennaltaehkäisemiseksi sekä toipumissuunnitelmaa näistä uhista selviytymiseksi niiden toteutuessa.

5.3.5 Tietoturvasuunnitelma

Tietoturvasuunnitelmaa lähdetään laatimaan riskianalyysin ja havaittujen uhkien pohjalta. Kun uhkatekijät ovat selvillä voidaan lähteä syventämään niitä ehkäisevät toimenpiteet konkreettisiksi toimenpiteiksi. Tarkastellaan tämän hetkistä tilanne ja ehdotetaan muutoksia siitä mitä tulevaisuudessa suosittelisin yrityksen ratkaisuksi kyseisen asian suhteen.

5.3.5.1 Palomuuri ja virustorjunta

Lähdetään ensimmäisenä tärkeimmästä kohteesta, eli asiakastietokannasta ja ohjelmistoista. Tällä hetkellä virustorjunta ja palomuuri ovat toteutettu sovelluspohjaisesti tietokoneilla käyttämällä AVGFree ja Comodo Personal Firewall. Nämä ovat molemmat konfiguroitu automaattisesti pysymään ajan tasalla sekä reaktiivisesti vastaamaan havaittuihin hälytyksiin. Toistaiseksi ratkaisu on toiminut halutulla tavalla. Sovelluspohjaisen palomuurin käyttö kyseisessä tapauksessa saattaa riittää, mutta tietokone on haavoittuvainen kuten aina sovelluspohjaisten palomuurien käytön kanssa. Sovelluspohjaiset virustorjunta- ja palomuuriohjelmistot havaitsevat ongelman yleensä vasta kun tartunta on jo saatu. Toisena vaihtoehtona olisi reitittimen vaihdon yhteydessä (mikäli tähän ryhdytään) konfiguroida tarpeeksi tarkat pääsylistat, mutta tämäkin vaih-

toehto tulee ajankohtaiseksi mikäli yritys päättää siirtyä yritysliittymään ja siinä tapauksessa tämä toteutus saadaan tehtyä operaattorin kautta.

Tämä onnistuisi jo aikaisemmin mainitun PPO-pakki ratkaisun kautta. Samassa yhteydessä voitaisiin harkita saman ratkaisun kautta PPO:n tarjoamaa virusturvaa joka tulisi samaan hintaan. He, kuten monet muutkin operaattorit, käyttävät F-Securen antivirus- ja palomuuriohjelmistoa. Tällä ratkaisulla saataisiin nykyiset työasemat sekä tulevaisuudessa hankitut, suojattua.

Internet selaimet työasemalla tulisi konfiguroida automaattisesti hävittämään evästeet sekä salasanat. Automaattista täyttöä ei tulisi myöskään käyttää. Virusturva olisi hyvä myös konfiguroida tarkastamaan automaattisesti sähköpostien liitetiedostot.

Kun yritys siirtää AcuteFDS:n uuteen Fysio -ohjelmistoon niin kaikki liikenne menee Internetin välityksellä heidän palvelimilleen. Tämä salataan SSL-salauksella, mutta tottakai työasemien päässä on edelleen tarve sovelluspohjaiselle palomuurille ja virusturvalle.

Näillä toimenpiteillä saataisiin viruksista ja haittaohjelmista, sekä hakkereista muodostuvat uhat pienemmiksi. Monitorointi valitettavasti on jo hieman hankalampaa ohjelmistopohjaisten sovellusten lokien lisäksi. Riippuen reitittimestä, jos siirrytään esim. Ciscon malleihin jäisi access-listoihin aina merkintä kun tulee liikennettä joka ei täytä näiden ehtoja. Näitä säännöllisesti tarkastelemalla voitaisiin pitää kirjaa tunkeutumisyrityksistä.

5.3.5.2 Varmuuskopiointi, redundanssi

Varmuuskopiointi on erittäin tärkeässä osassa tällä hetkellä. Varsinkin nykyisellään koska asiakastietokanta ja kaikki oleelliset tiedot sijaitsevat tällä hetkellä yhdellä yrityksen tietokoneella, on kokonaisuus näin ollen haavoittuva. Varmuuskopiot tästä tietokannasta otetaan päivittäin, yleensä muistitikulle joita on yksi jokaiselle päivälle. Tikkuja kuitenkin säilytetään myöskin yrityksen tiloissa, joten ratkaisu ei ole hyvä. Itse varmuuskopioinnista aiheutuu myöskin ylimääräistä vaivaa yrityksen työntekijöille.

Merkittävän parannuksen nykyiseen menetelmään tarjoaisi siirtyminen AcuteFDS:n tarjoamaan uudempaan versioon Fysio -ohjelmistosta. Näin ylläpito ja varmuuskopiointi saataisiin siirretty heidän taholleen. AcuteFDS ylläpitää asiakkastietokantaa omilla palvelimillaan sekä varmuuskopioivat sen säännöllisesti, esim. päivittäin. Tämä olisi hyvä myös mainita kirjallisesti SLA-sopimuksessa kun se laaditaan AcuteFDS:n kanssa.

Muu varmuuskopiointi voitaisiin toteuttaa Windowsin omien varmuuskopiointi työkalujen kautta. Tämä voitaisiin ajastaa tapahtuvaksi esim. yöllä tai illalla jolloin työasemilla on vähemmän käyttöä. Keskitetty sijainti voisi olla esim. PPO:n palvelin jolta järjestetään tilaa varmuuskopioille. Heidän Pakki -ratkaisussaan on mahdollista neuvotella myös varmuuskopiointi tärkeille tiedostoille. Samalla saataisiin varmuuskopiot fyysisesti eri osoitteeseen samoin kuin Fysio-ohjelmiston kanssa.

Mitä kirjalliseen sisältöön tulee, näitä on hieman hankalampi varmuuskopioida millään tavalla. Paras vaihtoehto olisi konvertoida asiakirjat myös digitaaliseen muotoon esim. skannaamalla ne tietokoneelle ja sitten lisätä kyseiset tiedostot varmuuskopioitavien tiedostojen luetteloon.

Redundanttisuus olisi tarpeen tilanteissa missä ulkoiset Internet-yhteydet katkeavat. Kun uuteen Fysio -ohjelmistoon on siirrytty WAN-yhteyksien merkitys kasvaa 100-prosenttiyksikköä. Näin ollen vaihtoehtoisena yhteytenä voisi harkita esim. mobiiliyhteyttä joltain operaattorilta. Tässä vaihtoehtoja onkin enemmän. Suosittelisin vaihtoehtoina PPO, Elisa tai DNA, koska kaikilta löytyy tukiasemia alueelta. Soneraltakin tukiasema löytyy, mutta se sijaitsee fyysisesti kauempana. Yhteyksien katketessa, voitaisiin toimintaa jatkaa ainakin yhdeltä tietokoneelta (harvoin useampi yhtäaikaisesti käytössä) tai myös jakaa tämän yhden koneen yhteys lähiverkossa. Toinen vaihtoehto olisi hankkia 3g-reititin tai käyttää sellaista suoraan myös normaaliyhteydessä. Tällöin laite voitaisiin konfiguroida aktivoimaan mobiiliyhteys kun lankayhteys katkeaa. Näin saavutettaisiin tietty yhteysvarmuus aina kun asiakassovellusta tarvitaan. Samoin tämän 3g-reititin ratkaisun kanssa saataisiin taattua myös toimivuus myös maksupäätteelle jolla asiakkaat usein maksavat terapiansa.

5.3.5.3 Käyttöoikeudet, käyttäjätunnukset ja salasanat

Tällä hetkellä yrityksellä ei ole omilla koneillaan mitään yhdenmukaista käyttöoikeus tai tunnus käytäntöä. Tunnuksia ei myöskään hallita esim. Active Directoryn yli, koneen pienestä määrästä johtuen, vaan kaikki tunnukset ovat paikallisia. Tämä ratkaisu toimii yritykselle, koska ainoa kriittinen tarve on hoitaa sähköposti asiat sekä kirjaukset asiakas työkaluilla. Varsinkin kun siirrytään Internet -pohjaiseen versioon ohjelmistosta, koneiden henkilökohtaisten käyttöoikeuksien merkitys vähenee huomattavasti.

Käyttöoikeuksia on rajoitettu tällä hetkellä siten, että muiden henkilöiden omia profiili kansioita konekohtaisesti ei pysty katselemaan. Käytännössä siis jokaisen oma /Profiilinimi/ on suojattu ja tiedot pysyvät henkilökohtaisena. Muutoin jokaisella tunnuksella on täydet järjestelmän valvojan oikeudet, eli tuokin rajoitus voitaisiin halutessa kumota ja näin päästä käsiksi tiedostoihin mitä ei ole tarkoitettu kaikkien nähtäväksi. Tähän tulisi tehdä muutos ja yhtenäistää tunnusten luonti politiikka. Kaikki olemassa olevat tunnukset muutettaisiin käyttäjiksi ja koneille määritettäisiin yksi ainoa järjestelmänvalvojantili, joka luovutettaisiin esimiehelle sekä toimitusjohtajalle.

Yrityksessä käytetään tällä hetkellä paljon samoja salasanoja ja ne ovat erittäin yksinkertaisia. Usein ne ovat selkokielisiä sanoja. Jotta näiden osalta päästäisiin parempaan varmuuteen, olisi syytä ottaa vaihtuvat salasanat käyttöön jokaisessa sovelluksessa. Salasanat voisivat vaihtua esim. 1-2 kuukauden välein ja edellyttäisivät vähintään 8 merkkiä, isoja ja pieniä kirjaimia sekä numeroita tai erikoismerkkejä. Myöskään viimeiset 6 edellistä salasanaa eivät kelpaisi. Tämä toki aiheuttaa työntekijöille enemmän muistettavaa, mutta kokonaisvaltaisesti tämä olisi tietoturvan kannalta paras ratkaisu. Kaikki yrityksen tietokoneet tulisi myös aina muistaa lukita tai käyttäjän kirjautua ulos aina kun poistutaan koneelta, jotta voidaan välttää tietoturvariskejä.

Jos yritys ottaa PPO:lta Pakki -paketin ja tietokoneet leasataan, olisi tällöin erityisesti syytä tehdä kokonaisuus tällä tavalla. Muutos helpottuisi myös siinä suhteessa, että vastuu ylläpidollisista tehtävistä jäisi täysin operaattorin vastuulle eikä työntekijöiden.

5.3.5.4 Fyysinen tietoturvallisuus

Kun huomioidaan mahdolliset riskit jotka aikaisemmin riskianalyysin yhteydessä havaittiin, tämän hetkinen tilanne ei ole paras mahdollinen. Yrityksellä ei ole minkään-

laista hälytysjärjestelmää jos kiinteistöön esim. murtaudutaan. Samoin minkäänlaista valvontajärjestelmää ei ole käytössä. Molemmat näistä ovat yleensä melko kalliita ratkaisuja ja riski uhille on erittäin pieni, mutta se on kuitenkin aina olemassa.

Murtohälytysjärjestelmän hankkimista pitäisin melko tärkeänä, koska tällä saataisiin tietty varmuus aina, että kiinteistö on kunnossa. Tällä saataisiin ehkäistyä murtoja sekä tarvittaessa henkilö paikalle nopeasti.

Kameravalvonta on toinen puute minkä hankkiminen olisi myös suotavaa. Näin voitaisiin valvoa toimitilojen ympäristöä ja reagoida tarvittaessa hälyttämällä esim. poliisi paikalle. Kamera järjestelmä voitaisiin yhdistää yrityksen lähiverkkoon hankkimalla kamerat jotka tukevat datansiirtoa ethernetin yli. Yhdelle tietokoneelle asennettaisiin kameroiden hallinta järjestelmä ja se voitaisiin konfiguroida esim. liikettä havaitessaan lähettämään viesti tai sähköposti yrityksen henkilöstölle. Tämä ratkaisu ei ole pakollinen, mutta se toimisi yhtenä seikkana jolla ulkoisia uhkia voitaisiin ehkäistä ennen ongelmien syntymistä.

Yrityksen toimitiloissa pääsyä toimistoon sekä tietokoneilla tulisi myöskin seurata ja kontrolloida, jotta asiattomia ei tiloissa liiku. Kun toimistossa ei ole ketään paikalla, tulisi se aina olla lukittuna. Tällä tavalla voidaan estää ulkopuolisten pääsy asiakirjoihin sekä tietokoneille. Jatkossa mikäli terapiahuoneisiin hankitaan tietokoneita, tulisi myös huoneiden olla lukittuna kun ne eivät ole käytössä ja vähintäänkin työpäätteiden tulisi olla lukittuna.

5.3.6 Jatkuvuus- ja toipumissuunnitelma sekä toimenpideohjeet

Mikäli jokin ennakoiduista riskitekijöistä toteutuu, tulee yrityksellä olla toimintasuunnitelma tilanteen varalle. Muutoin kyseinen riski saattaa johtaa yrityksen toiminta kyvyttömyyteen pitkäksikin ajaksi. Käydään uhkatekijät läpi ja laaditaan suunnitelma kuinka yritys voi jatkaa toimintaansa riskin toteutumisen jälkeen sekä kuinka menetellä riskin aikana.

5.3.6.1 Luonnonmullistukset, tulipalo, vesivahinko, kiinteistövauriot

Mikäli skenaario missä jokin luonnonvoima aiheuttaa vahinkoa yritykselle toteutuu, voidaan toimia seuraavalla tavalla. Ensimmäisenä tulisi arvioida tuhojen laajuus ja vakavuus. Jos kiinteistö on vaurioitunut tulee yrityksellä olla toissijainen paikka, jossa toimintaa voidaan harjoittaa tai terapiaa voidaan antaa esim. kotikäynneillä ainoastaan kunnes ongelma saadaan ratkaistua. Kyseessä ovat vuokratut toimitilat, joten omistajan velvollisuus on varmistaa, että vakuutukset ovat kunnossa ja tarvittaessa pyrkiä järjestämään toiset tilat yrityksen käyttöön. Työkalusovelluksia voidaan käyttää pitkälti Internetin yli SSL:llä mistä vain, joten kyseessä ei ole pakko olla työkone. Mikäli yritys on kuitenkin siirtynyt PPO-pakki sopimukseen, voi operaattori toimittaa uuden leasatun koneen vaurioituneiden tilalle.

Koska puhutaan mittavista kiinteistövaurioista kyseisessä skenaariossa korjaukset saattavat viedä paljonkin aikaa. Yrityksen toiminta ei saisi keskeytyä yli viikoksi kokonaan. Jos kiinteistön vuokraaja pystyy osoittamaan toiset tilat missä toimintaa voidaan jatkaa, tämän tulisi tapahtua 1 viikon kuluessa tai jos vanha kiinteistö voidaan korjata niin se tulisi tapahtua viikon sisällä. Kotikäynneillä yritys voisi jatkaa toimintaansa yhden päivän sisällä tapahtuneesta, mutta ei tällöin toimi täydellä kapasiteetillaan. Uudet leasatut laitteet operaattorilta tulisi saada 2 päivän kuluessa tapahtuneesta.

5.3.6.2 Laiteviat ja ongelmat

Kyseisellä ohjeella voidaan suunnitella toiminta tapauksessa jossa laite rikkoontuu, tuhoutuu tai katoaa. Kuten edellä jo sivuttiin kiinteistövaurioiden osalta jos jokin laite vioittuu tulee uusi saada tilalle mahdollisimman nopeasti. Ensimmäisenä tulee kartoittaa laiteongelman laajuus. Jos yritys on siirtynyt PPO:n pakki -ratkaisuun voidaan operaattorin kanssa säätää SLA-sopimukseen 2 päivän viive laitteiston korvaamiselle. Samoin pitää kartoittaa mitä laitteita tämä koskee, mutta suotavinta olisi, että se koskee kaikkia lähiverkonlaitteita. Tällä tavoin jos jokin laite on vioittunut tai kadonnut saadaan uusi nopeasti tilalle leasattuna operaattorilta.

Mikäli laite ei ole kokonaan toimintakelvoton niin sama 2 päivän viive laitteen vian tunnistamisessa ja korjaamisessa kuten SLA-sopimuksessa on säädetty. Jos ongelma on siis laitteen jossain komponentissa tai vastaavassa, noudatetaan SLA:ssa säädetty korjausaikaa, eli 30min vasteaika ja 1h korjausaika, 8-17 ma-pe. Jos taas laite joudutaan vaihtamaan kokonaan, noudatetaan SLA:ssa säädettyä laitevaihdon aikaa, eli 2h

vaste ja 24h laitevaihto, 7-20 ma-pe. Asiasta tulee tehdä vikailmoitus molemmissa tapauksissa operaattorin suuntaan.

Mikäli ongelma koskee Acute Fysion toimintaa, tehdään vikailmoitus AcuteFDS:n suuntaan jolloin he reagoivat siihen sovitulla vasteajalla.

Hätätapauksissa voidaan jatkaa työskentelyä esim. kotikoneella, mutta ensin tulee varmistaa, että kone on suojattu vähintään sovelluspohjaisella palomuurilla ja virusturvalla. Syytä olisi myös tarkastaa, ettei käytettävä kone ole jo altistunut jollekin haittaohjelmalle.

5.3.6.3 Murto, varkaus, vandalismi

Riippuen millaisesta vahingosta on kyse seurataan osittain samoja ohjeita kuin laiteongelmissa tai kiinteistövaurioissa. Laitevaihto tarvittaessa operaattorin kautta tai jos kiinteistö on vaurioitunut, yhteys kiinteistönomistajaan. Vakuutukset olisi hyvä aina olla kunnossa.

Kyseisten tapausten yhteydessä aina yhteys viranomaisiin ja tehdään rikosilmoitus jos ilkivalta täyttää rikoksen tunnusmerkit. Mikäli tällainen tapaus sattuu tulee viimeistään ottaa käyttöön suositeltu murtohälytysjärjestelmä ja/tai kameravalvonta.

5.3.6.4 Haittaohjelmat, virukset sekä datan tuhoutuminen tai vaurioituminen

Mikäli havaitaan tilanne jossa jokin työasema on saastunut tulee työasema ensimmäisenä kytkeä pois verkosta ja näin eristää muista laitteista. Tämän jälkeen asiasta tulisi tehdä vikailmoitus operaattorin suuntaan ja heidän korjata ongelma. Mikäli jotain tärkeää dataa on havaittu korruptoituneen, on siitä pidettävät juuri tästä syystä varmuuskopioita toisaalla operaattorin ylläpidossa. Tällöin riippumatta tartunnan vakavuudesta voidaan se poistaa tai ottaa käyttöön uusi työasema ja palauttaa tärkeä data sille varmuuskopioista. Tässä noudetaan kummassakin tilanteessa SLA:ssa säädetty 30min vasteaikaa ja 1h korjausaikaa paitsi jos laite joudutaan vaihtamaan kokonaan jolloin noudatetaan laitevaihto ohjeistusta.

5.3.6.5 Internet yhteyksien katkeaminen

Mikäli Internet yhteydet katkeavat tulee ensisijaisesti ilmoittaa operaattorille asiasta vikailmoitus jotta viankorjaus saadaan käynnistettyä. Tässä noudatetaan normaalia SLA:ssa säädetty vaste- ja viankorjausaikaa.

Suotavaa olisi kuitenkin itse pyrkiä rajaaman vikaa tai korjaamaan ongelma kokonaan. Yleisesti laitteiden virtaresetit auttaa varsinkin modeemi ja reititin ongelmiin. Samoin verkkokaapeleiden kytkennät olisi syytä tarkistaa.

Mikäli yritys hankkii redundanttiseksi vaihtoehdoksi 3g-reitittimen ja mobiiliyhteyden, tämän tulisi vastaavissa tilanteissa aktivoitua. Kyseistä skenaariota tulisi testata esim. irrottamalla puhelinkaapeli joka tulee modeemin. Näin nähdään aktivoituuko 3g-yhteys. Mikäli tämä ratkaisu toimii voidaan yhteyksien muuten ollessa poikki kuitenkin jatkaa toimintaa. Mikäli 3g-yhteys ei toimi siitä tulee tehdä vikailmoitus sille taholle, jolta se on hankittu. Mikäli kyseinen ratkaisu on myös PPO:lta voidaan yhteyteen soveltaa samoja SLA-ehtoja kuin kiinteään yhteyteenkin.

5.3.6.6 Tietomurto, tietovarkaus

Mikäli yrityksen tärkeitä tietoja kuten asiakastietoja, laskutustietoja, terapia istuntojen raportteja tai muuta vastaavaa vuotaa vääriin käsiin tulee ensin analysoida ja selvittää mitä kautta kyseinen tilanne on tapahtunut. Onko kyseessä ollut tietomurto Internetin kautta, yrityksen oman verkon kautta, vai fyysisesti käyty katsomassa luvatonta tietoa. Tässä avustaa operaattori kun asiasta tehdään vikailmoitus heidän suuntaansa. Kun kanava jota pitkän hyökkäys ja anastus tuli, on selvillä ensimmäisenä kehitetään ratkaisu jolla kyseinen turva-aukko saadaan tukittua jatkossa.

Itse varkaudelle ei valitettavasti voida paljoa tehdä. Kun syy ja tapa on selvillä voidaan kaikin keinoin pyrkiä minimoimaan anastajan hyöty kyseistä tapahtumasta ja jatkossa estää vastaavat tilanteet. Mikäli tapahtuma täyttää rikoksen tunnuspiirteet tulee asiasta tehdä rikosilmoitus poliisille.

5.4 Yhteenveto

Yrityksen tämän hetkisessä tilassa on paljon puutteita suhteessa ideaaliseen tilanteeseen, mutta kaikki ongelmat on mahdollista korjata. Palvelunhallinta ja tietoturva ovat suurimmat kysymykset tällä hetkellä. Kokonaisuus puuttuu, kaikki asiat ovat yrityksen vastuulla eikä niillä ole minkäänlaista keskitettyä menettelyä tai hallintaa. Kaksi suurinta muutosta jotka olisi syytä korjata ensimmäisenä ovat työkalujen päivittäminen ajan tasalla sekä palveluiden integroiminen Internet -yhteyteen ja näin siirtyminen PPO:n yritysasiakkaaksi.

PPO-pakki yritysliittymä ratkaisu olisi paras vaihtoehto kokonaisvaltaisen palvelunhallinnan kannalta. Operaattori tarjoaa kattavaa pakettia kaikille yrityksen tarvitsemille palveluille ja keskittäminen on aina helpoin vaihtoehto kuin kilpailuttaa jokainen eri osa-alue eri yrityksellä. Näin saadaan ongelma tilanteissa selkeä kuvio, yhteys operaattoriin sen sijaan, että joudutaan selvittämään mihin tahoon pitäisi olla yhteydessä. Samalla tämä ratkaisu täydentää uuteen Fysioon siirtymistä, koska Internet liittymälle voidaan sopia SLA:ssa parempi ylläpito kun normaalille kuluttajaliittymälle. Näin saadaan myös ehdoton toimintavarmuus (katso kappale 5.).

Kun nämä kaksi pääkohtaa on kontrollissa voidaan paneutua tarkemmin muihin yksittäisiin osiin yrityksen toimesta. Suositus on kuitenkin, että se mikä voidaan siirtää saman tahon ylläpitoon, siirretään. Kokonaisuudessaan kustannuksiltaan tämä ratkaisumalli on varmasti kalliimpi, mutta antaa selkeät ohjeet miten toimitaan ongelmien ilmetessä sekä luo vakaan pohjan jatkon kannalta. Kun toimintamallit ja käytännöt ovat toimivat on jatkossa muutoksia helpompi käsitellä ja hoitaa eteenpäin.

Osana PPO-pakki ratkaisua yrityksen tulee siis neuvotella samaan ylläpitoon lähiverkkolaitteensa, Internet -yhteys, lähituki, viankorjaus, laitehuolto, sähköpostipalvelut ja mahdollisesti uusi kotisivujen ylläpito näin halutessaan. Tällä vältytään kokonaisuuden hajottamiselta useiden eri ylläpitäjien suuntaan sekä minimoidaan yrityksen oma vastuu IT-puolen asioihin.

Fysio32-ohjelmiston uudempaan versioon tulisi siirtyä mitä pikimmin yhteistyössä AcuteFDS:n kanssa. Itse siirtymäprosessi on varsin vaivaton, koska ainoana teknisenä edellytyksenä on asiakastietokannan siirtäminen Acutelle heidän ohjeidensa mukaan

vanhalta tietokoneelta. Tämän jälkeen voidaan siirtymä uuteen tehdä heidän ilmoittamallaan aikataululla. Samassa yhteydessä suosittelisin määriteltäväksi jonkinlaisen SLA-sopimuksen jolla taataan tietty palvelunlaatu heiltä (katso kappale 5.). Tällä varmistetaan yrityksen toimintakyky ja mikäli ongelmia ilmenee on olemassa selkeä sopimus jota voidaan näissä tilanteissa tulkita sekä toimia sen mukaisesti. Tarjouspyyntö AcuteFDS:ltä tulisi yrityksen itse pyytää sekä ilmoittaa samalla sopimukseen haluamansa ehdot.

Tietoturvallisuuden suhteen yrityksen tulisi tarkistaa omat käytänteensä ja pyrkiä ottamaan ehdotetut muutokset käyttöön oman aikataulunsa mukaisesti. Suositus olisi ottaa muutokset käyttöön mahdollisimman pian. Tämä koskee kaikkia yrityksen sisäisiä menettelyitä tietoturvan osalta sekä skenaarioita jotka on esitetty riskianalyysin yhteydessä. Kun oma selusta sekä asiakkaiden turvataan voidaan toimintaa harjoittaa ja kehittää turvallisin mielin pelkäämättä tiedon joutumista vääriin käsiin tai yrityksen joutuvan muun uhan kohteeksi. Mikäli näin kävisi voi yritys turvautua jatkuvuussuunnitelmaan. Jatkuvuussuunnitelman osalta tulisi etukäteen varmistaa, että kyseiset ehdotetut menettelyt ovat suoritettavissa. Mikäli uhka on jo toteutunut on myöhäistä lähteä sopimaan jatkuvuusmenettelyistä mitkä tulisi tehdä hyvissä ajoin etukäteen.

Tämän opinnäytetyön kautta uskoisin yrityksen saavan tarpeelliset valmiudet lähteä kehittämään toimintaansa oikeaan suuntaan. Ohessa on annettu heille tarvittava lähtötieto sekä analysoitu nykyisen menettelyn heikot kohdat sekä laadittu kehitysehdotukset kuinka kokonaisuutta voisi parhaiten yrityksen tarpeet huomioiden viedä eteenpäin. Materiaalia laatiessa on pyritty sen helppolukuisuuteen sekä ymmärrettävyyteen jotta yritys pystyy siitä tehokkaammin hyötymään, koska varsinaista IT-puolen tuntemusta on erittäin vähän yrityksellä. Koko dokumentaatio on tarkoitettu yrityksen käyttöön ja he voivat tarpeen ilmetessä soveltaa tässä annettua informaatiota parhaallaan katsomalla tavalla.

Osittain vaikeutena kyseisen projektin osalta oli yrityksen pieni koko ja IT-puolen puuttuminen yrityksen sisällä. Tämä myötävaikutti lopputulokseen jossa pyrittiin mahdollisimman maallikolle ymmärrettävissä olevaan sisältöön. Verkkopuolen suunnittelu ja muutokset jäivät minimaaliseksi, koska yrityksen oman verkon koko on niin pieni. Tästä syystä painotus työn sisällön sekä yrityksen tarpeiden suhteen oli palvelunhallinnassa sekä tietoturvassa. Palveluiden määrä itsessään on melko pieni, joten

siitä syystä pyrittiin työssä ottamaan selkeäksi kiintopisteeksi yrityksen toiminnan kannalta tärkein työkalu eli Fysio -ohjelmisto ja laajennettiin kokonaisuutta tästä. Käytännöntoteutus jää yrityksen omaan harkintaan, koska päätöksen tekoon vaikuttaa voimakkaasti tämän hetkinen taloustilanne sekä tulevaisuuden näkymät.

Yrityksen tulevaisuuden näkymien osalta voitaisiin sanoa, että ohessa ehdotetut muutokset tulevat varmasti ajankohtaisiksi 1-3 vuoden sisällä. Tästä syystä yrityksen tulisi omaksua valtaosa ehdotetuista ratkaisuista tai tarvittaessa muokata niitä vielä enemmän näköisekseen. Tavoite tulisi kuitenkin olla, että yrityksen menettelyt olisivat nykystandardien mukaiset mahdollisimman pian sekä yhtenäinen kokonaisuus helposti hallittavissa.

LÄHTEET

3GPP 2011. HSPA: High speed packet access. viitattu 29.10.2011. http://www.3gpp.org/HSPA

AcuteFDS 2011. Fysioterapio ohjelmisto. Tuotekuvaus. viitattu 6.11.2011. http://www.acutefds.fi/tuotteet-ja-palvelut/fysioterapia

Brainbell.com 2011. Introduction to Networking. Ring Topology. kuvio. viitattu 25.11.2011. http://www.brainbell.com/tutorials/Networking/Ring_Topology.html

Cisco System Inc. 2011. Configuring a BGP Router Server, Figure 2 IX eBGP Full Mesh. kuvio. viitattu 9.10.2011. http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_route_server_xe.html

Cisco System Inc., 2011, Configuring a BGP Router Server, Figure 3 IX with eBGP Route Server. kuvio. viitattu 9.10.2011. http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_route_server_xe.html

Cisco System Inc. 2011. Configuring a BGP Router Server, Figure 1 IX Shared Switching Infrastructure. kuvio. viitattu 9.10.2011. http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_route_server_xe.html

Cisco Systems Inc. 2006. CCNP: Building Scalable Internetworks v5.0, Module 4: Integrated IS-IS. Cisco Systems Inc.

Cisco Systems Inc. 2006. CCNP: Building Scalable Internetworks v5.0, Module 6 BGP Autonomous Systems. Cisco Systems Inc.

Cisco Systems Inc. 2011. Interior Gateway Routing Protocol. viitattu 25.11.2011. http://docwiki.cisco.com/wiki/Interior_Gateway_Routing_Protocol

Cisco Systems Inc. 2011. Internetworking Technology Handbook. Quality of Service Networking. viitattu 25.11.2011. http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook#Quality_of_Service_Networking

Cisco Systems Inc. 2006. CCNP: Building Scalable Internetworks v5.0, Module 3 OSPF. Cisco Systems Inc.

Cisco Systems Inc. 2006. CCNP: Building Scalable Internetworks v5.0, Module 2 Overview of Scalable Internetworks. Cisco Systems Inc.

Cisco Systems Inc. 2009. Open System Interconnection Protocols. Summary of the OSI protocol suite. viitattu 5.10.2011. http://docwiki.cisco.com/wiki/Open_System_Interconnection_Protocols

Cisco Systems Inc., Cisco TV CDS 2.1 ISA Software Configuration Guide, Network Design, Figure 2-7 Hybrid Topology with Caching Nodes. kuvio. viitattu 9.10.2011. http://www.cisco.com/en/US/docs/video/cds/cda/tv/2_1/configuration/isa_guide/NetworkDesign.html

Da Silva, H. 2005. Optical Access Networks. viitattu 25.11.2011. http://www.co.it.pt/seminarios/webcasting/itcbr_09_03_05.pdf

Ericsson 2009. The evolution of EDGE. White paper. viitattu 25.11.2011. http://www.ericsson.com/res/docs/whitepapers/evolution_to_edge.pdf

FTTH Council 2006. FTTH Council - Definition of Terms Revision Date: 11 August 2006. FTTH Council

Hautamäki, J. 2009. IT-Palveluiden hallinta -kurssi. Luentomateriaali. Jyväskylän Ammattikorkeakoulu

Hautamäki, J. 2009. Tietoturvan teoria -kurssi, luentomateriaali, Jyväskylän Ammattikorkeakoulu

Hautamäki, J. 2011, Tietoturvan suunnittelu, koulutusmateriaali, Jyväskylän Ammattikorkeakoulu

Hedrick, C. 1988. RFC 1058: Routing Information Protocol, Rutgers University

ITSMF.fi 2011. ISO/IEC 20000. viitattu 31.10.2011. http://www.itsmf.fi/iso20000

Kannuksen fysikaalinen hoitolaitos 2011. Kotisivut. viitattu 27.11.2011. http://www.kannuksenfysikaalinen.fi

Koivisto M. 2007. KFHL Laatukäsikirja. Kannuksen Fysikaalinen Hoitolaitos

Kotikoski, S. 2009. Tietoturvan teoria -kurssi. luentomateriaali. Jyväskylän Ammattikorkeakoulu

Leino, J. 2009. Aktiivilaitteiden tietoturva -kurssi. Tietoliikennetekniikka. Kurssimateriaali. Jyväskylän ammattikorkeakoulu

Malkin G. 1998. RFC 2453: RIP version 2. Bay Networks

ManageEngine, ZOHO Corp. 2011. A beginner's guide to SNMP. viitattu 25.11.2011. http://www.snmplink.org/snmparticles/abeginnersguide/#1

Mitchell, B. 2011. Wireless / Networking Guide, Mesh Network Topology. kuvio. viitattu 9.10.2011. http://compnetworking.about.com/od/networkdesign/ig/Computer-Network-Topologies/Mesh-Network-Topology-Diagram.htm

Mitchell, B. 2011. Wireless / Networking Guide, Tree Network Topology. kuvio. viitattu 9.10.2011. http://compnetworking.about.com/od/networkdesign/ig/Computer-Network-Topologies/Tree-Network-Topology-Diagram.htm

NextiraOne 2011. Intergration services: Integrating technologies for customised solutions. viitattu 31.10.2011. http://www.nextiraone.eu/nl/services/integration_services

Novell 2011. Novell's Networking Primer: Data transmission. kuvio. viitattu 9.10.2011. http://www.novell.com/info/primer/prim05.html

PennWell Corporation 2011. FTTN/C. viitattu 25.11.2011. http://www.lightwaveonline.com/fttx/fttn-c/

Poole, I. 2011. UMTS / WCDMA basics tutorial & Overview. Adrio Communications Ltd. viitattu 25.11.2011. http://www.radio-electronics.com/info/cellulartelecomms/umts/umts_wcdma_tutorial.php

PPO 2011. PPO pakki. tuotekuvaus. viitattu 5.11.2011, http://www.ppo.fi/alltypes.asp?menu_id=1091, viitattu 5.11.2011

Rantonen, M. 2009. Käyttöjärjestelmien tietoturva -kurssi. luentomateriaali. Jyväskylän Ammattikorkeakoulu

Siltala, J. 2008. Laajakaista tekniikka -kurssi, ADSL-tekniikka. kurssimateriaali

Siltala, J. 2008. Laajakaista tekniikka -kurssi. Kaapelimodeemit. kurssimateriaali

Stoneburner, G., Hayden, C., Feringa, A. 2004. Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A, NIST Special Publication 800-27 Rev A

Telecom Forum 2011. General Packet Radio Service. viitattu 29.10.2011. http://www.telecomspace.com/datatech-gprs.html

Telecommunication standardization sector of ITU 2004. ITU-T Rec. G.991.2 (12/2003). standardi. ITU

Telecommunication standardization sector of ITU 2006. ITU-T G.991.1 (10/98). standardi. ITU

Telecommunication standardization sector of ITU 2006. ITU-T G.993.2 (02/06). standardi. ITU

The Art of Service 2009. ITIL® V3 Foundation Complete Certification Kit: 2009 Edition. The Art of Service

Wikipedia 2011. Fiber-to-the-x. kuvio. viitattu 16.9.2011. http://upload.wikimedia.org/wikipedia/commons/thumb/3/32/FTTX.png/300px-FTTX.png

Wikipedia 2011. Fiber-to-the-x. kuvio. viitattu 27.10.2011. http://upload.wikimedia.org/wikipedia/commons/thumb/7/74/PON_vs_AON.png/350px-PON_vs_AON.png