PIENYRITYKSEN TIETOHALLINTOSTRATEGIA 2006 - 2010

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto
Opinnäytetyö
Kevät 2006
Sami Herkepeus

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HERKEPEUS, SAMI: Pienyrityksen tietohallintostrategia 2006 - 2010

Tietoliikennetekniikan opinnäytetyö, 54 sivua, 11 liitesivua

Kevät 2006

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on kehittää Fennoscan Systems Oy:lle tietohallintostrategia. Työssä kartoitetaan yrityksen nykytilannetta sekä sitä, kuinka jo olemassa olevia resursseja voitaisiin hyödyntää tehokkaammin ja taloudellisemmin. Lisäksi tämän työn tavoitteena on kehittää yrityksen sisäistä dokumentointia yksityiskohtaisemmaksi.

Teoriaosuudessa käydään läpi TCP/IP-mallin kerrokset, lähiverkkojen yleisimmät verkkotekniikat (kuten Ethernet) sekä laitteet (kytkin, toistin, hubi, keskitin, reititin ja verkkokortti) ja kaapelityypit. Langattomien verkkojen osalta käsitellään mm. perusarkkitehtuureita (mm. Ad-Hoc) sekä siirtotekniikoita (DSSS, FHSS). Lisäksi käsitellään langallisten ja langattomien lähiverkkojen perustoimintaa. Tietoturva-asiat ovat nykymaailmassa yhä tärkeämmässä roolissa, eikä niihin liittyviä tekijöitä sovi unohtaa tästäkään työstä. Tietoturva on jaettu kuuteen osa-alueeseen: luottamuksellisuuteen, eheyteen, saatavuuteen, todentamiseen, pääsynvalvontaan sekä kiistämättömyyteen. Yritysten tietoturvaa ja erityyppisiä palomuureja käsitellään myös jonkin verran.

Yleensä tietohallintostrategia suunnitellaan 3 - 5 vuodeksi eteenpäin. Sen tärkeimmäksi tehtäväksi voidaan kuvata tietohallintoon liittyvät ratkaisu- ja toimintamallit, joita yksikön toiminnassa tullaan noudattamaan. Tietohallinnon keskeisin tehtävä on yksikön toiminnan tukeminen kaikin mahdollisin tietoteknisin keinoin. Tässä tapauksessa yksikkö on Fennoscan Systems Oy.

Opinnäytetyön käytännön osuus koostuu kahdesta osiosta: nykytilanteesta ja tietohallintostrategiasta. Nykytilanneosiossa on kartoitettu yrityksen nykyinen lähiverkon tilanne ja tämänhetkiset toimintatavat. Tässä osiossa on perehdytty lähinnä yrityksen työjärjestelyihin ja tietoverkkoon liittyviin asioihin. Tietohallintostrategiassa on linjattu tulevaisuuden suunnitelmia vuosille 2006 - 2010.

Tutkimuksen perusteella voidaan todeta, että tietohallintostrategian avulla yrityksen on helpompi varautua tulevaan. Lisäksi voidaan todeta, että tietohallintostrategian avulla yritys voi kehittää ja tehostaa toimintaansa.

Asiasanat: tietohallintostrategia, tietoverkot ja tietoturva

Lahti Polytechnic
Faculty of Technology

HERKEPEUS, SAMI: The strategy of information management in a small enterprise 2006 - 2010

Bachelor's thesis in Information Technology, 54 pages, 11 appendices

Spring 2006

ABSTRACT

The objective of this study was to create a strategy of information management for Fennoscan Systems. The study was focused on the company's current situation and how the existing resources could be taken into account more efficiently. In addition, the objective of this study was to improve the documentation within the company.

The theory section of the thesis describes the TCP/IP model, the most common modes of operation within a LAN (Ethernet), different devices (switches, repeaters, hubs, routers and network adapters), as well as some cable types and techniques. The WLAN section describes the basic architectures (e.g. Ad-Hoc) and transfer techniques (DSSS, FHSS). In addition, basic techniques of LAN and WLAN are described. Nowadays data security is a very important issue, so miscellaneous aspects regarding it are also considered. Security is divided into six different divisions; confidentiality, integrity, availability, documentation, access protocol and indisputableness. Data security and different types of firewalls are also discussed.

Usually the information management strategy is planned for a period of 3-5 years. It defines the solutions and patterns that the company will follow regarding its information management issues. The activity of the main unit is supported by the information management unit with all possible methods of information technology. In this case the main unit is Fennoscan Systems.

The empirical part of the analysis consists of two parts; the present-day conditions and the new information management strategy. The current situation and the procedures in Fennoscan Systems are discussed. This section also describes the administrative working patterns and issues related to the information networks. The strategy specifies the future plans for the years 2006 - 2010.

On the basis of this study it will be easier for Fennoscan Systems to prepare for the future and for their new customers. It remains to be seen whether the strategy will help the company to improve its operations and make them more efficient and possibly even accomplish financial savings.

Key words: strategy of information management, networks and data security

SISÄLTÖ

LYHENNELUETTELO

10Base-T	10 Mbit/s Baseband Twisted Pair. IEEE:n määrittelemä standardi, jossa määritellään, miten Ethernet-verkko rakennetaan suojaamattomasta parikaapelista. Verkko on rakenteeltaan tähtiverkko, ja sen maksiminopeus on 10 Mbit/s.
100Base-T	100 Mbit/s Baseband Twisted Pair. IEEE:n komiteassa luotu määrittely, jossa verkon maksiminopeudeksi on määritelty 100 Mbit/s.
1000Base-T	1000 Mbit/s Baseband Twisted Pair. IEEE:n komiteassa vuonna 1998 ehdotettu määrittely uudeksi 1000 Mbit/s nopeudella liikennöitäväksi Ethernet-verkoksi.
ARPANET	Advanced Research Projects Agency Network. Yhdysvaltain puolustusministeriön käyttöönottama korkeakoulujen ja tutkimuslaitoksien sisäinen pakettivälitteinen verkko. Toiminnassa vuosina 1969 - 1990, jonka jälkeen Internet on korvannut sen.
CAT-luokitus	Parikaapelit on jaettu eri nopeusluokkiin, esim. CAT5 (100 Mbit/s), CAT5e (1000 Mbit/s).
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance. Langattoman verkon siirtotien varausmenetelmä, jossa törmäykset havaitaan etukäteen lähettämällä siirtotien varaava signaali ennen dataa.
CSMA/CD	Carrier Sense Multiple Access/Collision Detection. Langallisen verkon siirtotien varausmenetelmä, jossa havaitun törmäyksen jälkeen sama data lähetetään satunnaisen ajan kuluttua uudelleen.

DSSS	Direct Sequence Spread Spectrum. Suorasekventointimenetelmä, yksi langattoman tietoverkon fyysisen tason hajaspektritekniikka.
FDDI	Fibre Distributed Data Interface. Tietoliikenteessä valokuitutekniikkaan perustuva lähiverkkostandardi, jonka standardointi aloitettiin vuonna 1982.
FHSS	Frequency Hopping Spread Spectrum. Taajuushyppelymenetelmä, toinen langattomassa tietoverkossa käyettävistä fyysisen tason hajaspektritekniikoista.
FTP	File Transfer Protocol, tiedonsiirtoprotokolla.
FTP-kaapeli	Foiled Twisted Pair, foliosuojattu parikaapeli.
Full Duplex	Liikennöintitapa, jolla tiedonsiirto tapahtuu samanaikaisesti molempiin suuntiin.
Half Duplex	Liikennöintitapa, jolla tiedonsiirto tapahtuu vuorosuuntaisesti.
IEEE	Institute of Electrical and Electronics Engineers. Yhdysvalloissa toimiva järjestö, joka toimii lähinnä tiedonsiirtoon aiottujen lähiverkkojen standardoimiseksi ja julkaisee niiden standardeja.
IEEE 802.3	IEEE:n kehittämä lähiverkon toimintastandardi, tunnetuimpia ovat mm. Ethernet, Token ring ja WLAN.
IEEE 802.11	IEEE:n kehittämä langattoman tietoliikenteen standardi. Sisältää useita alistandardeja, joista suosituin tällä hetkellä 802.11g.

IETF	Internet Engineering Task Force. Internet-protokollien standardointiorganisaatio.
IP-osoite	Internet Protocol. Palvelinkoneelle annettava 32-bittinen osoite, jolla verkon solmu tunnistetaan ja jolla määritetään reititystietoja. Sisältää palvelin- ja verkko-osan.
LAN	Local Area Network. Rajoitetulla maantieteellisellä alueella toimiva datasiirtoverkko.
MAC-osoite	Media Access Control. Verkkokortin ethernet-verkossa yksilöivä osoite. Useimmiten fyysisesti kirjoitettu jo tehtaalla kortille, mutta sitä voi myös vaihtaa ohjelmallisesti jälkikäteen. Osoite koostuu 12 heksadesimaalisesta numerosarjasta, joista ensimmäinen on valmistajan itselleen varaama etuliite ja jälkimmäinen juokseva sarjanumero.
MAN	Metropolitan Area Network. Yleisnimitys alueverkoille, jotka kattavat kaupungin tai jonkun muun taajama-alueen.
PROXY	Sovellusyhdyskäytävä. Järjestelmähallinnan määrittelemä yhdyskäytävä sovellusten välillä, johon liittyy sovellusten käyttäjien autentikointi.
RC4	Ron’s Code 4, RC4-salausavainta käytetään langattomissa lähiverkoissa, joissa on käytössä WEP-suojaus, liikenteen salaamiseen ja salauksen purkamiseen.
RFC	Request For Comments. RFC:t ovat asiakirjoja, jotka kuvaavat erilaisia Internetin käytäntöjä, lähinnä eri protokollia ja standardeja.

SDSL	Symmetric Digital Subscriber Line, symmetrinen digitaalinen tilaajalinja. Nopeus kumpaankin suuntaan yhtä suuri.
SSH	Secure Shell. Suomalaisen Tatu Ylösen kehittämä salausohjelmisto. Ohjelmaa käytetään tiedon salaamiseksi siirrettäessä tietoa IP-verkon yli.
SSL	Secure Sockets Layer, salausprotokolla jolla suojataan Internet-sovellusten tietoliikennettä IP-verkkojen yli.
STP	Shielded Twisted Pair, suojattu parikaapeli.
TCP/IP	Transmission Control Protocol/Internet Protocol. Tietoliikenteen tiedonsiirtokäytäntö, joka kehitettiin Yhdysvaltain puolustusministeriön toimesta. Kehitystyö aloitettiin 1960-luvulla, ja sitä jatkui 1980-luvun alkupuolelle.
TKIP	Temporal Key Integer Protocol. Tietoturvaprotokolla, joka on käytössä WPA-tekniikalla salatuissa langattomissa verkoissa.
Token Ring	Lähiverkon toimintastandardi, fyysiseltä topologialtaan tähtirengas mutta loogisesti rengasverkko, jossa käytetään valtuudensiirtoa.
UTP	Unshielded Twisted Pair, suojaamaton parikaapeli.
VPN	Virtual Private Network. Tekniikka, jonka avulla on mahdollista yhdistää toimipisteitä tietoturvallisesti julkisen verkon avulla.

WAN	Wide Area Network. Laaja tietoliikenneverkko, jolle on tyypillistä suuri maantieteellinen ulottuvuus.
WEP	Wireless Equivalent Privacy. Langattomissa lähiverkoissa käytetty suojausmenetelmä.
WLAN	Wireless Local Area Network. Langaton lähiverkko, joka käyttää siirtotienä infrapuna- tai radioaaltoja.
WPA	Wireless Fidelity Protected Access on langattoman lähiverkon tietoturvatekniikka, joka kehitettiin WEP-salauksen ongelmien paljastuttua.
XML	Extensible Markup Language on metakieli, jolla määritellään rakenteellisia merkkauskieliä.

1 JOHDANTO

1.1 Opinnäytetyön taustatiedot

Fennoscan Systems Oy on perustettu 1991. Yrityksellä on lähes viidentoista vuoden kokemus teknisten dokumenttien käsittelystä sähköisessä muodossa. Yritys markkinoi ainoana Pohjoismaisena jälleenmyyjänä australialaisen Mincom Pty:n valmistamaa LinkOne-ohjelmistoa, joka on tarkoitettu varaosakirjojen sekä huolto- ja käyttöohjeiden tuottamiseen ja jakeluun sähköisessä muodossa.

Yritys valmistaa myös omia ohjelmia ja tekee tarvittaessa asiakaskohtaisia ohjelmointiprojekteja dokumenttien julkaisuun sekä tietokannasta että Internet-jakeluun. Palveluna siirretään asiakkaan tekniset manuaalit sähköiseen muotoon. Sovituissa rajoissa hoidetaan palveluna koko teknisen dokumentaation tuottaminen ja jakelu.

Tällä hetkellä yrityksessä on kuusi työasemaa ja viisi palvelinta. Työasemissa on käyttöjärjestelminä Microsoft Windows 2000 ja Microsoft Windows XP, palvelimissa on käyttöjärjestelminä Microsoft Windows 2000, Windows 2000 Server sekä Windows 2003 Server.

Yrityksen runkoverkkona toimii PHP:n verkossa Utforsin 2 Mbit/s SDSL-linja (Symmetric Digital Subscriber Line). Sisäinen verkkoratkaisu on toteutettu kategorian 5 parikaapeloinnilla, jonka nopeusluokitus on 100 Mbit/s. Yrityksellä on internetyhteyssopimus Utforsin kanssa. Sähköposti- ja Internet-palvelinta ylläpitää Nebula Oy.

1.2 Opinnäytetyön tavoitteet

Tämän opinnäytetyön tavoitteena on kehittää Fennoscan Systems Oy:lle tietohallintostrategia. Keskeisenä tavoitteena on nykyisten resurssien tehokkaampi hyödyntäminen. Samalla keskitytään tietoturvan kehittämiseen.

Työn tutkimusongelmana on se, miten kehittää toimiva tietohallintostrategia. Aikaisempaa dokumentaatiota tietohallinnon suunnittelusta ei ole. Sisäverkosta, palvelimista ja työasemista ei ole olemassa dokumentaatiota.

Tutkimusmenetelminä käytetään analysointimenetelmiä. Näiden avulla kartoitetaan nykytilanne, ja sen jälkeen onkin vuorossa varsinaisen tietohallintostrategian luominen.

2 TIETOHALLINTOSTRATEGIA

Käsitteenä strategialla on monia merkityksiä. Strategisen johtamisen koulukunnasta riippuen määritelmät poikkeavat toisistaan. Toiselle strategia on sotasuunnitelma, toiselle visio ja joillekin vain joukko toimenpiteitä. Kattavimman määritelmän esittää Minzberg (1987). Hän jaottelee strategian viidelle eri tasolle:

- suunnitelma
- ase tai isku
- toimintatapa
- asema tai asemointi
- näkökulma

(Ruohonen & Salmela 2003, 150.)

Minzbergin (1994) näkemys strategiasta pohjautuu tiedostamattomaan kehitykseen ja tietoiseen ajatteluun ja suunnitteluun. Tietohallintostrategiaa suunnitellessa tällainen lähestymistapa voisi olla toimiva. (Ruohonen & Salmela 2003, 150.)

Tietohallintostrategialla on yksi tärkeä tehtävä. Sen tehtävänä on kuvata tietohallinnon ratkaisut ja periaatteet, joilla yrityksen toimintaa ohjataan tulevaisuudessa. Yksinkertaisuudessaan tämä tarkoittaa yrityksen teknisen arkkitehtuurin kehittämistä. Samalla huomioidaan myös ohjelmistot ja niiden käyttöön liittyvät asiat. (Bäckman & Lemmetyinen 1992, 57.)

Yrityksen tietohallintolla tarkoitetaan yleensä sitä yrityksen osastoa, joka suunnittelee ja ylläpitää tietojärjestelmiä. Yleisesti tätä osastoa kutsutaan tietohallinto-, tietotekniikka- tai atk-osastoksi. Nykyisin yrityksen tietojenkäsittelyä saatetaan toteuttaa eri puolilla organisaatiota ja keskitetty osasto tukee koko organisaation tietojenkäsittelyä. (Ruohonen & Salmela 2003, 123.)

3 TCP/IP

3.1 TCP/IP-malli yleisesti

Aikojen saatossa erilaiset verkot, puhelin-, data- ja kaapeliverkot, ovat yhtenäistyneet. Kun ennen jokaisessa verkossa kulki tiettyä sille kuuluvaa dataa, niin nykyään samassa verkossa kulkee ääni, kuva ja data. Tällaisen verkon runkona toimii yleensä TCP/IP-protokollaperhe (Transmission Control Protocol/Internet Protocol). (Kaario 2002, 13.)

TCP/IP-verkoilla yhdistetään monenlaisilla käyttöjärjestelmillä toimivia ja erilaisiin tarkoituksiin suunniteltuja laitteita toisiinsa. TCP/IP-verkkoja voidaan käyttää kaikkialla, missä on mahdollista toteuttaa TCP/IP-protokollapino. Tavallisen toimistoympäristön lisäksi sitä voidaan käyttää mm. langattomissa ympäristöissä ja automaatioverkoissa. Samanlaista monikäyttöisyyttä ei ole muilla tietoliikenteen verkkoteknologioilla. (Kaario 2002, 14.)

Protokolla tarkoittaa tiettyä säännöstöä, jolla kaksi samaa protokollaa käyttävää osapuolta voivat toimia yhdessä niin, että molemmat ymmärtävät toisiaan. Todellisessa elämässä esimerkiksi autolla ajo toteutetaan tietyllä protokollalla eli liikennesääntöjen mukaisesti. (Kaario 2002, 14.)

TCP/IP on protokollaperhe, joka rakentuu verkkokerroksen ympärille. Verkkokerroksen nimi on IP (Internet Protocol). TCP (Transmission Control Protocol) on verkkokerroksen yläpuolella, kuljetuskerroksella, toimiva luotettavan palvelun takaava protokolla. Muita protokollaperheeseen kuuluvia protokollia ovat mm. UDP (User Datagram Protocol) ja SNMP (Simple Network Management Protocol). (Kaario 2002, 15.)

Nykyinen TCP/IP-protokollaperhe on 1960-luvulla syntyneen ARPANETin (Advanced Research Projects Agency Network) jälkeläinen. ARPANETin ytimenä toimi Network Core Protocol. Internet nimenä oli tuolloin vielä tuntematon. Alkuun ARPANET yhdisti vain muutaman kilobittiluokan verkon laitteet, mutta

sen jälkeinen kasvu on ollut valtava. Sitä on käytetty mm. satelliittien liikennöintiin. (Kaario 2002, 15.)

Ensimmäisiä toimivia sovelluksia olivat Telnet ja FTP (File Transfer Protocol), mutta todellinen täyosuma oli sähköpostin keksiminen vuonna 1972. Lopullisen sinetin Internetin valtavalle kasvulle antoi vuonna 1991 julkistettu hypertekstisovellus Gopher ja samalla syntynyt World Wide Web (WWW). Ensimmäinen graafinen selain, Mosaic, julkaistiin vuonna 1992. Siitä eteenpäin Internetin kasvu on ollut valtava, liikennemäärä on jopa kymmenkertaistunut. (Kaario 2002, 15.)

Internet on kasvanut syntymästään lähtien räjähdysmäisesti. Vuoteen 2005 mennessä Internetin liikennemäärä onkin moninkertaistunut vuodesta 1991, jopa 4 - 10 kertaiseksi vuosittaistasolla.

3.2 TCP/IP-mallin kerrokset ja niiden tehtävät

TCP/IP-protokollaperheellä tarkoitetaan protokollajoukkoa, joka liittyy kiinteästi IP-protokollaan. TCP/IP-protokollaperheessä on periaatteessa viisi kerrosta (kts. KUVIO 1): fyysinen-, siirto-, verkko-, kuljetus- ja sovelluskerros, mutta kahta alinta kerrosta ei ole IETF:ssä (Internet Engineering Task Force) tarkemmin määritelty. Syynä on se, että TCP/IP-verkossa voidaan käyttää mitä tahansa verkkotekniikkaa. (Kaario 2002, 22.)

4	SOVELLUSKERROS
3	KULJETUSKERROS
2	VERKKOKERROS
1	SIIRTO- JA FYYSINEN KERROS

KUVIO 1. TCP/IP-pino (Kaario 2002, 22)

Sovelluskerroksen tehtävä on toimia tietoliikennesovelluksien yhteisenä kommunikointirajapintana verkkoon. Sovellusesimerkkejä ovat mm. sähköposti, päätekäyttö ja hakemistopalvelut. Sovelluskerros on lopullinen rajapinta sovelluksen ja tiedonsiirron välillä. (Kaario 2002, 21.)

Kuljetuskerros huolehtii yhteyden muodostamisesta järjestelmien välillä ja datan kuljettamisesta verkossa. Kuljetuskerroksen yläpuoliset kerrokset eivät ole tekemisissä tietoliikenneverkon kanssa. Kuljetuskerros toimiikin tässä eräänlaisena linkkinä alempien ja ylempien kerrosten välillä. Esimerkkiprotokollia tällä kerroksella ovat mm. TCP ja UDP. Tarvittaessa kuljetuskerros huolehtii pakettien vastaanottojärjestyksestä ja uudelleenlähetyksistä. (Kaario 2002, 21.)

Verkkokerroksen ehdottomasti tärkein tehtävä on datapakettien reititys verkon läpi oikeaan kohteeseen. Lisäksi se voi huolehtia palveluna vuonvalvonnasta ja laaduntarkkailusta. Protokollaesimerkiksi tälle kerrokselle soveltuu IP. (Kaario 2002, 20.)

Siirtokerros huolehtii bittivirran luotettavasta siirtotiestä. Tämä toteutetaan yhteyskäytännöllä, joka erottaa signaalista datan, tarkistaa sen oikeellisuuden ja lähettää sen eteenpäin määrämuotoisessa paketissa. Siirtoteitä voi olla käytössä yksi tai useampi, jotta yhteyden laatuvaatimukset saadaan toteutettua. Olennaisin osa siirtokerrosta on MAC-kerros (Media Access Control), joka takaa siirtokerroksen käytettävyyden eri käyttäjien kesken. Tunnetuin protokolla on CSMA/CD (Carrier Sense Multiple Access/Collision Detection). (Kaario 2002, 20.)

Fyysinen kerros toimittaa bittivirran fyysisesti eteenpäin huolehtimalla mm. liittimistä, siirtotien sähköisistä ominaisuuksista ja signaalitasoista. Fyysinen kerros ottaa kantaa fysikaalisiin ilmiöihin muiden kerrosten ollessa lähinnä ohjelmallisia määrittelyjä. Tärkeimpiä parametrejä ovat siirtovirhesuhde, siirtonopeus ja siirtoviive. Kerroksen tehtävä on myös synkronoida datansiirtoa. (Kaario 2002, 19.)

4 LÄHIVERKOT

4.1 Lähiverkon kuvaus

Verkko on erilaisten kaapelien, radioyhteyden tai valokuidun avulla yhteen liitetty tietokonelaitteiden joukko. Nämä laitteet kommunikoivat keskenään eri yhteyksien välityksellä. (Jaakohuhta 2002, 4.)

Verkko voidaan jakaa kolmeen eri kategoriaan: LAN (Local Area Network), MAN (Metropolitan Area Network) ja WAN (Wide Area Network). Näistä LAN on maantieteellisesti rajatuin pienehkö verkko. Se on yleensä yhden organisaation hallinnassa oleva verkko, jolla on suuri siirtonopeus. MAN kattaa kaupungin, kuntayhtymän tai taajama-alueen ja laajin verkoista, WAN, toimii paikkakunnalta toiselle tai jopa maanrajojen ulkopuolella maanosien välisenä verkkona. (Jaakohuhta 2002, 4.)

4.1.1 Lähiverkon ominaispiirteitä

Lähiverkko on dataverkko, joka yhdistää tietokoneet ja oheislaitteet. Tietokoneiden välisen datasiirron toiminta on hyvin tarkasti määriteltyä. Verkon toiminta-alue voidaan rajoittaa esimerkiksi tiettyyn rakennukseen tai jollekin alueelle. Lähiverkkoja voidaan yhdistää toisiinsa etäyhteyksillä. (Puska 2000, 14.)

Nopeus lähiverkossa on kymmenestä megabitistä per sekunti (Mbps) jopa kymmeneen gigabittiin per sekunti (Gbps). Nopeutta nostettaessa yritykselle koituu kertaluonteinen investointikustannus eikä erillisiä liikennöintimaksuja aiheudu. (Puska 2000, 14.)

Lähiverkot ovat jaetun median verkkoja. Tämä tarkoittaa sitä, että kaikki tietokoneet on liitetty samaan siirtotiehen. Tällöin, kun yksi tietokone lähettää dataa,

kaikki verkossa olevat tietokoneet kuulevat sen. Kohdekone tunnistetaan dataan sisältyvästä osoitteesta. (Puska 2000, 14.)

4.1.2 Lähiverkon laitteet ja niiden tehtävät

Kaapeloinnin avulla päätelaitteet liitetään verkkolaitteisiin. Kaapelointi toimii siirtotienä näiden laitteiden ja verkon palveluiden välillä. (Jaakohuhta 2002, 35.)

Lähiverkossa kaapelointi voidaan toteuttaa koaksiaali- tai parikaapelilla tai valokuidulla. Kaapelointi on myös media, tarkemmin määriteltynä siirtomedia tai siirtotie. Median päätyypeistä on olemassa monta versiota, ja esimerkiksi valokuitu on jaoteltu yksimuoto- ja monimuotokuituihin, ja nämä edelleen ulko- ja sisäasennuskuituihin. (Jaakohuhta 2002, 35.)

Valokuidun ydin on lasia, ja se on suojattu monella erilaisella suojakerroksella. Valokuidun kaksi päätyyppiä ovat yksimuoto- ja monimuotokuitu. Monimuotokuitu on yleisin lähiverkkokäytössä, pitkillä matkoilla taas käytetään yksimuotokuitua sen parempien siirto-ominaisuuksien johdosta. Kaapelin merkinnässä ensimmäinen luku ilmaisee ytimen halkaisijan, toinen luku vaipan halkaisijan. Molemmat mitat ovat millin tuhannesosia. (Jaakohuhta 2002, 63.)

Kierretty parikaapeli muodostuu ytimestä ja eristeestä. Ydin on kuparia, joka on suojattu eristävällä materiaalilla. Ydin ja eriste yhdessä muodostavat johtimen. Kun kaksi em. johdinta on kierretty toisiinsa, on kyseessä yksiparinen kierretty parikaapeli. Seuraavalla sivulla olevassa taulukossa (TAULUKKO 1) on lueteltu yleisimmät parikaapelityypit ja niiden ominaisuudet. (Jaakohuhta 2002, 65.)

TAULUKKO 1. Ethernet-kaapeloinnit nopeusluokittain (Jaakohuhta 2002, 339)

NOPEUSLUOKKA	KAAPELI
10Base2	50 ohm koaksiaali
10Base5	50 ohm koaksiaali
10Base-T	UTP, STP, Cat 4,5,6
10Base-F	50/125 um MM
10Base-F	62,5/125 um MM
10Base-F	8-9/125 um SM
10Base	AUI-kaapeli
100Base-TX	UTP, STP, Cat 5,5+,6
100Base-T4	UTP, STP, Cat 3,5,5+,6
100Base-FX HDX	62,5/125 um MM
100Base-FX FDX	62,5/125 um MM
100Base-FX FDX	8-9/125 um SM
1000Base-T	UTP, STP, Cat 5,5+,6
1000Base-TX	UTP, STP, Cat 6
1000Base-CX	Twinax STP 150 ohm
1000Base-SX	50/125 um MM
1000Base-SX	62,5/125 um MM
1000Base-LX	50/125 um MM
1000Base-LX	62,5/125 um MM
1000Base-LX	8-9/125 um SM

TAULUKKO 2. Taulukon 1 selitykset. (Jaakohuhta 2002, 339)

TAULUKON 1 SELITYKSET		
MM	Multi mode fiber	monimuotokuitu
SM	Single mode fiber	yksimuotokuitu
STP	Shielded twisted pair	suojattu kierretty pari
UTP	Unshielded twisted pair	suojaamaton kierretty pari
HDX	Half duplex	vuorosuuntainen
FDX	Full duplex	kaksisuuntainen
AUI	Attachment unit interface	laiteliitäntä
Cat	Category	luokka

Tietokone liitetään verkkoon verkkokortilla. Verkkokortti sovittaa lähiverkossa käytetyn kaapeloinnin ja tietokoneen toisiinsa. Verkkokortista käytetään myös lyhennettä NIC (Network Interface Card). Usein verkkokortti on integroitu tietokoneen emolevylle. Tällöin sen huoltaminen ja vaihtaminen on mahdotonta. Useimmiten käytössä parempi vaihtoehto onkin erikseen asennettava verkkokortti. Verkkokortissa on oma prosessori ja muisti, joilla se hoitaa verkon ja tietokoneen välistä liikennöintiä. Tärkein osa on lähetin-vastaanotin, joka hoitaa verkkoliikenteen. (Jaakohuhta 2002, 117.)

Jokainen verkkokortin valmistaja liittää korttiin kiinteän 48-bittisen MAC-osoitteen. Osoitteet määrittelee ja jakaa IEEE (Institute of Electrical and Electronic Engineers). Tällä varmistetaan, että jokainen verkon komponentti liikennöi omalla yksilöllisellä osoitteellaan. Osoitteen kolme ensimmäistä tavua ovat valmistajan tunnus, loput kolme tavua valmistaja voi itse määritellä. Joidenkin verkkokorttien osoitteen voi muuttaa tarvittaessa. Osoitteen saa selville verkko-ohjelmiston komennoilla tai soveltuvalla diagnostiikka-ohjelmalla. (Jaakohuhta 2002, 117 - 118.)

4.1.3 Lähiverkon aktiivilaitteet ja niiden tehtävät

Toistin tunnetaan myös hubina tai keskittimenä. Toistimella jaetaan mediaa, jolla tarkoitetaan laitteen tai kaapelin kapasiteetin jakamista kaikille käyttäjille samaan aikaan. (Jaakohuhta 2002, 98 - 99.)

Toistimella vahvistetaan verkossa kulkevaa signaalia ja näin saadaan verkolle ulottuvuutta. Toistimella voidaan myös liittää verkkosegmenttejä toisiinsa. Nimensä mukaisesti toistin toistaa vastaanottamansa signaalin kaikkiin portteihin, paitsi siihen, josta signaali tuli. Toistin ei suodata eikä tarkista virheellistä liikennettä. Toistimella voidaan sovittaa erilaisia medioita toisiinsa, esim. valokaapeliverkon voi liittää parikaapeliverkkoon. (Jaakohuhta 2002, 100.)

Kytkin on kehysten välittäjä, jonka tehtävä on välittää kehykset lähdeportista kohdeporttiin mahdollisimman nopeasti annettujen ohjeiden mukaisesti. Lähiverkko-

kytkimillä voidaan tehostaa hitaiksi käyneitä verkkoja. Nykyisin kytkin on lähiverkon keskeisin osa ja sen saa liitettyä erilaisiin verkkoihin: (Jaakohuhta 2002, 137 - 138.)

Kytkimen idea on tarjota sen jokaiselle portille verkon täysi kaista, verkosta riippuen 10 - 10000 Mbps. Nopeuden mahdollistaa kytkimen taustaväylä ja kehyksen reititys. (Jaakohuhta 2002, 137 - 138.)

Reititin yhdistää tai eristää lähiverkkojen aliverkot toisiinsa. WAN-verkoissa reititin sovittaa liikenteen modeemin ja lähiverkon välille. Reitittimellä voidaan rajata myös levitysviestejä lähiverkossa. Reititin sisältää MAC-osoitteen, jolla se tunnistetaan lähiverkossa. (Jaakohuhta 2002, 110.)

4.2 Työryhmä- ja toimialueverkko yrityksen käytössä

Yrityksen sisäinen tietokoneverkko voi olla joko palvelinperustainen toimialueverkko tai vertaisverkkoperiaatteella toimiva työryhmäverkko. Verkkotyypin valinta riippuu yrityksen koosta, toimialasta, tietoturvatasosta, toiminnan laajuudesta, verkon käyttäjien tarpeista sekä käytettävissä olevasta rahasta. Palvelinpohjainen ratkaisu on usein järkevä valinta suuren yrityksen käyttöön keskitetyn ylläpidon helppouden takia. Nykypäivänä ylläpito saattaa olla ulkoistettu palvelu. Pienissä yrityksissä, joissa tiedonsiirto on vähäistä, saattaa työryhmän käyttö olla perusteltua edullisempana ja näppärämpänä vaihtoehtona.
(Oulun kauppaoppilaitos 2005.)

Työryhmäverkossa ei välttämättä ole käytössä varsinaista palvelinta. Kaikki työasemat ovat tasavertaisia keskenään ja jakavat resurssejaan toisten käyttöön, esimerkiksi koneeseen liitetyn tulostimen tai jonkin tiedostokansion. Työryhmäverkon hallinta ei ole keskitetty yhdelle koneelle. Suurempien työasemakokonaisuuksien hallinta tällaisessa verkossa onkin hankalaa, koska jokaista konetta hallitaan erikseen. Työryhmäverkon ohjelmistojen ei tarvitse olla viimeistä huutoa olevia palvelinkäyttöön suunniteltuja ohjelmia, ja ylläpitäjien tiedot ja taidot

saattavat usein olla eri tasolla keskenään. Pienessä verkkokäytössä työryhmäverkko on edullinen ja paras vaihtoehto. (Oulun kauppaoppilaitos 2005.)

Palvelinperustainen verkko on yleensä suurten yritysten käytössä keskitetyn hallinnan ja ylläpidon vuoksi. Palvelimilla on useita erilaisia rooleja, esimerkiksi tulostin- tiedosto-, sovellus- ja sähköpostipalvelin. Palvelinperustaisen verkon käytöllä on useita etuja työryhmäverkkoon nähden: resurssit jaetaan yhdessä paikassa, turvallisuus on yhden ylläpitäjän käsissä, varmuuskopiointi on helppoa ja keskitettyä. Palvelimen kautta voidaan rajoittaa tiettyjen työasemien käyttöä. (Oulun kauppaoppilaitos 2005.)

4.3 Langalliset lähiverkot

4.3.1 Ethernet 802.3 ennen ja nyt

Ethernet on reilun 25 vuoden aikana toiminut 4800 bittiä sekunnissa (bps) siirtävällä radiotiellä, nykypäivän 1000 Mbps, ja kohta jo 10000 Mbps parikaapeli- ja valokuituverkossa. Se on maailman yleisin lähiverkkotekniikka. (Jaakohuhta 2002, 9.)

Ethernet toimii jaetulla siirtotiellä. Idea syntyi 1960-luvun lopulla Havaijin yliopistossa Norman Abramsonin johtamassa työryhmässä. Siitä sai alkunsa radioverkko nimeltä ALOHA. Järjestelmä käytti yhtä lähetyskanavaa ja yhtä tulevan liikenteen kanavaa. Pääkoneelta etäpisteisiin muodostettiin suora yhteys. Pääkoneelta lähtevä data lähetettiin kaikkiin etäpisteisiin yhtäaikaa. Datan otsaketiedoissa oli kohdeosoite, josta vastaanottava kone tunnisti, kuuluuko se sille. Pääkoneelle saapuva data tuli omaa kanavaansa pitkin käyttäen satunnaista uudelleenlähetystä datan häviämisen estämiseksi. Jos data tuli hylätyksi eli oli tapahtunut törmäys, asema tulkitsi sen niin, että jokin toinen asema oli lähettänyt dataa samaan aikaan. Tällöin asema odotti satunnaisen ajan ja lähetti datan uudelleen. Tätä

verkkoa kutsuttiin kilpavarausverkoksi, koska kaikki lähettävät asemat kilpailevat samasta kaistasta. (Jaakohuhta 2002, 9.)

Nykyajan Ethernet syntyi heinäkuussa 1972 Robert Metcalfen toimesta. Ensimmäisen kerran liikennöitiin toukokuun 22. päivä vuonna 1973. Tällöin nopeus oli 2,94 Mbps. Suurin parannus oli törmäyksentunnistus (collision detection). Se tarkoitti sitä, että asema kuunteli ennen lähetystä onko kaista vapaa. Vuoden 1977 lopulla Metcalfe työtovereineen sai patentin työlleen, monilähetysjärjestelmälle, joka nykyisin tunnetaan nimellä CSMA/CD. (Jaakohuhta 2002, 11 - 12.)

IEEE aloitti kesäkuussa 1981 802.3 -projektin, jonka tavoitteena oli tuottaa kansainvälisesti hyväksytty standardi. Varsinainen Ethernet 802.3 -standardi syntyi IEEE:n toimesta 1983. Nykyään Ethernet ja 802.3 tarkoittavat samaa asiaa. (Jaakohuhta 2002, 14 - 15.)

4.3.2 Ethernetin toiminta

Perinteisesti lähiverkko on toiminut 10 Mbps väylätyyppisessä verkossa. Päätelaitteet on kytketty väylään toistimen kautta, jolloin muodostuu törmäysalueita. Törmäysalue on se alue, jonka sisällä törmäys havaitaan. Levitysviestialue on alue, jonka sisällä levitysviestit tavoittavat kaikki päätelaitteet. (Jaakohuhta 2002, 91 - 92.)

Ethernet-verkossa liikennöinti perustuu CSMA/CD-menettelyyn. Lähettävä asema kuuntelee kaistaa ennen lähetystä, ja jos kaista on vapaa, sanoma lähetetään. Vain yksi asema kerrallaan saa lähettää. Joskus voi kuitenkin käydä niin, että kaksi asemaa lähettää yhtä aikaa. Tällöin tapahtuu törmäys, jonka jälkeen törmäyksen havainnut asema vahvistaa törmäyksen ja lähettävät osapuolet arpovat satunnaisen uudelleenlähetysajan. Uutta dataa ei voi myöskään lähettää ennen kuin edellinen lähetys on saapunut vastaanottajalle. Muut asemat odottavat tällöin vuoroaan, koska kaista on jaettu niin, että ainoastaan yksi voi sitä käyttää kerrallaan. (Jaakohuhta 2002, 92 - 93.)

Kun lähetystarpeet kasvavat eli syntyy ruuhkaa, on tarjolla kaksi vaihtoehtoa:

- Eristetään samaa siirtotietä käyttävät asemat pieniin ryhmiin.
- Nostetaan nopeutta, jolloin dataa siirtyy enemmän samassa ajassa.

(Jaakohuhta 2002, 93 - 94.)

Pieniin ryhmiin jaettaessa on ryhmien välillä kuitenkin oltava yhteys, joka avautuu tarvittaessa. Tämä edellyttää yhteyden välille siltausta. Nopeuden nostamiseen on nykyään monta vaihtoehtoa. Ethernetille on määritelty neljä nopeutta: 10, 100, 1000 ja 10000 Mbps. Nopeusvaihtoehtojen lisäksi voidaan siirtyä vuorosuuntaisesta liikenteestä kaksisuuntaiseen liikenteeseen. Lisäksi voidaan ottaa käyttöön lähiverkkokytkin. (Jaakohuhta 2002, 93 - 94.)

4.3.3 Kytkentäinen Ethernet

Lähiverkkokytkimellä voidaan helposti tehostaa hitaaksi käynyttä lähiverkkoa. Vanhaan jaettuun Ethernetiin saadaan lisää kaistaa, eikä koko verkkoa tarvitse uusia. Periaatteessa kytkimen voi sijoittaa hubin tilalle muutoksia tekemättä ja kytkin lähtee toimimaan tehdasasetuksin. Hallinnan ja lisäominaisuuksien asettamiseksi kytkimeen tehdään lisäasetuksia, jotta kytkimen käyttö olisi mahdollisimman tehokasta. (Jaakohuhta 2002, 137.)

Kytkimen idea on tarjota jokaiselle siihen kytketylle koneelle täysi kaista, joka Ethernetissä on 10/100/1000 tai jopa 10000 Mbps. Nopeuden takana on kytkimen sisäinen taustaväylä ja kehyksen reititys. Kytkin toimii moniporttisiltana eli kehys muodostetaan ja kaistasta kilpaillaan lähettävällä portilla jokaisen kehyksen kohdalla uudelleen. (Jaakohuhta 2002, 138 - 139.)

Kytkimeen liitetty kone voi liikennöidä joko kaksi- tai vuorosuuntaisesti. Kaksisuuntaisessa liikenteessä ei tarvita törmäyksentunnistusta. Liikennöinnin aikana vain liikennöivät osapuolet kuulevat toisensa. Kaksisuuntaisuus mahdollistaa samanaikaisen lähetyksen ja vastaanottamisen. Hubit, joissa on useita työasemia,

eivät keskustele kaksisuuntaisesti, koska hubissa liikennöintiin tarvitaan törmäyksentunnistusta. Tällöin työasemat, jotka ovat kytkettynä hubissa, ovat siis jaetussa eivätkä kytkentäisessä Ethernetissä. (Jaakohuhta 2002, 140 - 141.)

4.4 Langattomat lähiverkot

4.4.1 Ethernet 802.11

Ensimmäinen versio IEEE 802.11 -suosituksesta julkaistiin 1997 ja siitä parannettu versio vuonna 1999. Näihin versioihin on saatu laajennuksia: IEEE 802.11a, joka toimii 5 GHz alueella tukien 54 Mbps nopeuksia, sekä IEEE 802.11b, joka toimii 2,4 GHz alueella 11 Mbps nopeudella. IEEE 802.11 -suositus määrittelee toiminnan sellaisessa langattomassa lähiverkossa, jossa kanavanvarauksen päätöksenteko on yksittäisen työaseman tai keskitetyn tukiaseman varassa. (Granlund 2001, 230.)

IEEE 802.11 -suosituksessa määritellään kaksi verkkotopologiaa: vertaisverkko- ja asiakas/palvelin-tyyppinen ratkaisu. Jälkimmäistä voidaan laajentaa niin, että tukiasemat liitetään yhteen runkoverkkoon, jossa on useampi palvelin. Kukin palvelin hoitaa tällöin oman toimialueensa liikenteen. (Granlund 2001, 230.)

Suosituksen mukaisesti rakennettuun langattomaan lähiverkkoon on mahdollista liittyä kolmella eri tavalla. Perusarkkitehtuuri tunnetaan nimellä BSS (Basic Service Set). BSS muodostuu laitejoukosta, jotka osaavat kommunikoida toistensa kanssa. (Granlund 2001, 230.)

Jos laitteiden muodostamaa verkkoa ei kytketä kiinteään verkkoon, verkkoa kutsutaan nimellä IBSS (Independent Basic Service Set). Tyypillisesti IBSS-verkko on lyhytaikainen ratkaisu, esimerkiksi neuvottelu-/koulutustilanne, jolloin osallistujat tuovat omat laitteet mukanaan, ja laitteet ovat langattomasti yhteydessä toisiinsa tilanteen ajan. Kun tilanne päättyy, myös verkko purkautuu. Tämän ominai-

suuden vuoksi IBSS-verkkoa kutsutaan myös nimellä Ad-Hoc-verkko. IBSS-verkossa kaikki laitteet voivat keskustella suoraan toistensa kanssa. (Granlund 2001, 231.)

BSS-verkko muodostuu kiinteästä tukiasemasta ja siihen liittyvistä työasemista. Liikenne kulkee tukiaseman kautta. BSS-verkossa luotettavuus perustuu tukiasemaan; jos tukiasema hajoaa, työasemat voivat muodostaa Ad-Hoc-verkon, mutta menettävät yhteydet kiinteän verkon palveluihin. Tiedonsiirto laitteelta toiselle kulkee tukiaseman kautta, joten kapasiteettia on käytössä kaksinkertainen määrä. (Granlund 2001, 231 - 232.)

BSS-verkkoa voidaan laajentaa ESS-verkoksi (Extended Service Set), jolloin useampi tukiasema on kytketty samaan runkoverkkoon. Runkoverkosta käytetään nimitystä DS (Distribution System). ESS on yleisin tapa muodostaa langattomia lähiverkkoja, joissa verkon kantavuus ei rajoitu vain yhteen kerrokseen tai muutamaan huoneeseen. Runkoverkko sallii myös laitteiden liikkumisen solusta toiseen, ilman että käyttäjä huomaa tukiaseman vaihdosta. (Granlund 2001, 232.)

4.4.2 Langattomat siirtotekniikat

Fyysisellä kerroksella dataa siirretään kahdella eri tavalla: 2,4 GHz tai 5 GHz ISM-alueilla (Industrial Scientific Medical) toimiva radiotaajuus, RF (Radio Frequency) sekä 850 - 950 nm:n alueella infrapuna, IR (Infra Red). Molemmilla tavoilla on omat etunsa. Radioaallot läpäisevät seiniä ja muita fyysisiä esteitä, jolloin tukiaseman ja työaseman ei tarvitse olla näköyhteydessä. Infrapunasiirtoa varten laitteiden täytyy olla näköyhteydessä. Laitteiden lyhyen kantaman vuoksi käyttö on jäänyt vähäiseksi. Tyypillisiä käyttökohteita ovat laitteet, joiden virtalähdekäyttö on rajoitettu, esim. matkapuhelimet (Granlund 2001, 234.)

Radiotiellä datan siirtoon käytetään joko suorasekvenssihajaspektriä DSSS (Direct Sequence Spread Spectrum) tai taajuushyppelyhajaspektriä FHSS (Frequency Hopping Spread Spectrum). Hajaspektritekniikkaa käytettäessä jokainen käyttäjä

levittää lähetteensä koko taajuusalueelle, jolloin kukaan ei saa käyttöönsä koko kaistaa. Lähetteen levitys aiheuttaa myös sen, että data näkyy joillakin alueilla kohinana. Käytännön hyöty levityksestä on se, että useat sovellukset voivat käyttää samaa kaista-aluetta, mutta kukin sovellus käyttäytyy kuin toimisi omalla yksityisellä kaistallaan. Vapaita radiotaajuuksia ovat 2,400 - 2,485 GHz ja 5,725 - 5,825 GHz, mutta maakohtaisia laajennuksia ja rajoituksia on käytössä. (Granlund 2001, 234.)

Langattoman lähiverkon suojaukseen käytetään WEPiä (Wireless Equivalent Privacy). WEP kattaa sekä autentikoinnin että siirrettävän tiedon salaukseen käytettävän RC4-jonosalaajan. (Granlund 2001, 256.)

Kun laite liittyy verkkoon, sille lähetetään haaste hallintasanomassa, joka sen tulee salata omalla WEP-avaimella. Autentikoitava asema salakirjoittaa koko sanoman, ja siitä muodostuu vastaus. Järjestelmä purkaa vastauksen omalla avaimellaan ja päättää, hyväksytäänkö vai hylätäänkö aseman pääsy verkkoon. (Granlund 2001, 256.)

Siirrettävä tieto salataan RC4-jonosalaajalla, jonka kehitti Ron Chivest. Se on symmetrinen salausmenetelmä, jossa salaus ja purku tapahtuvat samalla avaimella. Ongelmana tässä menetelmässä on avaimien vaihto. Yleisesti WEP-avain syötetään koneelle verkkokortin asennuksen yhteydessä, ja salaus jää sitten käyttäjän harteille. Avain voidaan valita neljän avaimen sarjasta tai voidaan käyttää myös työasemakohtaisia avaimia, jolloin yksi avain on ainoastaan tukiaseman ja työaseman tiedossa. (Granlund 2001, 257.)

WEP-salauksen heikkouksien paljastuttua kehitettiin WPA-salaus (Wireless Fidelity Protected Access). WEP-salauksessa havaitut aloitusvektoriongelmat on korjattu ja salausavainta vaihdetaan 10 000 paketin välein automaattisesti. Salauksessa käytetään TKIP-protokollaa (Temporal Key Integer Protocol). Se mahdollistaa jaetun salaisen avaimen suojaamisen. TKIP parantaa langattoman verkon turvallisuutta pakettikohtaisilla salausavaimilla, jotka ovat RC4-menetelmällä salattuja 128-bittisiä avaimia. WPA:n huono puoli on palvelun-estohyökkäyksistä

selviytyminen. Hyökkäyksen havaittuaan WPA sulkee koko verkon minuutiksi, jolloin myös lailliset käyttäjät putoavat verkosta.
(Wikipedia 2005.)

5 TIETOTURVA

5.1 Tietoturvan perusperiaatteet

Tietoturva koostuu kolmesta osa-alueesta: luottamuksellisuudesta, eheydestä ja saatavuudesta. Saatavuus edustaa myös todennusta, ja toisaalta luottamuksellisuus edellyttää todennusta. Jos henkilöllisyyttä ei voida varmistaa, ei turvajärjestelyistä ole hyötyä. Kaikki edellämainitut osa-alueet koskevat tietoa eri muodoissa: tiedostona, tiedonsiirtona tai muistissa olevina bitteinä. Tietoturvan toimivuuden kannalta edellisten osa-alueiden lisäksi edellytetään kolmen muun periaatteen toteutumista. Nämä ovat todentaminen, pääsynvalvonta ja kiistämättömyys (kts. KUVIO 2). (Järvinen 2002, 22.)

TIETOTURVA	
Luottamuksellisuus	Todennus
Eheys	Pääsynvalvonta
Saatavuus	Kiistämättömyys

KUVIO 2.. Tietoturvan kuusi perustavoitetta (Järvinen 2002, 23)

5.1.1 Luottamuksellisuus

Luottamuksellisuus tarkoittaa sitä, ettei kukaan pääse käyttämään sellaista tietoa, joka ei ole hänelle tarkoitettu. Tietoa pääsevät lukemaan ja muokkaamaan vain ne, jotka ovat siihen oikeutettuja. Jotta käyttäjä voidaan tunnistaa, hänet on ensin todennettava, ja jotta tieto säilyisi suojattuna, se on salattava. Kun tieto on riittävän hyvin salattu turvallisella menetelmällä, se ei paljastu, vaikka joku onnistuisi salakuuntelemaan tietoliikennettä tai varastamaan tallennukseen käytetyn koneen. (Järvinen 2002, 22.)

5.1.2 Eheys

Tiedon eheydellä tarkoitetaan sitä, ettei kukaan ulkopuolinen pysty muuttamaan tiedon sisältöä luvatta. Muuttaminen käsittää esimerkiksi tiedostojen poistamisen tai asiattomien muutoksien tekeminen. Virukset rikkovat tiedostojen eheyden niihin tarttuessaan, ja hakkerit murtautuessaan www-sivuille. Eheys voi särkyä myös satunnaisen levy- tai tiedonsiirtovirheen vuoksi. Tiedoston sisäinen eheysvika on hankala ongelma, jos vikaa ei huomata ajoissa ja virheellinen tiedosto tallennetaan kunnossa olevan version päälle. Tällainen ongelma saattaa muodostua saatavuusongelmaksi eli saatavilla ei ole ehjää versiota tiedostosta. (Järvinen 2002, 23.)

Eheyden takaamiseksi käytetään tarkistussummia, lokitiedostoja, tiedonsiirtoprotokollia sekä erilaisia tarkistus- ja virustorjuntaohjelmia. Tietojen salaaminen turvaa yleensä eheyttä, mutta saattaa jopa pahentaa siirto- ja käsittelyvirheitä. (Järvinen 2002, 23.)

Tietojen arkistointivaiheessa eheys on erityisen tärkeässä asemassa. Yrityksen taloustiedot ja turvallisuusjärjestelmälokit on arkistoitava niin, ettei niitä voi myöhemmin muuttaa. Varmuuden vuoksi kannattaa käyttää esimerkiksi CD-R-levyjä, joille voi kirjoittaa vain kerran. (Järvinen 2002, 24.)

5.1.3 Saatavuus

Saatavuus turvaa tietojärjestelmien toimintaa. Verkkoyhteyksien ja -palvelujen täytyy toimia 24 tuntia vuorokaudessa ja seitsemän päivää viikossa. Tavallisessa toimistotyössä riittää usein normaalin työajan puitteissa toimivat järjestelmät, öisin sekä viikonloppuisin varmistetaan tiedostot. (Järvinen 2002, 24.)

Palveluiden saatavuutta voidaan häiritä esimerkiksi palvelunesto- eli DoS -hyökkäyksillä (Denial of Service). Tällaisten hyökkäysten tarkoitus on ainoastaan

estää palvelujen saatavuus, ei murtautuminen (luottamuksellisuus) tai sotkeminen (eheys). (Järvinen 2002, 24.)

Tietojen saatavuuden varmistamiseen on varauduttava varmuuskopioimalla sekä laitteiden toiminnan turvaavilla menetelmillä, esimerkiksi UPS-laitteilla (Uninterruptible Power Supply). Lisäturvaksi laitteet on sijoitettava lukkojen taakse. (Järvinen 2002, 24.)

Yritykselle saattaa tulla yllättäviäkin ongelmia. Kun esimerkiksi tiedosto on tallennettu 15 vuotta sitten vanhalle, jo käytöstä poistuneelle 5,25 tuuman levykkeelle vanhalla sovelluksella, ei sen avaaminen olekaan niin helppoa kuin voisi kuvitella. (Järvinen 2002, 24.)

5.2 Tietoturvan muut osa-alueet

5.2.1 Todentaminen

Luottamuksellisuuden edellytyksenä on todentaminen, eli varmistutaan siitä, että olio on se, mitä pitääkin. Olio voi tässä yhteydessä olla käyttäjä, laite, tiedon alkuperä, verkkopalvelu tai jokin verkosta ladattu ohjelma. (Järvinen 2002, 24 - 25.)

Todentaminen on teknisesti hankalaa, mutta sen enempää ajattelematta, se suoritetaan monta kertaa päivässä. Kun esimerkiksi tuttu puhelinnumero näkyy puhelimen näytöllä sen soidessa, soittajan uskotaan olevan juuri se tuttu, joka tunnetaan. Sähköpostia tarkistettaessa katsotaan lähettäjäosoitetta, ja uskotaan sen olevan oikea. (Järvinen 2002, 25.)

Koska tiedoilla ja biteillä ei ole mitään aistein havaittavaa ominaisuutta, on otettava käyttöön keinotekoiset todennusmenetelmät.

- Käyttäjä todennetaan salasanan avulla, olettaen että salasana on oikean käyttäjän hallussa. Kun todennus on tehty, käyttäjä valtuutetaan tietojen käyttöön.
- Laitteen todennus ihmiselle on hankalaa. Sen sijaan laitteiden välinen todennus on yksinkertaista ja perustuu erilaisiin salausmenetelmiin.
- Verkosta saadun tiedon todennus on vaikeaa. Tiedon alkuperästä ei välttämättä ole tietoa eikä siitä kuka, tiedon on verkkoon laittanut.
- Verkkopalvelut todennetaan sen osoitteen perusteella. Verkkopalveluiden todentamiseen voidaan käyttää SSL-tekniikkaa (Secure Socket Layer).

(Järvinen 2002, 25.)

Todentaminen edellyttää yksilöllisiä ominaisuuksia, joten ihmisten välinen todennus on yleisesti ottaen helppoa. Todennukseen on olemassa seuraavat kolme vaihtoehtoa:

1. yksilölliset ominaisuudet eli lähinnä biometriset tunnisteet (ääni, ulkonäkö, käsiala ja silmän verkkokalvo)
2. jokin hallussa oleva esine, esimerkiksi pankkikortti
3. käyttäjän tiedossa oleva tieto, esimerkiksi salasana tai PIN-koodi (Personal Identification Number).
   (Järvinen 2002, 26 - 27.)

5.2.2 Pääsynvalvonta

Pääsynvalvonnalla huolehditaan siitä, että vain todennetut henkilöt pääsevät järjestelmätietoihin käsiksi. Pääsynvalvontaa suorittavat käyttöjärjestelmät ja sovellukset. (Järvinen 2002, 26.)

Pääsynvalvontaan voidaan liittää myös käytön seuranta (lokitiedostot). Tällöin järjestelmä pitää kirjaa käyttäjistä, jotka ovat kirjautuneet järjestelmään, muokanneet tiedostoja tai käyttäneet ohjelmia. Näistä lokeista voidaan hyötyä tietoturvarikkeitä selvitettäessä. (Järvinen 2002, 26.)

5.2.3 Kiistämättömyys

Erityisesti sähköisen kaupankäynnin tyypilliset ostovaiheet täytyy pystyä todistettavasti näyttämään tapahtuneiksi. Jos asiakas kiistää tilauksen tai kauppias toteaa, ettei ole tilausta vastaanottanut, niin kaupankäynti loppuu lyhyeen. Samaten kauppiaan täytyy voida todistaa tavaran lähteneen varastostaan eteenpäin. (Järvinen 2002, 27 - 28.)

Kiistämättömyys saavutetaan soveltamalla aiemmin mainittuja periaatteita eheydestä ja todennuksesta. Lisäksi edellytetään aikaleimojen, päiväys ja kellonaika, käyttöä tapahtumien varmentamiseksi. (Järvinen 2002, 28.)

5.3 Tietoturva yrityksissä

Tietoturva mielletään yrityksissä helposti ainoastaan tietokoneisiin ja teknisiin asioihin liittyväksi käsitteeksi, jonka tavoitteena on hakkerien ja virusten torjunta sekä varmuuskopiointi. Tietoturvan laajempi merkitys ymmärretään vasta tarkasteltaessa kaikkia siihen liittyviä osa-alueita. Seuraavassa taulukossa (TAULUKKO 3) on valtionhallinnon vuonna 1993 tekemä osa-alueluokittelu. (Järvinen 2002, 112.)

TAULUKKO 3. Tietoturvan osa-alueet

	OSA-ALUE	KÄSITTÄÄ
1	hallinnollinen turvallisuus	organisaation: -tietoturvalinjaukset -johtaminen -toiminnan organisointi -vastuut -tietoturvapolitiikka
2	henkilöturvallisuus	työntekijöiden: -ohjeistus -koulutus -aiheuttamat tahattomat vahingot -tahalliset sabotaasit
3	toimitilaturvallisuus	toimitilojen: -kulunvalvonta -murtosuojaus -lukitukset
4	tietojenkäsittelyn turvallisuus	laitteiden: -käyttö -operointi -toiminnan varmistaminen poikkeustilanteissa
5	tietoliikenteen turvallisuus	tietoliikenteen: -jatkuvuus -siirrettävän tiedon salaaminen ja eheys
6	laitteistoturvallisuus	tietokoneiden ja verkon aktiivilaitteiden toiminnan varmistaminen
7	ohjelmistoturvallisuus	käytössä olevien ohjelmistojen suojaaminen, lisenssien hallinta sekä rekisteröinti
8	käyttötoimintojen turvallisuus	tietokoneiden ja verkon aktiivilaitteiden päivittäinen ylläpito, käyttö, huolto ja valvonta
9	tietoaineistoturvallisuus	tietoaineiston käsittely niin, ettei luottamukselliset tiedot vuoda ulkopuolisille
10	yksityisyyden suoja	työntekijöiden ja yrityksen toimintaan liittyvien henkilöiden tietojen suojaaminen

5.4 Palomuurit

5.4.1 Käyttötarkoitukset

Palomuuri toimii ns. rajavartijana yrityksen sisäisen ja ulkoisen tietoliikenteen välissä. Tehtävä on hankala, sillä rajaa ei voida verkon toiminnallisuuden vuoksi sulkea kokonaan. Nykyajan palomuurin täytyy kyetä toimimaan kaikilla protokollakerroksilla yhtä aikaa. Tämä vaatii palomuurilta suoritustehoa protokollatietojen keräämiseen ja liikenteen suodatukseen. (Kaario 2002, 305.)

Nykyään palomuureja käytetään paljon myös henkilökohtaisissa koneissa. Varsinkin nykyajan etätyömahdollisuudet edellyttävät suojatun ja salatun reitin muodostamista Internetin läpi työpaikalle. (Kaario 2002, 305.)

5.4.2 Palomuurityypit

Palomuureja on olemassa sekä rauta- että ohjelmistotasolla. Rautatason palomuureja on kolmea eri tyyppiä: pakettisuodatuspalomuuri, piiritason yhdyskäytävä ja sovellustason yhdyskäytävä. Lisäksi uusimmissa palomuureissa on ns. tilallinen suodatusominaisuus, joka mahdollistaa yksinkertaisten suodatussääntöjen avulla erilaisten tilatietojen tallentamisen. (Kaario 2002, 305 - 307.)

Pakettisuodatuspalomuuri käyttää liikenteen suodatukseen IP-paketista saatavaa tietoa. Varsinkin reitittimiä käytettäessä pakettisuodatus on yleistä, koska erilaisten pääsylistojen konfigurointi on helppoa lähde- ja kohdeosoitteen perusteella. Pakettisuodatus ei ole täydellinen tietoturvaratkaisu, mutta täydentää muita suotimia. (Kaario 2002, 305.)

Piiritason yhdyskäytävä suodattaa liikennettä porttinumeron ja määritellyn konfiguraation perusteella. Porttinumeroiden lisäksi piiritason yhdyskäytävä voi toimia

yhteistyössä pakettisuodattimen kanssa ja sallia liikenteen johonkin tiettyyn porttiin tietystä osoitteesta. Yhdyskäytävä voi nimensä mukaisesti toimia ns. proxyna niin, että vain yhdyskäytävän osoite välitetään julkiseen verkkoon. Tällöin on usein käytössä NAT-osoitemuunnos (Network Address Translation), joka on yksi tietoturvaa parantava seikka. Mahdollinen hakkeri näkee ainoastaan yhdyskäytävän, ei sen takana olevia koneita. (Kaario 2002, 306.)

Sovellustasolla toteutettu palomuuri vaatii enemmän suorituskykyä kuin edellä mainitut palomuurit. Se käyttää suodatukseen kaikkien kerroksien tietoa, aina sovelluskerrokselle saakka. Tietoturvan kannalta tämä on tehokasta, mutta teknisesti sen toteuttaminen on vaikeaa. Ongelmana on mm. se, että tuettavien sovellusprotokollien määrä on rajallinen ja tiedon kaivaminen datapaketista on raskasta. Myös sovellusyhdyskäytävä, kuten piiritason yhdyskäytäväkin, voi toimia proxyna. (Kaario 2002, 306 - 307.)

Edellä mainittujen palomuurien toimintaan voidaan liittää tilallinen suodatus. Tällöin suodatuksen lisäksi tallennetaan tilatietoja yhteyden osapuolten välisestä liikenteestä. Lisäksi se mahdollistaa esimerkiksi kuormituksen tasauksen ja liikennetietojen keruun. Jälkimmäistä voidaan käyttää esimerkiksi laskutuksen toteuttamiseen. Tilallinen suodatus on erittäin tehokas tapa, ja erilaisia suodatusmahdollisuuksia on lähes rajattomasti. Toisaalta suodatuksen konfigurointimäärittelyt vaativat runsaasti resursseja ja suunnittelua. (Kaario 2002, 307.)

Useissa palomuureissa on mahdollisuus määritellä käyttöön ns. demilitarisoitu alue eli DMZ-alue (Demilitarized Zone). Tälle alueelle on mahdollista perustaa esimerkiksi Ekstranet-alue, joka on yrityksen asiakkaille tarkoitettu julkinen alue. DMZ-alueen palvelut käyttävät usein hyväkseen yrityksen suljetulla Intranet-alueella toimivia palvelimia. DMZ-toteutuksien haasteena ovat kriittiset yhteydet suojattuun verkkoon ja palveluiden käytettävyyden takaaminen. (Kaario 2002, 308.)

Ohjelmistopalomuureista ZoneAlarm on hyvin suosittu, koska se on ilmainen kotikäytössä. On olemassa kaupallinen versiokin, joka sisältää monipuolisempia toimintoja. Ohjelma valvoo asennuksen jälkeen sekä lähtevää että tulevaa

liikennettä. Jos jokin ohjelma yrittää ottaa yhteyttä Internetiin tai verkosta joku yrittää tulla koneelle, ohjelma ilmoittaa tästä käyttäjälle. Tällainen toiminta saattaa paljastaa mahdollisia spyware-ohjelmia koneelta, jolloin ne voidaan poistaa. Juuri tämän toiminnon vuoksi myös ohjelmistopalomuuri olisi hyvä asentaa yrityksen koneille rautapalomuurin lisäksi. Tosin ohjelmistopalomuuri on haavoittuvainen, koska jokin toinen ohjelma voi kytkeä sen pois päältä tai kiertää suojauksen. (Järvinen 2002, 321 - 322.)

Windows XP:ssä on sisäänrakennettu yksinkertainen palomuuri. Se täyttää perustarpeet, koska sillä voidaan rajoittaa liikennettä porttikohtaisesti. Sen heikkoudeksi voidaan lukea se, että lähtevää liikennettä ei rajoiteta mitenkään. (Järvinen 2002, 323.)

6 YRITYKSEN TIETOHALLINNON NYKYTILANNE

6.1 Henkilökunta ja koulutus

Tällä hetkellä yrityksessä on kolme työntekijää. Koulutustaustaltaan yksi on vuonna 2001 tietotekniikan valmistunut AMK-insinööri, hänen vastuullaan on projektien läpivienti ja ohjelmointitehtävät. Toinen työntekijöistä on peruskoulutukseltaan tietotekniikkamekaanikko, joka opiskelee AMK-insinööriksi työn ohessa. Hänen vastuullaan on teknisten varaosakirjojen tekeminen. Toimitusjohtaja on koulutukseltaan puualan insinööri.

Koulutusta ja lisäkoulutusta haetaan tarvittaessa lähinnä kirjallisuudesta ja Internetistä, mutta myös ulkopuolisilla kursseilla on mahdollista käydä. Henkilökunnan palkkaamisen hoitaa toimitusjohtaja työhakemusten ja haastattelujen perusteella.

6.2 Yrityksen verkko ja sen toiminta

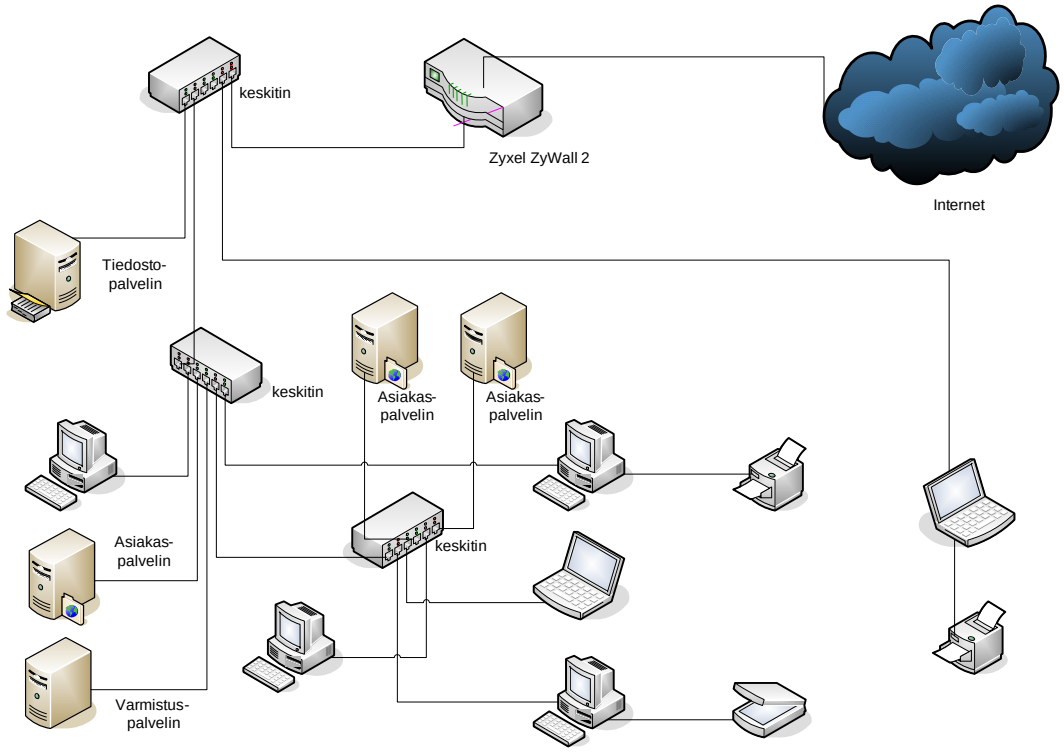
Yrityksen yhteydet ulkomaailmaan kulkevat PHP:n verkossa. Palveluntarjoajana on Utfors. SDSL-linjan nopeus on 2 Mbps, sekä lähtevä että tuleva liikenne kulkee samalla nopeudella. Utfors vastaa yhteyksien toiminnasta yrityksen sisätiloihin palomuurille asti. Siitä eteenpäin verkko on yrityksen hallinnassa ja ylläpitämä.

Sisäinen verkko on rakennettu keskittimillä. Kaapelointina on käytetty kategorian 5 parikaapelia, jonka nopeus on 100 Mbps (kts. TAULUKKO 1). Verkkolaitteiden hajoamisen varalle ei varsinaisia varalaitteita ole, mutta tarvittaessa sellaiset saadaan nopeasti hankittua. Verkon sisäisestä toiminnasta vastaa oman toimensa ohella tekninen tuki.

Verkkokorttien integrointi koneiden emolevylle on hyvin yleistä nykypäivänä. Vikatilanteessa kuitenkin koneen koko emolevy täytyy vaihtaa, mistä aiheutuu sekä ylimääräisiä kustannuksia että arvokasta työaikaa kuluu.

Verkko on toteutettu työryhmäverkkona, joka tällaisessa pienessä yrityksessä on varmasti paras vaihtoehto. Jokainen työntekijä käyttää omaa konetta, ja palvelimille on määritelty samat käyttäjät. Yritys on saanut Utforsilta käyttöönsä IP-avaruuden, josta IP-osoitteet on määritelty jokaiselle koneelle eli käytössä on kiinteät IP-osoitteet. Tämänhetkisestä verkosta ei ole olemassa dokumentointia.

Tämän työn yhtenä aihealueena on ajantasalla oleva dokumentointi. Olemassa oleva verkko dokumentoitiin työn alussa. Seuraavassa kuviossa (KUVIO 3) onkin esitetty yrityksen tietoliikenneverkon tilanne ennen tietohallintostrategiaa.



KUVIO 3. Yrityksen verkko ennen tietohallintostrategiaa

6.2.1 Nykyiset työasemat, palvelimet ja ohjelmistot

Yrityksessä on tällä hetkellä 6 työasemaa. Koneiden huolto suoritetaan vanhojen koneiden osalta itse, uudet koneet menevät takuuajan puitteissa koneen myyneen liikkeen huollettavaksi.

Palvelimia yrityksessä on viisi. Tiedostopalvelin, varmistuspalvelin sekä kolme asiakaskäytössä olevaa palvelinta. Viimeksi mainitut kolme asiakaspalvelinta ovat niin sanotussa serverihotellissa, eli yritys huolehtii niiden ylläpidosta ja ohjelmapäivityksistä. Tiedostopalvelin on nimensä mukaisessa käytössä yrityksen tiedostojen jakelukäytössä. Varmistuspalvelin varmistaa tiedostopalvelimen, sekä asiakkaiden palvelimet ohjelmallisesti ajastettuna.

Koneita ja laitteita hankittaessa tarjoukset pyydetään vähintään kahdelta toimittajalta. Hankinnat suoritetaan aina kokonaistaloudellisesti edullisella tavalla. Hankittavat koneet ja laitteet ovat uusia merkkikoneita, ja niissä on käyttöjärjestelmä valmiiksi asennettuna. Hankintapäätöksiä tehdään tarpeen mukaan ja hankinnoista vastaa aina toimitusjohtaja.

Tulostimia on yrityksen käytössä kolme. Niistä kaksi on mustavalkolasereita ja yksi on monitoimilaite (KUVIO 4), jossa on tulostin, kopiokone ja skanneri. Väri/värilaser-tulostimelle ei ole toistaiseksi ollut tarvetta.

KUVIO 4. Monitoimilaite

Yrityksellä on käytössä erilaisia ohjelmistoja. Käyttöjärjestelminä on työasemissa käytössä Windows XP Pro ja palvelimissa on käytössä Windows 2000/2003 palvelinversiot. Toimisto-ohjelmistona käytetään Microsoft Officen versioita 2000 ja 2003. Lisäksi asiakaspalvelimilla on käytössä tietokantaohjelmia, esim. Oracle. Ohjelmistojen asennuksen suorittaa jokainen käyttäjä itse. Pyrkimyksenä kuitenkin on, että kaikki asentavat ohjelmat samalla tavalla.

Ohjelmistohankintoja suoritetaan määrällisesti vähän. Pääasiassa hankitaan käyttöjärjestelmiä tai joitakin yksittäisiä ohjelmistoja. Ohjelmistohankinnoista vastaa toimitusjohtaja.

Virustorjuntaohjelmistona on tällä hetkellä käytössä F-Secure. Ohjelmiston toimintaan on oltu pääosin tyytyväisiä. Virustietokannat päivittyvät joissakin koneissa automaattisesti, joissakin käsityönä. Ohjelmisto on asennettu jokaiseen työasemaan ja palvelimeen.

Olemassa olevista koneista, laitteista ja ohjelmistoista ei ole olemassa erillistä rekisteriä, josta kävisi ilmi esimerkiksi niiden hankintapäivä ja käyttötarkoitus. Rekisteri tullaan kokoamaan tämän työn jälkeen. Rekisterin kokoamisessa käytetään apuna Alchemy Network Inventory -ohjelmaa, jolla lähiverkon kaikkien koneiden sisältämät ohjelmistot ja komponentit saadaan selville helposti.

6.2.2 Yleisimmät vikatilanteet

Vikatilanteita esiintyy hyvin harvoin, mutta silloin ne ovatkin yleensä vakavampia, lähinnä kiintolevyn tai virtalähteen rikkoontumisia. Tällaiset viat ovat odotettavissa olevia vikoja, eikä niitä pysty millään tavalla ennustamaan. Vikatilanteen sattuessa tutkitaan, mitä on tapahtunut, ja sovitaan toimenpiteistä tilanteen mukaan.

Ohjelmistovikoja on myös vaikea ennustaa. Jos jokin ohjelma sekoaa, siihen auttaa yleensä ohjelman uudelleenasennus tai päivitys. Itseohjelmoitujen ohjelmien seotessa on yleensä kyse ohjelmointivirheestä. Niitä on helppo korjailla kun

tiedetään mitä pitää korjata. Valmisohjelmien ohjelmointivirheitä ei voi korjailla itse.

6.2.3 Tietoturva yrityksessä

Yrityksen tietoturva on tällä hetkellä hoidettu F-Securen virustorjuntaohjelmistolla ja Zyxelin valmistamalla rautapalomuurilla. Lisäksi joissakin Windows XP -työasemissa on käytössä Windowsin oma sisäinen palomuuri. Zyxelin palomuurissa (KUVIO 5) on neljä ethernet-porttia, jotka voidaan konfiguroida joko LAN- tai DMZ-portiksi. Lisäksi siinä on mahdollisuus luoda kymmenen VPN-tunnelia.

KUVIO 5. Zyxelin palomuuri.ZyWall 5 (Zyxel 2005.)

Virustorjuntaohjelmiston päivitys on tällä hetkellä jokaisen työntekijän omalla vastuulla. Ainoastaan joissakin koneissa on automaattinen päivitystoiminta käytössä.

Zyxelin palomuuri on konfiguroitu niin, että sisäverkko ei näy ulospäin. Koneiden liikennöinti tapahtuu sen omalla kiinteällä IP-osoitteella, mutta palomuurissa on estetty osoitteiden pingaus ulkoapäin. Myös palomuurin IP-osoitteet on piilotettu ulkopuolisilta. Näillä toimilla mahdolliset hakkerointiyritykset on pyritty eliminoimaan. Erillistä DMZ-aluetta ei ole määritelty palvelimille.

Jokainen käyttäjä kirjautuu koneelleen omalla tunnuksellaan ja salasanalla, jotka käyttäjä on itse määritellyt. Jokainen käyttäjä on koneellaan pääkäyttäjä, lisäksi koneille on määritelty erillinen pääkäyttäjä, jonka tunnus ja salasana on jokaisen tiedossa. Palvelimille kirjaudutaan pääkäyttäjänä, jonka tunnus ja salasana on

myös jokaisen tiedossa. Jos käyttäjä unohtaa salasanansa, hän voi kirjautua pääkäyttäjänä koneelle ja määrittää itselleen uuden salasanan.

Tiedostopalvelin varmistetaan ohjelmallisesti varmistuspalvelimelle. Näin varsinaisen tiedostopalvelimen rikkoutuessa voidaan ottaa käyttöön nopeasti varapalvelin. Samalla tavalla varmistetaan myös asiakaskäytössä olevien palvelimien tiedot.

Varsinaisia hätäsuunnitelmia onnettomuuksien tai keskeisten henkilöiden poistumisen varalle ei ole olemassa. Mitään erillisiä vaitiolo- ja salassapitosopimuksia ei myöskään ole tehty. Pääkäyttäjätason salasanat ovat tallessa. Tulipalon varalta ei ole laitetoimittajien kanssa erillisiä sopimuksia varalaitteista. Vakuutukset ovat kuitenkin kunnossa, joten vahingon sattuessa aineelliset vahingot saadaan katettua, mutta menetettyjä tietoja ei voi korvata.

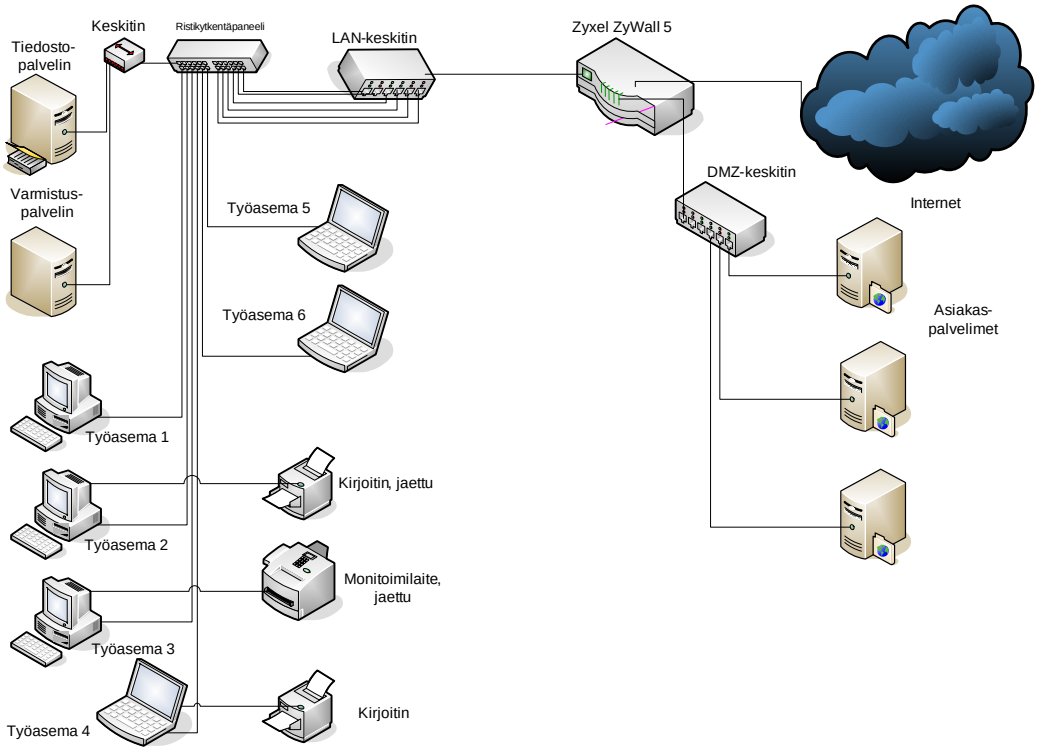
7 TIETOHALLINTOSTRATEGIA 2006 - 2010

7.1 Dokumentointi

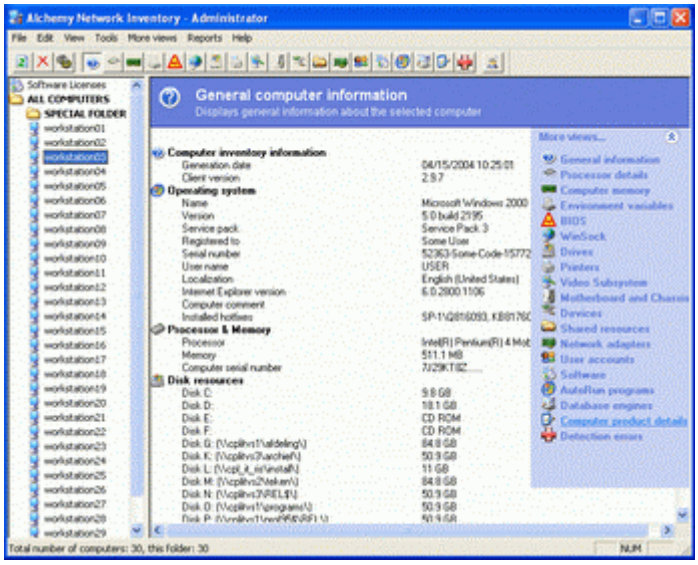
Kaiken kattava dokumentointi on tärkeä osa tietohallintoa. Sen avulla voidaan selvittää palvelimille vaihdetut salasanat sekä seurata tietohallinnon toimintaa. Dokumentointi ei saa jäädä vain yhden henkilön varaan, vaan jokainen työntekijä on vastuussa siitä omalta osaltaan. On kuitenkin hyvä olla olemassa yksi henkilö, joka on päävastuussa dokumentoinnista ja tietohallinnosta.

Ajan tasalla oleva laiterekisteri helpottaa työskentelyä vikatilanteissa. Tässä laiterekisterissä tulee olla koneiden ja laitteiden tekniset tiedot ja niiden sisältämät ohjelmistot. Myös verkosta on hyvä olla ajan tasalla oleva verkkokuva. Laiterekisteriä ja verkkokuvaa täytyy myös ylläpitää, jotta vikatilanteessa voidaan turvautua uusimpaan tietoon.

Seuraavassa kuviossa (KUVIO 6) on esitetty tietohallintostrategian aikana tehdyt laitteisto- ja konemuutokset: rautapalomuuri vaihdettiin uudempaan ja järeämpään malliin, asiakaspalvelimet siirrettiin DMZ-alueelle ja sisäverkossa otettiin käyttöön DHCP-palvelun tarjoamat yksityiset osoitteet. Laiterekisterin kokoaminen tehdään tietohallintostrategian valmistuttua. Siihen käytetään Alchemy Network Inventory -ohjelmaa (kts. KUVIO 7), jolla saadaan kerättyä lähiverkon koneilta niiden kokoonpanotiedot ja niiden sisältämät ohjelmistot XML-muotoiseen (eXtensible Markup Language) tiedostoon.



KUVIO 6. Ajan tasalla oleva verkkokuva



KUVIO 7. Ruutukaappaus Alchemy Network Inventory -ohjelmasta (Alchemy Lab 2005.)

Laite-/ohjelmistorekisteriin on hyvä kirjata myös laitteistovaatimukset, jolloin selviää, millaisia ohjelmistoja laitteilla voi suorittaa. Myös laitteiden laajennettavuus voidaan kirjata tulevaisuutta silmälläpitäen. Laajennettavuudella tarkoitetaan esimerkiksi sitä, voidaanko keskusmuistia lisätä tai vaihtaa hitaamman prosessorin tilalle nopeampi.

Erilaisten ohjelmistojen asennuksesta voitaisiin kehittää dokumentaatio. Ohjelmiston asennuksen yhteydessä esimerkiksi otettaisiin kuvaruutukaappauksia ja yleiset asetukset kirjattaisiin muistiin. Tällaisen dokumentaation avulla lähes kuka tahansa selvityisi ohjelman asennuksesta, vaikka ei olisi koskaan nähnytkään kyseistä ohjelmaa. Dokumentaatiosta on hyötyä varsinkin silloin, kun joku jää eläkkeelle tai siirtyy toisen yrityksen palvelukseen.

7.2 Tietoturvan kehittäminen

Tietoturvan kehittämiseen nykyajan verkoissa tulee suhtautua vakavasti. Tällä hetkellä tietoturva-asiat on hoidettu yrityksessä hyvin. Tietoturvan kehittämistä varten tehtiin tietohallintostrategian aikana tietoturvasuunnitelma, joka on tämän työn liitteenä (LIITE 1).

Yksi tärkeä kehityksen kohde on toipumissuunnitelma, esimerkiksi tulipalon varalle se on hyvä olla olemassa. Suunnitelman avulla voitaisiin kriisin sattuessa mahdollistaa nopea toiminnan jatkuminen. Suunnitelma on hyvä testata käytännössä, jolloin saadaan kuva toiminnasta kriisin aikana. Tällaisen suunnitelman tekeminen on iso urakka, mutta helpottaa oikeassa kriisitilanteessa työskentelyä. Toipumissuunnitelma tehdään sen laajuuden vuoksi vasta tämän työn valmistuttua.

Käyttäjätunnusten ja salasanojen muuttaminen on osa tehokasta tietoturvaa. Vähintäänkin salasana tulee vaihtaa määrätyin väliajoin. Myös palvelimilla pääkäyttäjän salasana tulee olla joka koneella erilainen. Salasanalle tulee määrittää minimipituus, ja sen täytyy sisältää sekä pieniä että isoja kirjaimia ja lisäksi numeroita. Mitä pidempi salasana, sen turvallisempi se on.

Virustorjunnan osalta otetaan joka koneella käyttöön uusi versio F-Securen virustorjuntaohjelmistosta ja asennetaan automaattinen päivitystoiminta käyttöön sen vuoksi, ettei käyttäjä välttämättä joka päivä muista päivittää viruskuvauksia.

Palomuurin sääntöjä muutetaan siten, että liikennöidään yhdellä julkisella osoitteella ulospäin ja sisäverkossa otetaan käyttöön yksityiset osoitteet (KUVIO 8) palomuurin jakamalta DHCP-alueelta. Palvelimet määritellään erilliselle DMZ-alueelle, sisäverkon ulkopuolelle.

KUVIO 8. Yksityisten osoitteiden määrittely

7.3 Tietoliikenneverkon kehittäminen

Työryhmäverkosta ei tässä vaiheessa vielä ole tarkoitus siirtyä toimialueverkkoon. Näin pienessä yrityksessä työryhmäverkko on helpompi ylläpitää. Toimialueverkkoon saatetaan siirtyä tulevaisuudessa, kun asiakaspalvelimien määrä lisääntyy.

Nykyisten verkkolaitteiden vanhetessa uudistetaan niitä pikkuhiljaa uudempaan tekniikkaan. Nykyisin käytössä olevat keskittimet vaihdetaan nopeampiin lähiverkkokytkimiin, jolloin saadaan lähiverkon koko kapasiteetti hyötykäyttöön ja samalla nopeutettua tiedonsiirtoa koneiden välillä.

Palvelimien lisääntyessä otettiin käyttöön KVM-jakaja (Keyboard-Video-Mouse) (KUVIO 9), jolla saadaan monelle koneelle käyttöön yksi näppäimistö, hiiri ja näyttö. Tällä ratkaisulla saatiin lisää pöytätilaa palvelinhuoneeseen, kun luovuttiin ylimääräisistä näytöistä, hiiristä ja näppäimistöistä.

KUVIO 9. Yrityksen käytössä oleva KVM-jakaja

Langattoman verkon käyttömahdollisuudet yrityksen sisäisessä käytössä ovat jo tällä hetkellä hyvät, esimerkiksi satunnaiset yrityksessä vierailevat asiakkaat voisivat hyötyä langattomasta verkosta. Langatonta verkkoa konfiguroitaessa otetaan huomioon tietoturvaseikat eli piilotetaan tukiaseman lähettämä tukiasematunnus SSID (Service Set Identification) ja otetaan käyttöön WPA-salausmenetelmä. Tukiasema (KUVIO 10) on jo olemassa, mutta se otetaan käyttöön vasta myöhemmässä vaiheessa.

KUVIO 10. Langaton tukiasema

Langattoman lähiverkon ohella käytöön voisi ottaa tulevaisuudessa WLAN-VOIP- puhelimet yrityksen sisäverkkoon. Sisäverkon ulkopuolella puhelimet toimivat tavallisena matkapuhelimena. Näin voitaisiin korvata normaalit, nykyisin käytössä olevat lankapuhelimet.

Seuraavassa taulukossa on vielä esitetty yhteenveto tietohallintostrategiassa määritellyistä tehtävistä. Samaan taulukkoon on pyritty nimeämään vastuuhenkilö kyseiseen tehtävään.

TAULUKKO 4. Tietohallintostrategian keskeiset tehtävät

Toimenpide	Kuvaus	Vastuuhenkilö(t)
Dokumentointi	Tehdään laiterekisteri ja huolehditaan sen ylläpidosta, piirretään verkosta kuva Dokumentoidaan ohjelmistoasennukset	Tekninen tuki
Toipumissuunnitelma	Kehitetään suunnitelma, jonka avulla toiminta jatkuu myös kriisitilanteessa	Kaikki yhdessä
Salasanat ja käyttäjätunnukset	Vaihdetaan palvelimille, suositellaan myös käyttäjille vaihtoa	Tekninen tuki

(jatkuu)

TAULUKKO 4 (jatkuu)

Virustorjunnan päivitys	Asennetaan automaattinen päivitystoiminta joka koneelle	Tekninen tuki
Palomuurin konfigurointi	Määritellään palomuurisäännöt	Tekninen tuki
Tietoliikenneverkon kehittäminen	Kehitetään tietoverkkoa tarpeen mukaan	Kaikki yhdessä

8 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tietohallintostrategian luomisen aikana dokumentoitiin entinen ja uudistettu verkko (kts KUVIOT 3 ja 6). Virustorjunta päivitettiin uudempaan versioon ja samalla asennettiin automaattinen päivitystoiminta joka koneelle. Palomuurin osalta muutoksia tehtiin itse laitteistoon. Koko laite vaihdettiin järeämpään ja samalla sisäverkossa otettiin yksityiset osoitteet käyttöön. Palvelimet määriteltiin erilliselle DMZ-alueelle. Palvelimille vaihdettiin myös salasanat, nyt jokaisella on omansa.

Tietohallinnon tulevaisuutta suunnitellaan roadmap-tutkimuksen avulla. Siinä kartoitetaan nykytilanne sekä mahdolliset muutokset vuoteen 2014 asti. Tapahtumien ennustaminen näin pitkällä aikavälillä on vaikeaa, joten taulukko ei välttämättä ole todenmukainen. Tarkoituksena onkin hahmottaa tulevaisuutta ja sitä, mitä se saattaa tuoda tullessaan.

TAULUKKO 5. Yrityksen tietohallinnon roadmap

YRITYKSEN TIETOHALLINNON ROADMAP		
	2006-2010	2010-2014
Sisäinen verkko	Toteutus cat5-kaapelilla ja keskittimillä Työryhmäverkko	Keskittimet korvataan kytkimillä? Langaton sisäverkko käytössä? Toimialueverkko käyttöön?
Työasemat	Uudistetaan vanhimpia	Uudistetaan vanhoja edelleen
Verkko	Nykyisin 100Mbps	Nopeus 1Gbps?
Tietoturva	Toipumissuunnitelma, virustorjunnan ja palomuurin ylläpito	Mobiililaitteiden yleistyminen? Keskitetty hallinta virustorjuntaan
Langaton verkko	Otetaan langaton verkko käyttöön	Saattaa korvata kiinteän sisäverkon?
WLAN-puhelimet	Tutkitaan tilannetta	Otetaan mahdollisesti käyttöön?

Tietohallintostrategian luominen onnistui kohtuullisen helposti. Tilannetta kuitenkin vaikeutti työn lähtötilanne eli dokumentoinnin puutteellisuus. Tästä oli kylläkin hyötyä siinä mielessä, että saatiin mahdollisuus suunnitella ja toteuttaa kaikki

alusta asti itse. Yrityksen tietohallinnon nykytilanne kartoitettiin oman työn ohella melko perusteellisesti.

Varsinaisen tietohallintostrategian luomisessa vaikeinta oli rajata tutkimukseen sisältyvät asiat ja käsitteet. Tässä työssä pyrittiinkin sitten ottamaan käsittelyyn ne tärkeimmät, joiden kehittämisen avulla todella saadaan tuloksia aikaan. Käytössä olevaan verkkoon muutoksien tekeminen toiminnan häiriintymättä on vaikeaa, mutta suuremmilta ongelmilta säästyttiin. Esimerkiksi palomuuria konfiguroitaessa yrityksellä oli toinen palomuuri käytössä ja sen tilalle vaihdettiin uudempi, johon säädöt oli jo valmiiksi tehty.

Työn edetessä ajantasalla olevan dokumentaation puute tuli korjattua, ja nyt onkin tarkoitus jatkaa dokumentointiprojektia ohjelmistoasennuksista ja laitteiden säädöistä. Tätäkin työtä tehdessä olemassaolevat dokumentaatiot olisivat helpottaneet valtavasti.

Tulevaisuudessa laiterekisteriä ja verkkokuvaa pidetään yllä aina muutoksien tullessa. Virustorjunnan päivityksiä tarkastellaan tarpeen mukaan ja tarvittaessa otetaan käyttöön keskitetty hallinta. Myös tietoliikenneverkkoa kehitetään ja uudistetaan. Työryhmäverkosta saatetaan jossakin vaiheessa luopua sen vaikeahkon ylläpidon vuoksi. Dokumentaatiota ohjelmistoasennuksista tehdään tarpeen mukaan ja aikaresurssien puitteissa. WLAN-verkko otetaan käyttöön heti kun siihen on aikaa paneutua. WLAN-VOIP-ratkaisut ovat tällä hetkellä suunnittelu-asteella, ehkäpä tulevaisuudessa ne ovat jo käytössä.

LÄHTEET

Alchemy Lab. 2005 [online]. Alchemy Network Tools. Alchemy Lab. [viitattu 16.11.2005] Saatavissa: http://www.alchemy-lab.com/products/atn/shot1.gif

Bäckman, R. & Lemmetyinen, A. 1992. Strategia tietohallintoon. Koteva Oy, Turku.

Granlund, K. 2001. Langaton tiedonsiirto. Docendo Finland. WS Bookwell, Porvoo.

Jaakohuhta, H. 2002. Lähiverkot – Ethernet. 3., uudistettu painos. IT Press. Edita Prima Oy, Helsinki.

Järvinen, P. 2002. Tietoturva & yksityisyys. Docendo Finland Oy. WS Bookwell, Porvoo.

Kaario, K. 2002. TCP/IP-verkot. Docendo Finland Oy. WS Bookwell, Porvoo.

Oulun kauppaoppilaitos. 2005. Johdanto verkkotekniikkaan [verkkodokumentti]. Oulun kauppaoppilaitos, [viitattu 31.8.2005]. Saatavissa: http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kaytto_ja_kehittaminen/lahiverkko_internet/lanjaint/johdanto_verkkotekniikkaan/jvt.htm

Puska, M. 2000. Lähiverkkojen tekniikka; pro training. Suomen ATK-kustannus, Helsinki.

Ruohonen, M. J. & Salmela, H. 2003. Yrityksen tietohallinto. 2. painos. Edita Prima Oy, Helsinki.

Wikipedia. 2005 [online]. Vapaa tietosanakirja.[viitattu 31.8.2005] Wikipedia. Saatavissa: http://fi.wikipedia.org/wiki/WPA

Zyxel. 2005 [online]. {viitattu 16.11.2005]. Saatavissa:

http://www.zyxel.fi/?kuvaus=1&deptID=11183&productID=45

LIITTEET

LIITE 1

Yrityksen tietoturvasuunnitelma

LIITE 2.

Oulun kauppaoppilaitos, Johdanto verkkotekniikkaan

LIITE 3.

Wikipedia - vapaa tietosanakirja, WPA-käsite

LIITE 1.

Yrityksen tietoturvasuunnitelma

Henkilöturvallisuus

Ohjeistetaan työntekijöitä vaihtamaan koneella käytettävää salasanaa kolmen kuukauden välein. Salasanat pidetään tallessa eikä niitä luovuteta ulkopuolisille. Palvelimien salasanat vaihdettava puolen vuoden välein.

Salasanoille määritetään minimipituus 6 merkkiä, lisäksi sen täytyy sisältää isoja ja pieniä kirjaimia sekä numeroita.

Toimitilaturvallisuus

Asiakaspalvelimet sijoitetaan erilliseen lukittuun laitetilaan. Huolehditaan ovien lukkiutumisesta kun lähdetään työpaikalta.

Tietojenkäsittelyn turvallisuus

Asiakaspalvelimilla säilytetään ainoastaan asiakkaan materiaalia, ei muuta ylimääräistä. Ohjelmistot karsitaan minimiin ja huolehditaan olemassaolevien ohjelmien ylläpidosta.

Tietoliikenteen turvallisuus

Pyritään turvaamaan tietoliikenteen jatkuvuus. Jos Kaivuri-Kalle kaivaa valokuidun poikki, niin siihen tuskin on apukeinoja.

Laitteistoturvallisuus

Asiakaspalvelimien saatavuus varmistetaan katkeamattomalla virransyötöllä.

LIITE 1. (jatkuu)

Ohjelmistoturvallisuus

Käytetään ainoastaan luvallisia ja lisensoituja, yritykselle rekisteröityjä ohjelmistoja.

Kerätään ohjelmistolisenssit yhteen taulukkoon ja säilytetään se turvallisessa paikassa.

Ohjelmistojen asennuslevyistä tehdään varmuuskopiot ja säilytetään ne turvallisessa paikassa.

Käyttötoimintojen turvallisuus

Päivittäin tarkistetaan, että palvelimet ovat päällä eikä niissä ole vikaa.

Viikottain tarkistetaan mahdolliset ohjelmistopäivitykset ja niiden tarpeellisuus.

Tietoaineistoturvallisuus

Säilytetään ja käsitellään tietoaineistoa niin, että ulkopuoliset eivät pääse siihin käsiksi.

LIITE 2.

Oulun kauppaoppilaitos - Johdanto verkkotekniikkaan

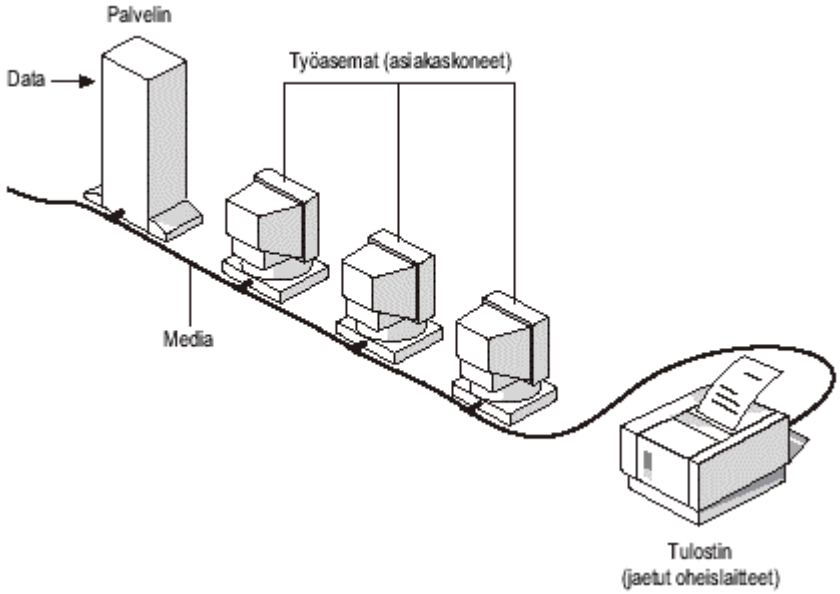
Se, onko tietokoneverkko palvelinperusteinen vaiko vertaisverkko, riippuu verkon tavasta jakaa informaatiota. Seuraavassa hyppäämme käsittelemään verkon perus-komponentteja niiden tehtävien pohjalta. Samalla voimme havainnollistaa verkko-tyyppien peruseroja.

Kun etsimme yleiskuvaa verkon rakenteesta, niin törmäämme väistämättä seuraa-viin verkon komponentteihin:

Palvelimet	Tietokoneita, jotka tarjoavat jaettavia resursseja verkon käyttäjille.
Asiakkaat	Tietokoneet, jotka käyttävät palvelimen tarjoamia resursseja.
Media eli siirtotie	Se tapa, jolla tietokoneet on kytketty toisiinsa.
Jaettava tieto	Tiedostot, joita palvelin tarjoaa verkossa.
Resurssit	Tiedostot, tulostimet tai muut asiat, joita verkossa käytetään.

Kun em. laitteet sijoitetaan verkkoon, verkko saattaisi näyttää seuraavalta:

LIITE 2 (jatkuu)



Kuva 7. Verkon komponentteja.

Se, mitä verkkotyyppiä pitäisi milloinkin käyttää, riippuu monista tekijöistä kuten

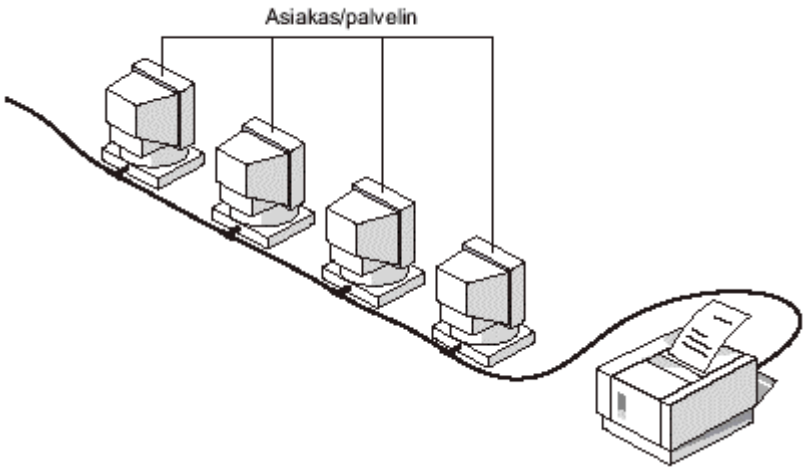
- organisaation koosta
- halutusta tietoturvataosta
- yrityksen toimialasta
- toiminnan laajuudesta
- verkon käyttäjien tarpeista
- käytettävästä rahamäärästä

Palvelinpohjaiset ratkaisut ovat nykyään suuremmissa organisaatioissa itsestään-selvyys. Niissä verkon ylläpito kaikkine toimintoineen on keskitettyä, tosin tänä päivänä mahdollisesti myös ulkoistettua. Sen sijaan pienissä työyhteisöissä tai paikoissa, joissa tiedon siirto on vähäistä ja rajattua (kuten kotona) vertaisverkko saattaa olla edullisin ja näppärin verkkoratkaisu.

LIITE 2. (jatkuu)

Vertaisverkko

Työasemien välisessä, koneesta koneeseen toteutetussa vertaisverkossa ei ole varsinaista palvelinkonetta tai mitään hierarkiaa koneiden välillä. Kaikki työasemat ovat keskenään tasa-arvoisia. Tämä merkitsee, että kukin kone voi toimia tarpeen mukaan sekä työasemana että palvelimena ilman että yhdelläkään tietokoneella on kokonaisvastuuta verkosta. Kun vertaisverkon työaseman toimii palvelimena, se jakaa omia resurssejaan muiden vertaisverkon työasemien käyttöön (esim. jaettu kirjoitin). Asiakkaana vertaisverkon työaseman on silloin, kun se käyttää verkon jaettuja resursseja. (vrt. kuva 8.)



Kuva 8. Vertaisverkossa jokainen työasema toimii sekä palvelimena että työasemana.

Vertaisverkkoja voidaan kutsua myös työryhmiksi (esim. Windowsia asennettaessa kone liitetään jonkin työryhmän tai toimialueen jäseneksi. Toimialue eroaa työryhmästä siinä, että toimialue luodaan lähiverkkopalvelimelle ja sitä hallitaan keskitetysti, kun taas vertaisverkosta puuttuu keskitetty hallinta.

LIITE 2. (jatkuu)

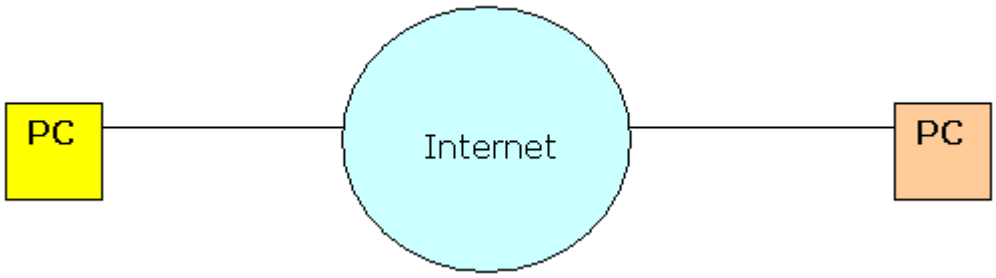
Jos vertaisverkossa on paljon käyttäjiä (yli 15-20), niin sen ylläpito on aika työlästä, koska vertaisverkossa jokaista konetta pitää hallinnoida erikseen.

Työryhmä (workgroup) Pieni osasto- tai työryhmäkohtainen lähiverkko, joka voi olla itsenäinen tai osa suurempaa verkkoa.

Miksi vertaisverkkoja sitten käytetään? Vertaisverkossa käyttöjärjestelmien ei tarvitse olla samalla tehokkuus- ja turvallisuustasolla kuin ohjelmien, jotka on erityisesti suunniteltu palvelinkäyttöön. Tämä taas johtuu siitä väistämättömästä tosiasiasta, että vertaisverkkojen ylläpitoon osallistuvat useimmiten useat eri työasemien ylläpitäjät, joiden tiedot ja taidot ovat harvoin yhteismitalliset. Toisaalta, jos verkko pysyy pienenä ja kaikki keskeiset asiat saadaan vertaisverkon kautta käyttöön, vertaisverkko saattaa olla jossain tapauksissa paras ja edullisin verkottamisvaihtoehto; erityisesti, jos verkko ei ole kovassa kasvussa eikä verkon keskitetty hallinta ole tärkeä kriteeri.

Peer to peer (file sharing)

Käsitettä vertaisverkko käytetään tänä päivänä myös eräässä toisessa merkityksessä. Tällä tarkoitetaan ns. tiedostonvaihtopalvelua, jota toimii esim. kotikoneiden välillä internetin välityksellä (vrt. kuva 9.). Siinä esim. kaksi kotikonetta (sininen ja oranssi) vaihtavat esim, mp3-tiedostoja internetin välityksellä. Tämä tapahtuu niin, että molemmat kotikoneet laittavat jakoon jonkin kansion, joka jaetaan nettiin. Erillisten ilmaisien tiedostojenjako-ohjelmien avulla (kuten KazaA) tiedostoja voidaan hakea ja kopioida ympäri maailmaa toisten kotikoneilta. Nykyään käydään kiivasta keskustelua siitä, onko menetelmä laillinen vain laiton. Lue asiasta halutessasi lisää täältä (pdf-tiedosto, aukeaa uuteen ikkunaan).



Kuva 9. Peer to peer -verkon toimintaidea.

Palvelinperustainen verkko

Kun halutaan saada suuremman ihmismäärän käyttöön, vertaisverkko on liian hankalasti ylläpidettävä järjestelmä. Palvelinperustaisessa verkossa verkon ylläpito voidaan keskittää yksiin käsiin ja yhteen paikkaan, jolloin verkon ylläpito selkiytyy. Se, miten hyvin palvelinpohjainen verkko lopulta toimii, riippuu palvelimen ylläpitäjän taidoista.

Palvelimen rooli on palvella. Palvelimia on erilaisia ja kukin niistä on omistautunut omalle tehtävälleen:

Tiedosto- ja tulostinpalvelimet	Palvelimet hoitavat pääsyä tiedostoihin ja tulostimiin. Ne ovat tiedostojen ja tiedon varastoimista varten (esim. tulostuksenhallinnan ohjaus). Tiedosto- ja tulostuspalvelinten tiedot tai tiedostot siirretään sen asiakkaan tietokoneelle, joka on sitä pyytänyt palvelimelta.

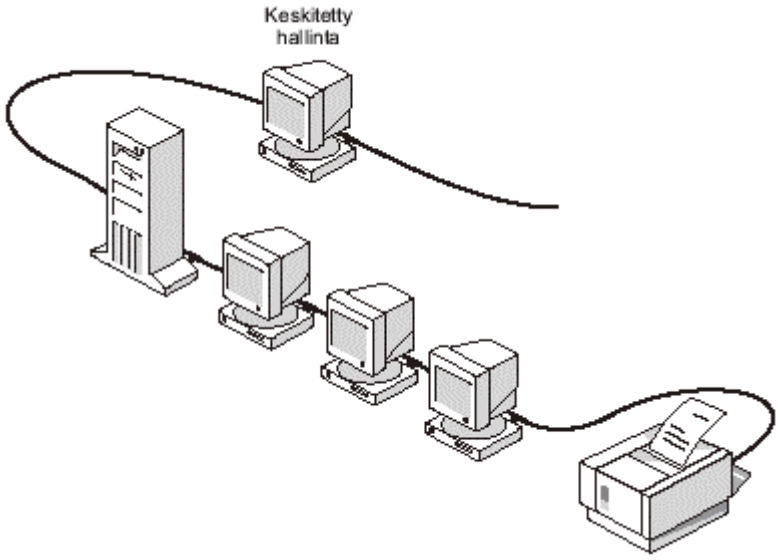
LIITE 2. (jatkuu)

Sovelluspalvelimet	Sovelluspalvelimet varastoivat tietoa, joka on järjestetty niin, että se on helposti asiakkaiden saatavilla. Sovelluspalvelimissa tietokanta pysyy koko ajan sovelluspalvelimessa ja vain kyselyn tulostieto siirretään asiakaskoneelle.
Postipalvelimet	Postipalvelimet toimivat sovelluspalvelimien tapaan siinä mielessä, että palvelin- ja asiakassovellukset on erotettu toisistaan ja dataa haetaan valikoidusti palvelimelta asiakaskaskoneelle.
Faksipalvelimet	Faksipalvelimet hoitavat faksiliikennettä verkosta ulos ja sisään jakamalla yhden tai useamman faksimodeemin.
Tietoliikennepalvelimet	Tietoliikennepalvelimet hoitavat tietovirtoja ja sähköpostiviestejä palvelimen oman verkon ja muiden verkkojen, isojen keskustietokoneiden ja etäkäyttäjien väillä. Ne ottavat yhteyttä palvelimiin modeemia ja puhelinjaa apuna käyttäen.
Hakemistopalvelimet	Hakemistopalvelimien avulla käyttäjät voivat paikallistaa, tallentaa ja varmistaa verkon informaatiota. Erilaisten palvelujen suunnittelu on tärkeää verkon laajentuessa. suunnittelijan on otettava huomioon kaikki verkon kasvuun liittyvät tekijät, jotta verkon käyttö ei esty, vaikka jonkin verkon palvelimen roolia muuttuu kesken kaiken.

LIITE 2. (jatkuu)

Palvelinperustaisella verkolla on monia etuja:

- Resurssien jakaminen. Palvelin on tarkoitettu tarjoamaan pääsy tiedostoihin ja tulostimiin sekä samalla ylläpitämään käyttäjän suorituskykyä ja turvallisuutta.
- Turvallisuus. Palvelinperusteisessa systeemissä turvallisuutta ylläpitää yksi taho, palvelimen ylläpitäjä (administrator), jotka vastaa turvallisuudesta kaikille verkon käyttäjille. Kuva 10. kuvaa tilannetta:



Kuva 10. Verkon keskitetty hallinta tarkoittaa, että koko verkkoa hallitaan yhdestä pisteestä. Toiminnan keskeisin juttu on lähiverkkopalvelimen ylläpitäjän ammattitaito.

- Varmuuskopiointi. Varmuuskopiointi voidaan tehdä keskitetysti ja sen ajoitus voidaan säätää tarkoituksenmukaisesti, vaikka varmuuskopiointi pitäisikin tehdä eri puolilta verkkoa. Lisäksi kokonaiset tietojärjestelmiä (systeemejä), jotka ovat toiminnallisesti kriittisiä, voidaan monistaa ja

varmuuskopioida keskitetysti ilman, että yksittäisen pitäisi vaivata asialla päätään.

- Käyttäjien suuri lukumäärä. Palvelinperusteinen verkko voi tukea tuhansia käyttäjiä, mikä ei ole mahdollista vertaisverkossa.
- Räätälöinti. Palvelimien kautta asiakastyöasemien laitteita voidaan rajoittaa kunkin käyttäjän tarpeiden mukaiseksi. Tämä koskee niin käyttöoikeuksia kuin laitteen fyysisiä ominaisuuksiakin.

LIITE 3

Wikipedia - vapaa sanakirja, WPA-käsite

WPA

WPA eli Wi-Fi eli Wireless Fidelity Protected Access on välivaiheen tietoturvatekniikka, joka kehitettiin WEP-salauksen ongelmien paljastuttua. WPA sisältää tulevan 802.11i – tietoturvastandardin ominaisuuksia, ja se on yhteensopiva niin nykyisten kuin tulevienkin laitteiden kanssa. WEP-salauksen heikot aloitusvektorit on korjattu ja lisäksi salausavainta vaihde-taan automaattisesti 10 000 paketin välein. WPA:ssa on käytössä TKIP-salaus (Temporal Key Integrity Protocol) eli WEP-avaimen hajautus mahdollistaa jaetun salaisen avaimen suojaamisen hyökkäyksiltä. TKIP parantaa langattoman verkon turvallisuutta huomattavasti ottamalla käyttöön pakettikohtaiset salausavaimet. TKIP salaa liikenteen RC4-algoritmilla mutta salausavaimen pituus on 128 bittiä. WPAn huonona puolena pidetään sen alttiutta palvelunestohyökkäyksille. Haavoittuvuus johtuu WPAn tavasta selvitä verkkohyökkäyksistä: WPA sulkee koko verkon minuutiksi havaittuaan hyökkäyksen, jolloin myös verko lailliset käyttäjät jäävät katkon aikana ilman palvelua. WPA tullaan korvaamaan IEEE 802.11i protokollalla.

TKIP

Temporal Key Integrity Protocol (TKIP) on langattomien lähiverkkojen tietoturvaprotokolla, joka huolehtii yhteyksien salaamisesta ja turvaamisesta. Se kehitettiin alkuperäisen WEP-protokollan tilalle, koska WEP-protokollasta on löytynyt lukuisia vakavia haavoittuvuuksia. TKIP-protokollan lisäksi alkuperäistä tietoturvastandardia laajennettiin myös muun muassa 802.1x-standardilla, ja uusia tietoturvastandardeja oikein noudattavat tuotteet voivat nykyisin saada WPA-merkinnän. Koko WPA-pakettikaan ei korjaa aivan kaikkia vikoja, ja ennen vuotta 2005 olisi tarkoitus ilmestyä markkinoille 802.11i-standardin mukaisia tuotteita, joissa koko tietoturvaratkaisu on suunniteltu uusiksi alusta loppuun.