Opinnäytetyö (AMK)

Tietotekniikan koulutusohjelma

Ohjelmistotuotanto

2012

Antti-Pekka Majanen

YRITYKSEN TIETOVERKON JA TIETOTURVAN PARANNUS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietotekniikan koulutusohjelma| Ohjelmistotuotanto

Huhtikuu 2012 | 30

Ohjaaja Tiina Ferm

Antti-Pekka Majanen

YRITYKSEN TIETOVERKON JA TIETOTURVAN PARANNUS

Tämän opinnäytteen tarkoituksena oli suunnitella turkulaiselle Kustannusosakeyhtiö Sammakolle tietoverkkoratkaisu ja tietoturva. Yrityksen infrastruktuuri sisältää toimiston ja kirjakaupan Turussa sekä kirjakaupan Helsingissä.

Lähtökohtana oli kartoittaa tarpeet ja määrittää, mitä tietoverkolta haluttiin. Isoimmat ongelmakohdat yrityksen nykyisessä tietoverkossa ovat verkon pieni koko ja tiedostojen jakamisen puuttuminen. Vaatimuksena yritykseltä oli, että suunniteltava tietoverkko palvelisi mahdollisimman hyvin liiketoiminnan tarpeita sekä sen käyttäminen olisi helppoa ja turvallista.

Nykyaikana langaton tiedonsiirtotekniikka on jo niin kehittynyttä, että se antaa hyvät mahdollisuudet rakentaa laajojakin tietoverkkoja langattomasti, siksi suunnittelemani tietoverkko pohjautuu langattomaan WLAN-tekniikkaan.

Tietoverkon suunnittelu näinkin isolle yritykselle oli haastavaa. Suunnitteluprosessissa käytettiin hyväksi tehtyä kartoitusta tämänhetkisestä yrityksen tietoverkon tilanteesta. Vaatimusmäärittelyn ja suunnittelutyön lopputuloksena valmistui suunnitelma yrityksen parannetusta tietoverkosta ja tietoturvasta. Mainittavimpia hyötyjä tämän parannussuunnitelman jälkeen ovat mm. langattomuus, verkkotulostus ja yrityksen sisäinen tiedostojen jako.

Tietoverkon ja tietoturvan parannussuunnitelmassa päädyttiin käyttämään langattomassa lähiverkossa 802.11 b/g-tekniikkaa WPA(TKIP)-salauksella. Tiedostojen jako tullaan toteuttamaan NAS-palvelimella ja verkkotulostus sähköpostitulostuksella. Tietoturvassa tullaan ottamaan tietoturvasuunnitelman myötä käyttöön lukuisia tietoturvaan liittyviä menetelmiä, aina riskienhallinnasta tietoturvan toteutukseen.

ASIASANAT:

WLAN, tietoverkot, lähiverkot, tietoturva

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Software Engineering

April 2012| 30

Instructor Tiina Ferm

Antti-Pekka Majanen

IMPROVING COMPANY'S COMPUTER NETWORK AND DATA SECURITY

The purpose of this thesis was to design computer network and data security for Sammakko Publishing House. The company has offices in three locations. Main office is located in Turku and the company also has two bookstores. The aim is to connect these offices to each other through the data network.

The starting point was to identify the needs and create requirements. The major problem areas in the current network are the network's small size and lack of file sharing. The main requirement of the company was that the network is designed to best support business needs. In addition, it should be easy to use, safe and easy to maintain.

Wireless technology has already become so advanced that it provides a good opportunity to build a widespread computer networks wirelessly. In this thesis, new data network is based on wireless communication.

The end result was a comprehensive reporting of the data network and security design. This thesis is also intended to be a help in possible problems and future upgrades.

KEYWORDS:

WLAN, data network, local area network, data security

SISÄLTÖ

KÄYTETYT LYHENTEET

ADSL	Verkkokytkintekniikka. Käytetään siirtäessä data puhelinlinjaa pitkin epäsymmetrisessä muodossa.
Bitti	Tässä työssä käsitellään tietotekniikan bittejä tiedonsiirron mittarina. Lähetty bittimäärä verrattuna aikaan (sekuntia), bit, binary digit.
Ethernet	Lähiverkkotekniikka.
HTTP	Hypertekstin siirtoprotokolla.
IEEE 802.11	Standardi langattomille lähiverkkotekniikoille.
Internet	Maailmanlaajuinen, yhteen liitettyjen tietoverkkojen kokonaisuus.
IP-Protokolla	Kaikkia internetissä olevia koneita yhdistävä TCP/IP-mallin internet-kerroksen protokolla.
IPSec	Joukko tietoliikenneprotokollia yhteyksien turvaamiseen.
ISP	Asiakkaalle internet-yhteyden tarjoava yritys.
LAN	Lähiverkkotekniikka.
MAC	Tässä työssä laitteiden yksilöivä MAC-osoite.
Mbps	Tiedonsiirtonopeus, mega bittiä/sekunti (1 000 000 bittiä/ sekunti).
NAS	Verkkotallennustapa.
NAT	Osoitteenmuunnos tekniikka.
OSI-malli	Open Systems Interconnection Reference Model.
Palomuuri	Tärkeä osa tietoturvaa, eristää ja suodattaa verkkojen välistä liikennettä.

RAID	Tallennustekniikka jossa useita kiintolevyä yhdistetty yhdeksi loogiseksi levyksi.
RJ-45	Yleinen lähiverkkojen kaapeloinnissa käytettävä liitintyyppi.
SNMP	TCP/IP –verkkoihin liittyvä hallintaprotokolla.
SSID	WLAN-verkon verkkotunnus.
Solmu/Piste	Tietoverkon osa (eng. node).
Tavu	Työssä käytetään tavua kerrannaisyksikkönä ilmoittaessa tiedonsiirron nopeutta (byte).
TCP/IP	Tietoverkkoprotokollan yhdistelmä (Transmission Control Protocol / Internet Protocol).
TKIP	Tietoturvaprotokolla jota käytetään langattomissa tietoverkoissa (Temporal Key Integrity Protocol) .
UPS	Laite jota käytetään virransyötön tasaamiseksi lyhyissä sähköverkon katkoksissa.
VPN	Tapa jolla voidaan yhdistää lähiverkkoja julkisen verkon yli.
WLAN	Langaton lähiverkkotekniikka.

1 JOHDANTO

Opinnäytteeni tarkoitus oli suunnitella Kustannusosakeyhtiö Sammakolle toimiva ja turvallinen yrityksen sisäinen tietoverkko. Kustannusosakeyhtiö Sammakko on vuonna 1996 perustettu itsenäinen yleiskustantamo. Toimipisteitä yrityksellä on toimisto Turussa sekä kirjakaupat Turussa ja Helsingissä.

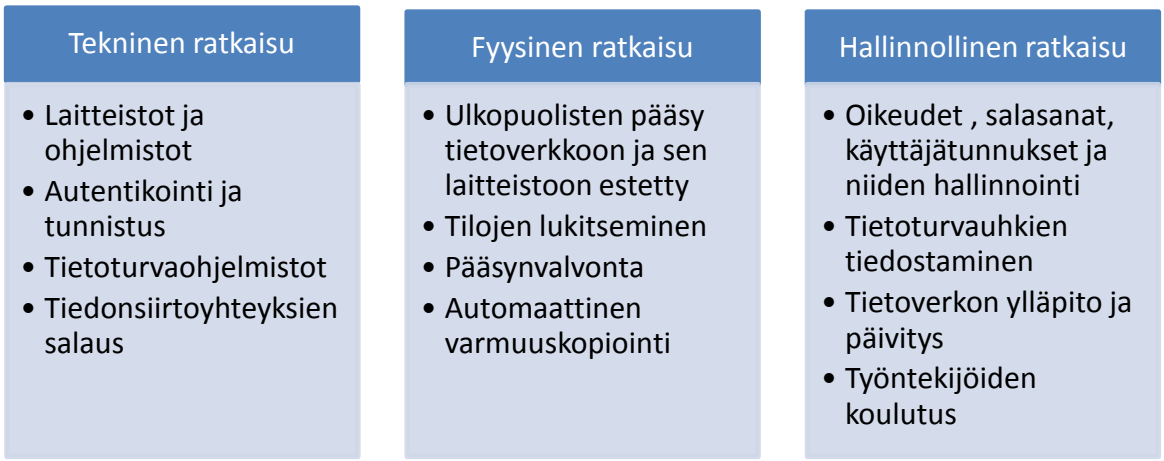
Tässä raportissa tullaan etenemään alkutilan ongelmien havainnointien ja niiden ratkaisujen kautta, suunniteltuun lopputilanteeseen. Opinnäytetyöni käynnistyi keväällä 2011 kartoittaessa yhdessä yrityksen johtoportaan kanssa yrityksen sen hetken tietoverkkoa, ja sen tietoturvatasoa. Sain tutustua ja kartoittaa tietoverkon nykyistä tilaa perusteellisesti ja sitä kautta sain hyvät eväät luoda uuden suunnitelman tehokkaasta yrityksen tulevasta tietoverkosta.

Työssäni suunnittelin verkkoinfrakstuurin sekä laitteistosuunnitelman, joka palvelisi mahdollisimman hyvin yrityksen tarpeita. Tärkeänä tavoitteena oli luoda kustannustehokas ja helposti ylläpidettävä verkko, jonka päivitykseen ei tarvita sen suurempaa asiantuntemusta tietotekniikasta tai tietoliikenteestä.

Yrityksessä on jo käytössä jonkinlainen lähiverkko mutta se on suppea, eikä se ole mitenkään kytköksissä yrityksen toimipisteiden välillä. Käytössä olevaa tietoverkkoa vaivaa myös ajoittaiset katkokset, jotka johtuvat eri verkkostandardien yhteensopimattomuudesta ja teknillisistä ratkaisuista.

Työni tärkeä osa onkin luoda luotettava tietoliikenneverkko, jossa minimoidaan riskit, jotka johtavat tiedonsiirron katkeamisiin ja sitä kautta työskentelyn tehottomuuteen.

Kustannusosakeyhtiö Sammakon sisällä käsitellään paljon luottamuksellista tietoa, jota suurimmaksi osaksi liikutellaan ja säilytetään sähköisenä datana. Tästä syystä tietoturva ja sen riskit ovat tärkeässä asemassa. Kuvassa yksi on määritelty tietoturvaratkaisu, johon paneudutaan tarkemmin opinnäytteen luvussa kolme.



Kuva 1. Tietoturvaratkaisu.

Opinnäytteeni rakenne voidaan jaotella eri osa-alueisiin. Työn alkupuolella kerrotaan suunnitteluprosessin aloituksesta, jossa kartoitettiin ja havainnointiin tietoverkon nykytilannetta. Projektin vaatimusmäärittelystä, työssä edetään itse tietoverkon suunnitteluun ja sen rakenteen muodostumiseen.

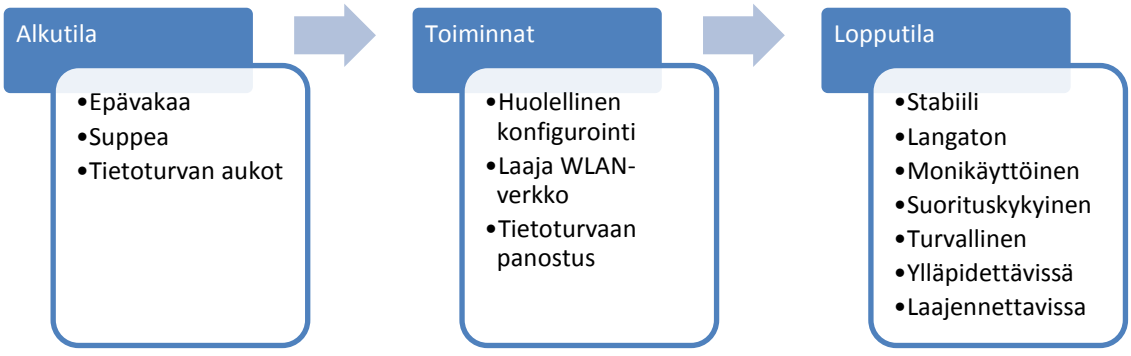
Työssäni esitellään myös tärkeimpiä asioita lähiverkkotekniikasta, etenkin langattomasta lähiverkkotekniikasta, johon toimeksiantajan lähiverkot tulee opinnäytteen jälkeen perustumaan.

Suunnitellun tietoverkon esittelystä opinnäytteessäni siirrytään tietoturvan riskienhallintaan ja tietoturvan toteuttamiseen Kustannusosakeyhtiö Sammakossa. Ennen yhteenvetoa, opinnäyte esittelee vielä suunnitelman tietoverkon testauksesta ja ylläpidosta.

2 TIETOVERKON SUUNNITTELU

Yrityksen tietoverkon suunnitteluprosessi käynnistyi kartoittamalla minkälainen tietoverkko on tällä hetkellä käytössä yrityksen sisällä. Yrityksen toimistolla tietoverkko toimii tällä hetkellä siten, että jokainen tietokone on kytketty reitittimeen langallisesti ja sitä kautta tietokoneet ovat saaneet yhteyden ADSL-modeemin avulla internettiin. Minkäänlaista lähiverkon hyödyntämistä esim. tiedostojen jakamista ei nykyisessä verkossa käytetä. Toimistotiloissa on myös langaton WLAN-reititin, jonka konfigurointi, ja etenkin sen suojaustekniikat ovat pahasti vanhentuneet.

Sammakon tiloista löytyy paljon tietotekniikkaa. Pääosin laitteet ovat henkilökohtaisia Windows-pohjaisia PC:itä ja tulostimia. Tarkoituksena onkin päästä eroon johdoista, joilla laitteet on tällä hetkellä yhdistetty toisiinsa ja sitä kautta laajempaan verkkoon (internettiin). Tämän opinnäytteen johdosta yrityksen toimistossa käytetään tulevaisuudessa poikkeuksetta langatonta tiedonsiirtoa. Yrityksen toive olikin, että jatkossa kirjakaupoissakin olisi oma langaton lähiverkko. Näin työntekijöiden tilaa vievä pöytätietokone voitaisiin päivittää kannettavaan tietokoneeseen. Ongelmia nykyisessä tilanteessa koituu myös tulostamisessa. Tulostus on vaatinut tulostusprosessin käynnistämisen siihen kytketystä tietokoneesta. Suunnitelmassa tulostus tapahtuisi sähköpostitulostuksella, joka on helpottava asia työnteon tehokkuuden kannalta. Keskeisin ongelma nykyisessä tietoverkossa on juuri tiedostojen siirtäminen ja verkon kapasiteetin käyttämättömyys. Alla oleva kuva kaksi esittää tietoverkon alkutilan ongelmia, niiden ratkaisuja ja suunnitelman lopputilanteen.

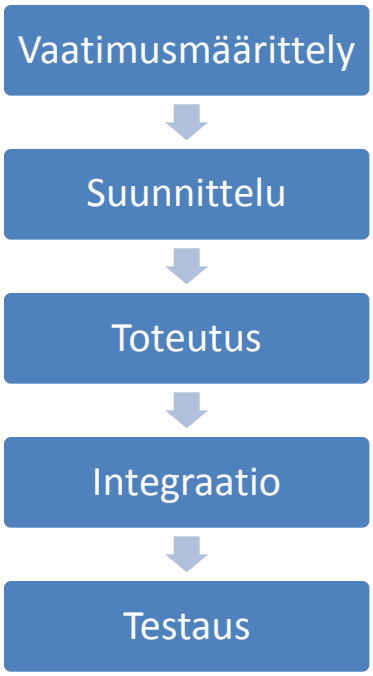


Kuva 2. Tietoverkon alku ja lopputila.

2.1 Suunnitteluprosessi

Kustannusosakeyhtiö Sammakon tietoverkon suunnitteluprosesissa käytin jo pitkään tunnettua vesiputousmallia. Mallia on käytetty lähinnä ohjelmistotuotantoprosesseissa, jossa suunnittelun vaiheet kulkeutuvat eteenpäin lineaarisesti.

Tässä työssä tietoverkon ja tietoturvan suunnitteluprosessi jakautui alla olevan kuvan kolme mukaisiin vaiheisiin.



Kuva 3. Suunnitteluprosessi.

Suunnitteluprosessin toteutus, integraatio ja testaus tullaan toteuttamaan fyysisesti todellisella kokoonpanolla, kun tietoverkon laitteet ovat hankittu. Testausta voidaan toki suunnitella etukäteen. Tietoverkon testaukseen paneudutaan kappaleessa neljä.

Vaatimukset yrityksen tietoverkolle voivat tulevaisuudessa myös muuttua. Näihin muutoksiin tullaan varautumaan jo suunnitteluvaiheessa. Muuttuvia vaatimuksia voi olla esimerkiksi verkon laajentuminen tai uuden tekniikan käyttöönotto. Dokumentoimalla nykyinen verkko mahdollisimman laajasti, ja ottaen huomioon laitehankinnoissa tulevaisuuden vaatimukset, voidaan palata alkuperäiseen suunnitelmaan ja joustavasti osio kerrallaan suorittaa tarvittavat muutokset.

2.2 Vaatimusten määrittely

Aluksi on tärkeää tietää, mitä tietoverkolta ja tietoturvallisuudelta vaaditaan yrityksessä. Tässä tapauksessa vaatimusmäärittelyssä kartoitettiin niitä vaatimuksia joita tietoverkon ja tietoturvan täytyy pitää sisällään. Ilman riittävän kattavaa vaatimusmäärittelyä koko suunnitteluprosessia ei olisi voinut toteuttaa. Jokainen vaatimus kirjattiin juoksevalla numeroinnilla. Alla olevassa kuvassa neljä on esitetty esimerkki tavasta jolla vaatimukset ovat dokumentoitu.

Numero	**ID**	**Käyttäjävaatimukset**
1	1	Työasemasta pitää päästä langattomasti lähiverkkoon yrityksen sisätiloissa.
2	2	Tiedostoja on pystyttävä siirtämään lähiverkon sisällä ja tallentamaan niitä yrityksen verkkokiintolevylle.
3	3	Lähiverkon ja internetyhteyden pitää olla riittävän nopea, riittääkseen tehokkaaseen työkäyttöön.
4	4	Tulostaminen pitää tapahtua hyödyntäen lähiverkkoa.
5	5	Etätyöskentelijän pitää pystyä käyttämään internetin kautta tiedostopalvelimen ominaisuuksia.
6	6	Yrityksen tietoverkkoon ei pidä päästä ulkopuolisten ilman erityistä lupaa.
Numero	**ID**	**Toiminnalliset vaatimukset**
1	50	Tietoverkon teoreettinen nopeus toimitiloissa pitää olla vähintään 10 Mbps.
2	51	Langattoman lähiverkon pitää tukea 802.11b/g-standardia.
3	52	Yrityksen tietoverkosta on kyettävä pääsemään internetiin.
4	53	Tiedostopalvelimen tallennuskapasiteetti pitää olla vähintään kaksi teratavua ($2 * 10^{12}$ tavua).
Numero	**ID**	**Ei-toiminnalliset vaatimukset**
1	100	Yrityksen tietoverkon laitteistojen tulee olla energiataloudellisia.
2	101	Yrityksen tietoverkon laitteistojen tulee olla kierrätettävissä.
3	102	Suunnitellun tietoverkon hankintakustannukset eivät saa ylittää 10 000€.
4	103	Tietoverkon suunnittelu ei saa aiheuttaa häiriöitä työntekijöiden työntekoon.

Kuva 4. Esimerkki vaatimusten kirjauksesta.

Tietoverkon vaatimusmäärittely kattaa laajuudeltaan yrityksen toimiston sekä kaksi kirjakauppaa. Laajimmillaan tietoverkon uudistus koskee kuitenkin toimistotilaa, jossa on eniten tietotekniikkaa. Vaatimuksia syntyi kaiken kaikkiaan 150 kpl. Seuraavassa on lueteltu havainnoillisesti krittisimmät vaatimukset, koskien suunniteltua tietoverkkoa ja tietoturvaa.

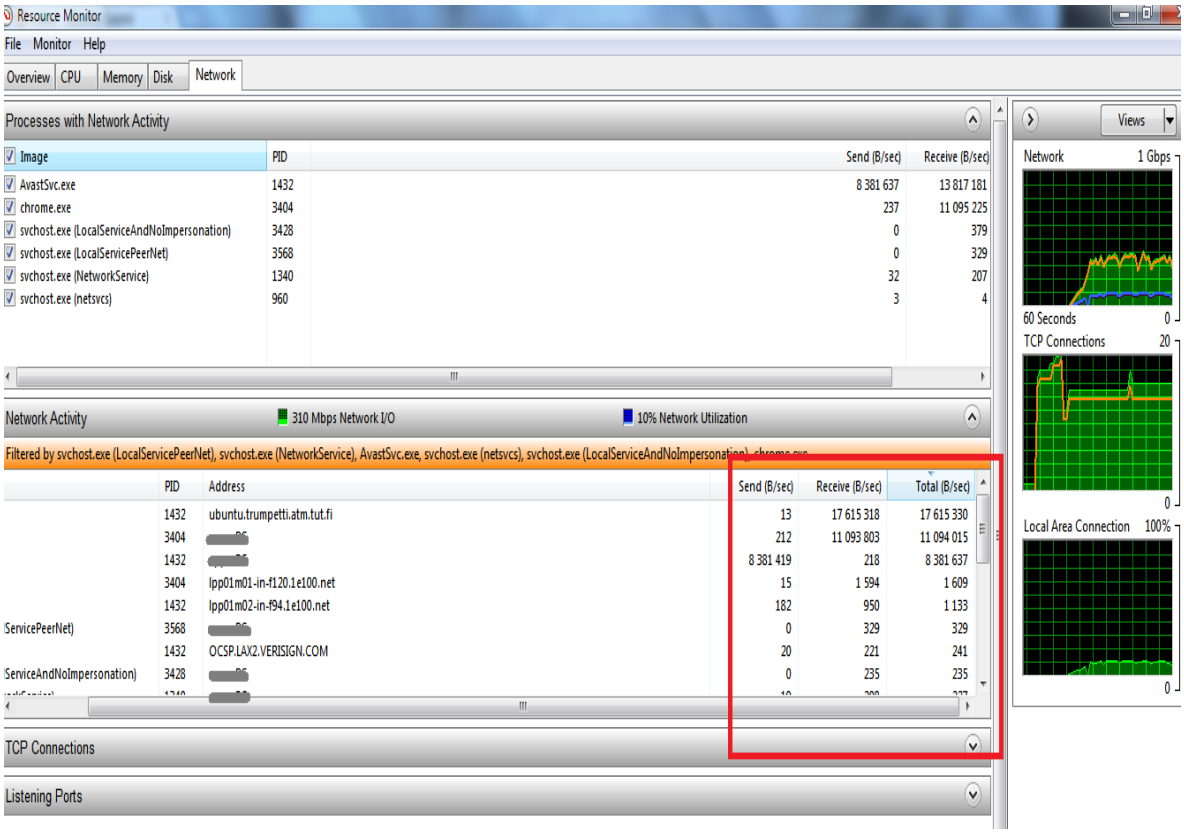
Yrityksen tietoverkko pitää olla nopea ja turvallinen. Nopeudella tarkoitetaan tässä tietoverkossa sitä, kuinka nopeasti tiedostoja pystytään siirtämään yrityksen tietoverkon sisällä.

Turvallisuudella Kustannusosakeyhtiö Sammakko haluaa tietoverkossaan sitä, että kukaan ulkopuolinen ei pääse käsiksi yrityksen tiedostoihin tai tietoihin. Tämä seikka asettaa tietyt kriteerit sekä priorisoinnit tiedostojen käyttöoikeuksille.

Yritys haluaa myös, että haittaohjelmien ja virusten varalta on suojauduttu hyvin. Tämä asettaa tietyt vaatimukset tietoturvaohjelmistoille ja palomuuritekniikoille.

Tietoverkon kapasiteetti pitää mitoittaa niin, että se kestää ilman häiriöitä kaikkien yrityksen työntekijöiden normaalin samanaikaisen työkäytön. Yhtäaikainen käyttö normaaliolosuhteissa tarkoittaa, sähköpostipalvelun käyttöä, normaalia selainpohjaista internetin käyttöä ja tiedostojen jakamista/latausta omasta tiedostopalvelimesta. Tämä asettaa myös vaatimukset internet-palveluntarjoajalle (ISP).

Verkon tilaa ja siinä siirrettävän datan määrää verkon ja työaseman välillä voidaan helposti seurata esimerkiksi MS Windows 7 -käyttöjärjestelmän resurssimonitori-ohjelman avulla (kuva 5). Esimerkkikuvassa viisi havaitaan kaistan käyttöaste ja reaaliaikainen verkon aktiivisuus.



Kuva 5. Kuvakaappaus MS Windows 7:n resurssimonitorista.

Toiminnot, joiden pitää löytyä tässä tietoverkossa on tiedostojen jako, toimiva palomuuri-tekniikka, nopeat ja kustannustehokkaat ohjelmistot sekä käyttäjäystävälliset käyttöliittymät.

Yrityksen työntekijät tekevät töitä paljon myös etänä, jolloin on tärkeää, että työntekijöiden pitää saada käyttöönsä yrityksen tiedostopalvelimelle tallennetut tiedostot myös toimipisteiden ulkopuolelta käsin. Tämä asettaa vaatimuksia tiedostojen jakamiselle sekä tietoturvalle.

Ylläpidettävyydellä yritys haluaa, että tietoverkon pitää olla yksinkertaisten siihen liittyvien ongelmien sattuessa helposti korjattavissa. Uuden tietoverkon dokumentoinneista pitää löytyä ohjeistus, miten mahdollisen ongelman esiintyessä täytyy toimia ja kehen tarpeen vaatiessa pitää ottaa yhteyttä.

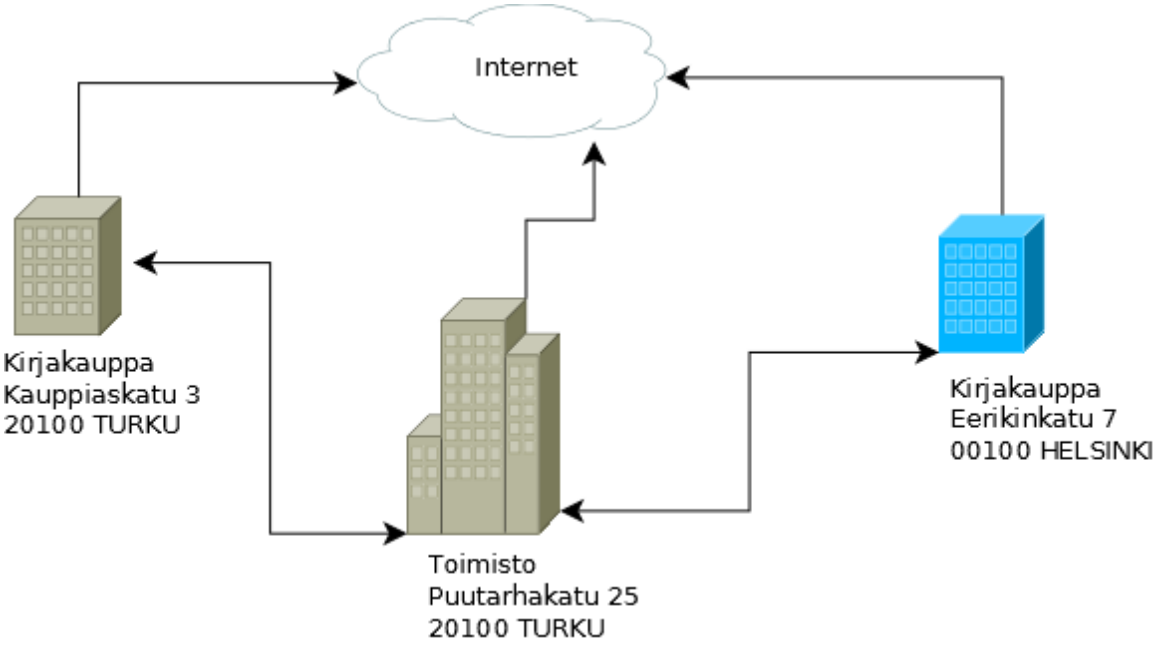
Uuden tietoverkon hankintakustannusten pitää olla edulliset ja tietoverkon laitteet energiakulutukseltaan ympäristöystävällisiä.

2.3 Suunnittelu

Tietoverkon suunnitteluprosessi käynnistyi hahmoittelemalla tietoverkon rakennetta ja sen perustarpeita. Perustavoitteena oli, että toimipisteiden välillä voitaisiin siirtää dataa ja kaikista toimipisteistä pääsisi myös internettiin.

Tietoverkkoa suunniteltaessa ylläpidin ajatustapaa, jossa jokainen osa-alue suunnitellaan toteutettavaksi mahdollisimman yksinkertaisesti ja tehokkaaksi. Yksinkertaisuudella tarkoitetaan tässä suunnitelmassa sitä, että verkkolaitteiden määrä olisi mahdollisimman pieni, mutta verkko olisi silti tehokas ja monipuolinen käyttää.

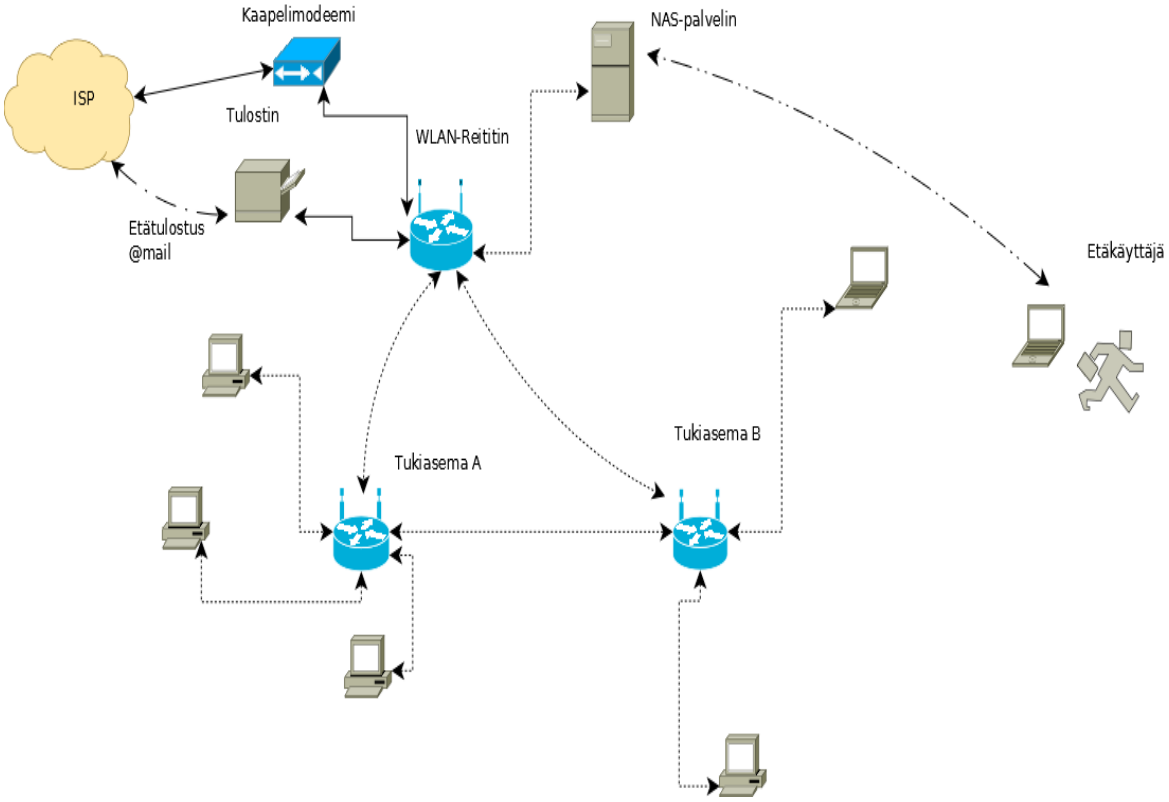
Allaolevassa kuvassa kuusi on hahmoiteltu koko tietoverkon perusajatusta.



Kuva 6. Yrityksen tietoverkon perusajatus.

Kustannusosakeyhtiö Sammakon toimisto muodostaa yrityksen hermokeskuksen, siellä tiedonsiirto on myös vilkkainta. Toimistolla on myös eniten käyttäjiä koko yrityksen tietoverkosta. Toimiston tietoverkon periaate on toteuttaa se mahdollisimman yksinkertaisesti ja langattomasti. Eräs tärkeä hyöty langattomasta tiedonsiirrosta onkin, että vanhaan puurakennukseen ei tarvitse tällöin tehdä johdoituksia.

Toimisto sijaitsee vanhassa puisessa rakennuksessa, paksut hirsiseinät aiheuttavat sen, että yhden WLAN-tukiaseman lähetysteho ei riittäisi, joten kantamaa on lisätty kahdella tukiasemalla. Kuvassa seitsemän ilmenee, miten toimiston tietoverkko rakentuu.



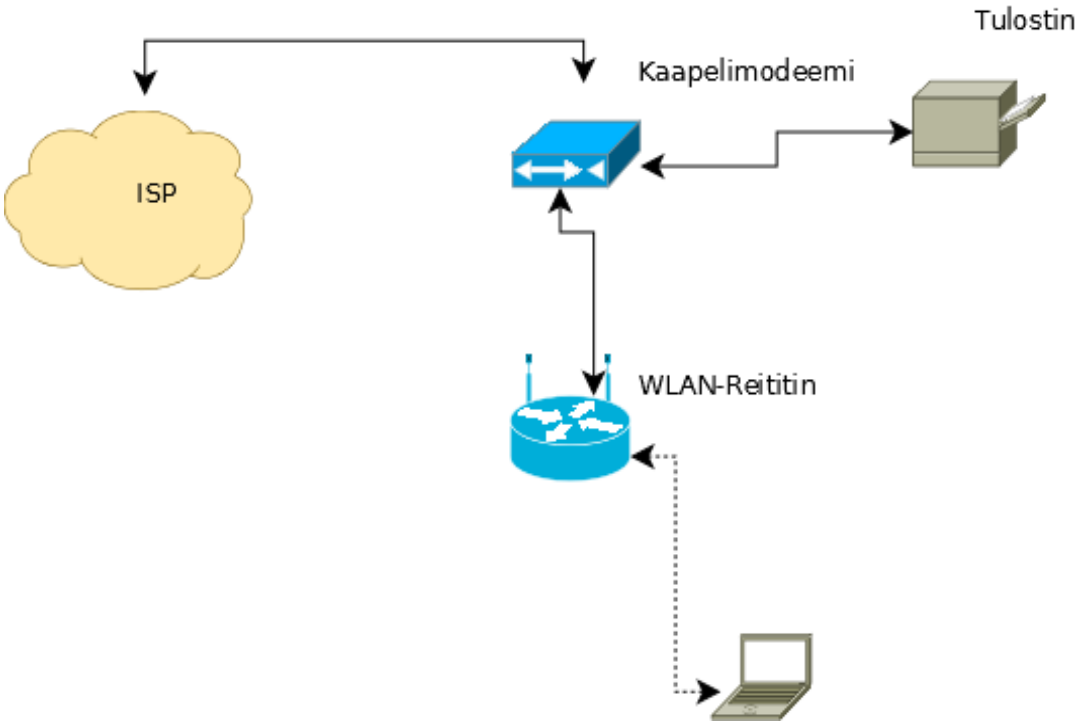
Kuva 7. Verkkorakenne, toimisto.

ISP (Internet Service Provider) palveluntarjoaja tarjoaa internetyhteyden, johon on päätelaitteeksi kytketty kaapelimodeemi. Kaapelimodeemiin on kytkettynä RJ-45 -verkkokaapelilla Ethernet-reititin, 802.11b/g WLAN-tukiasemalla. Reitittimeen on kytkeytyneenä langattomasti tukiasemat A sekä B.

Ethernet-reitittimeen WLAN-tukiasemalla on kytkettynä RJ-45 kaapelilla viiden teratavun NAS-palvelin, johon yrityksen työntekijät voivat tallentaa tiedostojaan sekä avata ja muokata niitä. NAS-palvelimeen pääsee käsiksi myös yrityksen lähiverkon ulkopuolelta, jos esimerkiksi etänä työskentelevä henkilö haluaa tallentaa tai jakaa tiedostojaan.

Tulostusominaisuudet ovat ennen olleet erittäin suppeat. Tulostus on aina vaatinut tiedostojen siirron tulostimeen kytkettyyn koneeseen, koska tulostusta ei ole jaettu yrityksen vanhassa lähiverkossa. Uudessa tietoverkossa tulostus tapahtuu verkkotulostuksena, tarkemmin sanottuna sähköpostitulostuksena. Työntekijä lähettää tulostimelle sähköpostia sille määriteltyyn sähköpostiosoitteeseen ja tulostustoiminta alkaa. Uudessa verkkotulostuksessa työntekijä voi tulostaa asiakirjoja mistä vain edellyttäen, että hän on kytkeytyneenä internettiin. Tämä seikka on tervetullut helpotus esim. etätyöskentelyssä.

Seuraavassa on suunnitelma kirjakaupan verkkorakenteesta. Kirjakaupat ovat tarpeiltaan ja vaatimuksiltaan täysin identtiset, joten myös tietoverkot tulee olemaan samanlaiset. Kuvassa kahdeksan ilmenee kirjakauppojen verkkorakenne.

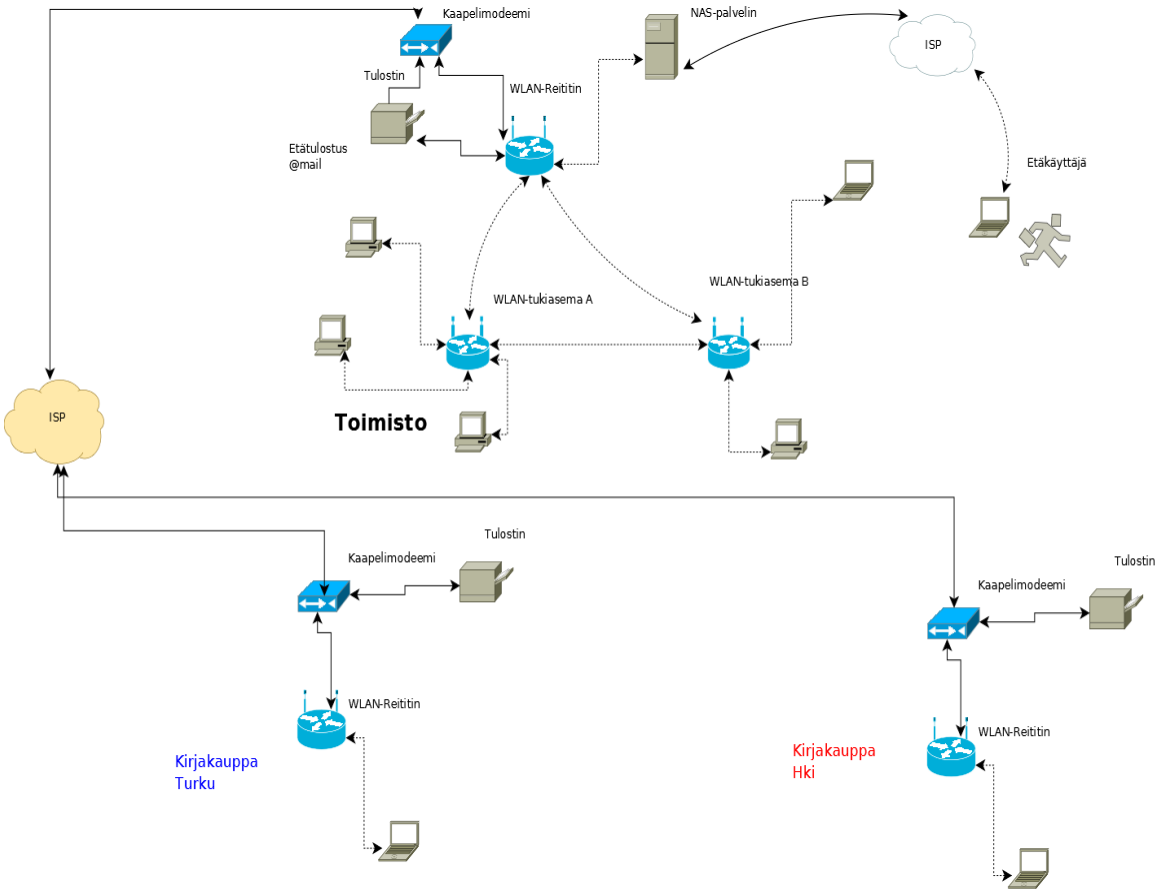


Kuva 8. Verkkorakenne, kirjakaupat.

ISP (Internet Service Provider) palveluntarjoaja tarjoaa internet-palvelut, johon on kytketty päätelaitteeksi kaapelimodeemi. Kaapelimodeemi on kytketty WLAN-reitittimeen, joka toimii myös tukiasemana. Kirjakauppojen neliöala sekä rakennustekniikat eivät vaadi lisä-tukiasemia. Tietoturva maksimoidaan kirjakaupoilla säätämällä lähettimen lähetystehoa sopivaksi, jolla estetään tarpeeton WLAN-verkon kuuluvuus toimitilan ulkopuolelle esim. kadulle.

Tukiasemaan on kytkettynä langattomasti yrityksen työntekijän kannettava tietokone. Tulostin on toimistolla sijaitsevan kaltainen verkkotulostin, jota käytetään sähköpostin välityksellä.

Kuvassa yhdeksän esitetään Kustannusosakeyhtiö Sammakon verkkorakenteen kokonaiskuva. Kuten kuvasta ilmenee, verkkorakenne on varsin yksinkertainen, tämä auttaa tietoverkon ylläpitoa ja mahdollistaa tulevaisuudessa tietoverkon nopean laajentamisen.



Kuva 9. Yrityksen tietoverkon rakenne.

2.4 Yrityksen tietoverkon rakenne

Tietoverkko tietotekniikassa on käsite, joka pitää sisällään päätelaitteiden yhdistämiseen tarkoitetun tietoliikenneverkon. Tässä yrityksen sisälle suunnitellussa tietoverkossa isoin rooli on lähiverkkotekniikassa.

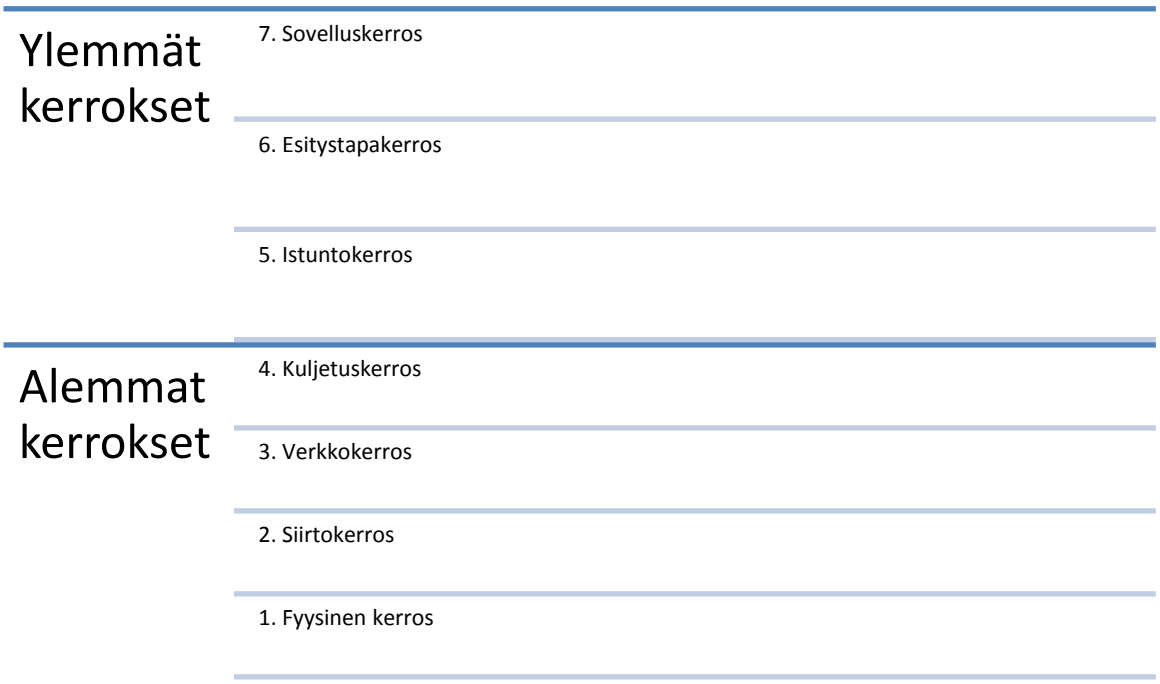
TCP/IP (Transmission Control Protocol / Internet Protocol). TCP/IP suuntautuu kahteen Internetissä käytettävään verkkoprotokollaan. Kyseinen tiedonsiirtomenetelmä yhdistää tietoverkon sisällä eri käyttöjärjestelmät ja verkko-osat toisiinsa. TCP/IP:tä käytetään sekä Internetissä että pienemmissä yksittäisissä verkoissa. [1]

TCP/IP-kokoelman protokollat tarjoavat tiedonsiirtomahdollisuuden kaikille palveluille, joita nykypäivän verkkokäyttäjän saatavilla on. Näitä kyseisiä palveluita ovat mm. sähköpostin lähetys, tiedonsiirrot, reaaliaikaiset viestit sekä www:n käyttömahdollisuus. [1]

TCP/IP pitää sisällään viitemallin, jossa sijaitsevat sovelluskerros, kuljetuskerros, verkkokerros ja peruskerros.

Toinen hyvin tärkeä tekniikka liittyen tietoverkkoihin on OSI-malli (Open Systems Interconnection Reference Model), joka on määritelty yhdistämään erilaiset verkkotekniikat toisiinsa, jotta ne pystyisivät kommunikoimaan keskenään tietoverkoissa standardoidulla tavalla.

OSI-malli pitää sisällää seitsemän kerrosta. Kerrokset kuvastavat tiedonsiirtoprotokollien arkkitehtuuria. Kuvassa kymmenen on esitetty seitsemän kerrosta, joista jokainen suorittaa tietyn verkkotoiminnon



Kuva 10. OSI-malli.

Ensimmäinen OSI-mallin kerrosta sanotaan fyysiseksi kerrokseksi. Se säätää laitteiston yhteyksiä sekä lähetyksen tietovirran koodausta, se myös nimestäkin päätellen siirtää fyysisesti dataa eri verkkosolmujen välillä.

Toinen kerros OSI-mallissa on siirtoyhteyskerros. Se sanelee säännöt, joilla lähetetään ja vastaanotetaan tietoa lähiverkkojen solmujen välillä.

OSI-mallin kolmas kerros on määritelty verkkokerrokseksi, joka määrittelee eri protokollat tiedon reititykselle erilaisien järjestelmien välillä. Kerros on myös vastuussa siitä, että lähetetty data siirtyy oikeaan osoitteeseen.

Neljännessä kerroksessa OSI-mallia sijaitsee kuljetuskerros, se ohjailee järjestelmien välistä tiedonkulkua, suorittaa virheentarkastuksen sekä määrittelee viestien tietorakenteen, sisältäen mm. www-selainten salaustoiminnat.

Viidentenä kerroksena sijaitsee istuntokerros. Istuntokerros ylläpitää istunnon tilaa. Se on tärkeä kerros tietoturvan ja ylläpidon kannalta.

OSI-mallin kuudes kerros on esitystapakerros. Se pitää sisällään protokollia, jotka ovat osana käyttöjärjestelmää. Esitystapakerroksessa kerrotaan järjestelmille myös se miten tieto halutaan esittää. Kerroksessa suoritetaan myös useasti datan salaustoimenpiteet.

OSI-mallin seitsemäs ja ylin kerros on sovelluskerros. Siinä käyttäjälle ”näkyvät” sovellukset suorittavat tarvittavia viestityksiä, ts. kerros määrittelee sen miten sovellukset vuorovaikuttavat eri verkkojen ja järjestelmien kanssa.

Lähiverkkotekniikassa TCP/IP-malli integroituu hyvin OSI-mallin kanssa, joten merkittäviä ovat protokollat jotka liittyvät eri kerroksiin. Esimerkiksi sovelluskerros, jossa sijaitsee hypertekstin siirtoprotokolla (HTTP), kuljetuskerros jossa TCP-lähetyksenohjausprotokolla, verkkokerroksen internet-protokolla (IP) sekä siirtoyhteyskerroksen osoitteenselvitysprotokolla (ARP).

IP-protokolla (Internet Protocol) TCP/IP-mallissa on erityisen tärkeä seikka käsiteltäessä internetiä, ja sen toimintaa. IP-protokolla on itse asiassa koko internet-verkon ydin sekä se on ainoa asia joka jokaista internettiä käyttävää laitetta yhdistää. IP-protokolla voidaan jakaa kahteen protokollaan, verkkotason protokolliin ja sovellustason protokolliin.

Verkkotason protokollat vastaavat verkkotason tiedonsiirrosta ja toimivat yleensä loppukäyttäjältä piiloitettuna. Kyseinen protokolla huolehtii myös pakettien toimittamisesta oikeaan osoitteeseen käyttäen IP-osoitteita (IP-Address). IP-osoite on yksilöivä osoite, jonka perusteella IP-paketit löytävät kohteen ja lähettävät vastauksen kohteesta takaisin. Tällä hetkellä käytössä on Ipv4-protokolla, jossa IP-osoite muodostuu 32-bittisestä luvusta (0 – 4294967295), joka on kirjoitettu neljän kahdeksan bittisen luvun jonona (0 – 255) esim. IP-os. 192.168.0.105 joka muutetaan binaariseen muotoonsa 11000000 10101000 00000000 01101001.

Tulevaisuudessa IP-osoitteet tulevat siirtymään 128-bittiseen Ipv6-järjestelmään, jossa n.4 miljardin mahdollisten Ipv4-osoitteiden sijasta voidaan verkkoa laajentaa yli 340 sekstimiljoonan ($340 * 10^{36}$) osoiteavaruuteen.

Työasemaverkoissa, kuten Kustannusosakeyhtiö Sammakon suunnitellussa verkossa on tärkeää tietää hieman perusteita myös verkon peitteistä, aliverkoista sekä myös osoitteiden muuntamisesta NAT (Network Address Translation) – menetelmällä.

Verkon peite on hyödyllinen kun halutaan tietää mitä tietty IP-osoite pitää sisällään ja mitkä osat kuuluvat mihinkin. Verkon peite on käytännöllinen, jos halutaan tietää ja merkitä se osa osoitteesta, joka kuuluu verkkoon.

Aliverkoissa perusajatus on se, että samassa aliverkossa olevat koneet osaavat lähetellä IP-paketteja käyttäen lähiverkon mekanismeja, kun taas paketti on tarkoitus lähettää lähiverkon ulkopuolisille sijainneille käytetään oletusyhdyskäytävää (default gateway) esim. reitittimen IP-osoite jonka kautta paketit kulkeutuvat.

Osoitteenmuunnos (NAT) on nykypäivänä erittäin yleinen menetelmä, se tarkoittaa lähinnä sitä, että osoitteenmuunnoksesta huolehtiva laite (yleensä reititin) muuntaa lähtevät osoitteet niin, että ulkopuolelle näkyvä IP-osoite onkin reitittimen IP-osoite eikä laitteen oma osoite.

2.5 Lähiverkko

Terminä lähiverkko käsittää tietoliikenne verkon, joka maantieteellisesti on rajattuna jollekin alueelle. Tässä tapauksessa Kustannusosakeyhtiö Sammakon tietoverkko sisältää kolme langatonta lähiverkkoa, joiden välillä voidaan siirtää tietoa, ja kaikista kolmesta on pääsy myös internetiin.

Lähiverkon tekniikoista erittäin tärkeä nykypäivänä on langaton lähiverkkotekniikka IEEE 802.11. IEEE 802.11 -standardeja on kehitelty ajan saatossa ja niitä on nykypäivänä käytössä useita eri versioita.

2.6 Langattomien lähiverkkojen radiotekniikka

Langattomissa lähiverkoissa käytetään vapaasti käytettäviä mikroaaltoalueita. Taajuuden säteilyn teho mitataan desibelimilliwateissa (dBm). Esimerkiksi 802.11b WLAN-laitteiden suurin lähetysteho Euroopan sisällä on 20 dBm (100 mW). [2]

”Mikroaaltoalueella on kaksi vapaasti käytettävää taajuusaluetta: yksi 80 MHz leveä kaistan 2,4 GHz: yläpuolella ja kolme kaistaa hieman yli 5 GHz:ssä.” [2]. Näillä taajusalueilla toimii useasti myös muita laitteita esim. kodinkoneita jotka saattavat häiritä WLAN-verkon toimintaa.

WLAN-tekniikassa pitää ottaa huomioon radioaaltojen etenemiseen vaikuttavat tekijät kuten vaimennus, heijastukset, monitie-eteneminen sekä taipuminen ja sironta. [2]

Lähetys eli TX-antenni muuntaa sähköenergiaa säteilyksi ja vastaanotinantenni (RX) puolestaan säteilyä sähköiseksi signaaliksi. [2]

2.7 WLAN-verkon säteily ja sen ominaisuudet

Säteilyn ominaisuuksia voidaan havoinnollistaa esim. taajuudella ja aallonpituudella. Alla olevasta kaavasta (1), jossa taajuus ja aallonpituus ovat kääntäen verrannollisia, saadaan laskettua aallonpituus.

$$f = \frac{c}{\lambda} \qquad (1)$$

Useamman aallon yhteenlaskussa on merkitystä myös vaihekulmalla. Samasta WLAN-verkon lähettimestä lähtevät aallot etenevät eripituisia reittejä, ne saapuvat vastaanottimeen eri vaiheessa. Tätä kutsutaan 180 asteen vaihe-eroksi. ”*180 asteen vaihe-erossa aallot kumoavat toisensa, ja samanvaiheisena aallot vahvistavat toisiaan*.” [2]

Kun määritellään vastaanotettua tehoa pitää ottaa huomioon lähettimen teho ja signaalin vaimentuminen. Riittävä vastaanottoteho on tärkeä tiedonsiirrossa. Syöttö ja lähetysteho mitataan watteina ja sen osina. Koska signaali ei WLAN-verkoissa etene tyhjiössä on edessä aina väliaineita, jotka vaikuttavat logaritmisesti. Desibeliteho lasketaan tällöin seuraavasti kaavan (2) osoittamalla tavalla.

$$P[dB] = log_{10} \frac{\mathrm{P}\, final}{\mathrm{P}\, ref} \qquad (2)$$

WLAN-verkon antenneihin vaikuttaa polarisaatio, joka määräytyy antennin kulmasta ja ominaisuuksista. Tässä suunnitellussa WLAN-verkossa käytetään diboli-antenneja, jotka vastaanottavat/lähettävät pystypolarisoituja aaltoja.

”Polarisation vuoksi vastaanotto- ja lähetysantenni kannattaa sijoittaa samaan kulmaan maanpinnan suhteen.” [2]. Tässä tietoverkossa vastaanotto/lähetys-antenneja on useita, johtuen halutusta laajasta peittoalueesta. Useat suunta-antennein toteutetut WLAN-linkit häiritsevät toisiaan, siksi suuntaamme toimiston tukiasemien diboliantennit vastakkaisiin polarisaatioihin.

2.8 Langattoman verkon suorituskyky

WLAN-verkoissa suorituskykyä mitataan seuraavilla asioilla:

- Siirtonopeudella (bit/s)
- Viiveellä
- Viiveen vaihtelulla
- Hävinneillä kehyksillä per kokonaisliikenne (frames).

Tärkein suorituskykyä mittaava parametri on tietenkin nopeus, tarkemmin siirtonopeus joka vaikuttaa koko verkon käytettävyyteen. Siirtonopeudessa on pakko todeta se tosiasia, että mainostettu nopeus WLAN-verkoissa ei koskaan yllä luvatulle tasolle. WLAN-tekniikassa käytetään törmäysten välttämiseen vuoronvarausta, kehystystä ja kuittauksia, jotka alentavat siirtonopeutta.

Lisäksi esteet, välimatkat ja häiriöt aiheuttavat sen, että siirtonopeus jää parhaimmillaankin n. 60-70% luvatusta bittinopeudesta (bit/s).

Tärkeä on myös viive ja sen vaihtelu, kun esimerkiksi tietoverkon yli käytetään ns. puhepalveluita. Suuri viive häiritsee käyttöä suunnattomasti, puhe voi kuulua viiven takia myöhässä ja näin ollen kommunikointi voi olla turhauttavaa.

2.8.1 IEEE 802.11 b/g

Kustannusosakeyhtiö Sammakon tietoverkossa käytetään langattomassa tiedonsiirrossa 802.11b/g –standardia.

Tämä tarkoittaa sitä, että kahta standardia, 802.11b:tä ja 802.11g käytetään verkossa rinnakkain. Standardi on hyvä, koska se antaa joustovaraa laitteistojen yhteensopivuudelle. Tietoverkossa voidaan täten käyttää eri ikäisiä tekniikoita ja ne sopivat silti yhteen.

802.11 b/g –verkko hyödyntää vapaasti käytettävää 2,4 GHz:n taajuusaluetta. ”*Jos kaikki yhteyspisteet ovat uudempaa tekniikkaa, mutta osa päätelaitteista tukee vain 802.11b:tä, on saman solun alueella kahdenlaisia päätelaitteita, ja käytetty siirtotapa valitaan päätelaitteen mukaisesti.”* [2].

2.9 Tietoverkon laitteisto

Seuraavassa selvitän laitteisto-tasolla mitä Kustannusosakeyhtiö Sammakon tietoverkko pitää sisällään.

Kulmakivenä Sammakon tietoverkoissa on reititin (router). Se yhdistää tietoverkot, tässä tapauksessa yrityksen lähiverkon internettiin. Reititin toimii ns. tienhaarana jakaessa dataliikennettä tietoverkosta toiseen tunnettuun verkkoon. Kyseinen laite toimii jo edellä mainitun OSI-mallin kerroksella kolme.

Kustannusosakeyhtiö Sammakon tietoverkossa tulee olemaan yhteensä kolme langatonta WLAN-reititintä integroiduilla tukiasemilla. Kyseisiä laitteita tulee olemaan yksi kappale per toimipiste.

Laitteista asetetaan ainakin osoitteenmuunnos NAT toimintaan ja salaustekniikkana käytetään WPA:ta. Reitittimet ja siten koko langaton lähiverkko tulee toimimaan automaattisella 802.11b/g –tekniikan valinnalla.

Tukiasema (Access Point) on langattomassa lähiverkossa tärkeä laite, kun halutaan laajentaa verkon kuuluvuutta. Edellä mainittu langaton reititin itsessään toimii jo tukiasemana mutta kahdella toimiston lisä-tukiasemalla turvataan langattoman lähiverkon kuuluvuus koko toimiston alueella.

Jotta yrityksen sisällä työntekijät voivat käyttää, jakaa ja tallentaa tiedostojaan lähiverkon yli helposti ja varmasti, tietoverkkosuunnitelmassa tiedon tallennus toteutetaan NAS-palvelimella (Network Access Storage - Server). Käytettävänä laitteena tulee toimimaan viiden teratavun ulkoinen Ethernet-kiintolevy.

Tässä ratkaisussa yrityksen työntekijät voivat käyttää dataa NAS-palvelimelta myös lähiverkon ulkopuolelta. Ominaisuus on erittäin hyödyllinen tehtäessä esim. töitä etänä. NAS-palvelin tullaan myös konfiguroimaan myös siten, että verkkotallennusväline varmuuskopioi automaattisesti jokaisen halutun henkilökohtaisen tietokoneen yrityksen tietoverkon sisällä.

3 TIETOTURVAN RISKIENHALLINTA

Seuraavassa käsitellään Kustannusosakeyhtiö Sammakon tietoturvan riskien hallintaa ja olen laatinut viisi vakavinta riskiä yrityksen tietoturvan kannalta. Tietoturvan riskejä voidaan kartoittaa laatimalla taulukko josta ilmenee uhka, prioriteetti, vaikutukset ja uhkien ehkäisytapa. Kuvassa yksitoista on esimerkkinä kartoitettu Sammakon tietoturvaan liittyviä uhkia.

Uhka	**Prioriteetti**	**Riski**	**Vaikutukset**	**Ehkäisytapa**
Tiedostojen varastaminen/väärinkäyttö verkon välityksellä	Ylin	Korkea	Taloudelliset, imagolliset	Tietoverkon salausmenetelmät, käyttöoikeudet
Tiedostojen varastaminen fyysisesti	2	Korkea	Taloudelliset, imagolliset	Tallennusvälineiden kryptaus, huolellinen säilytys
Tietoverkon laiterikot	3	Keski	Taloudelliset	Laitteiden dokumentointi, vikaantuneen laitteen korvaaminen, varmuuskopiointi
Onnettomuudet	4	Matala	Taloudelliset	Toipumissuunnitelma
Työntekijä	5	Keski	Taloudelliset, imagolliset	Kouluttaminen, huolellisuus, tietojen käyttöoikeudet, dokumenttien jäljittävyys
Muut uhat: Palvelunestohyökkäykset, virukset,madot verkonkuuntelut, osoitehuijaukset, krakkerit, hakkerit yms.	1-6	Keski	Taloudelliset, imagolliset	Tietoverkon salausmenetelmät, työasemien tietoturvaohjelmistot, kouluttautuminen, fyysinen laiteturva

Kuva 11. Yhteenveto tietoturvariskeistä

Ulkoinen uhka

Ulkoisella uhalla käsitetetään kyseisen yrityksen kannalta tiedon varastamiseen liittyvät uhat. Ne voivat olla hyökkäyksiä yrityksen NAS-palvelimelle tai yrityksen WLAN-verkkoon kohdistuvia väärinkäyttöjä, joilla päästään käsiksi yrityksen tiedostoihin.

Merkittäviä ulkoisia uhkia ovat myös fyysiset ulkoiset uhat. Yrityksen tietoja voidaan varastaa yrityksen toimitiloista esim. julkaisemattomia käsikirjoituksia, tai varastaa vastaavanlaista tietoa yrityksen työntekijältä esim. vapaa-ajalla.

Todennäköisyys tälläiseen uhkaan on kohtalaisen suuri, joten se tullaan priorisoimaan erittäin korkeaksi. Menetyksiä joita uhan sattuessa saattaa aiheutua ovat lähinnä imagollisia, mutta myöskin taloudellisia, riippuen uhan toteutustavasta ja vakavuudesta.

Laiterikot

Laiterikoilla tarkoitetaan Kustannusosakeyhtiö Sammakon tietoturvan osalta sitä, että jokin osa tai laite suunnitellusta tietoverkosta tuhoutuu tai vikaantuu. Pahimmillaan se aiheuttaa työn seisahtumisen ja taloudelliset tappiot. Laiterikkojen sattuessa ylläpidon on toimittava nopeasti, jotta tietoverkko saadaan takaisin entiseen tilaansa. Todennäköisyys laiterikon uhalle on kohtalainen, uhka on erittäin vaikeasti ennustettava ja siksi verkkolaitteiston ylläpidosta pitää huolehtia.

Onnettomuudet

Tahattomat onnettumuudet voivat sattua koska tahansa, pahimmillaan se voi lamaannuttaa koko yritystoiminnan, mutta jo pelkästään tietoverkon lamaantumisen jälkeen voi koitua suuriakin taloudellisia tappioita jos työnteko pääsee seisahtumaan verkon kaatumisen takia.

Yrityksessä ei käsitellä vaarallisia aineita tai tehdä tulitöitä, joten mahdollinen uhka voi syntyä laajemmasta tulipalosta tai vesivahingoista rakennuksen putkistoissa. Uhkaan on varauduttu yrityksen tietoverkon toipumissuunnitelmalla.

Työntekijä

Yrityksessä työskentelee alle 15-työntekijää jotka käyttävät yrityksen tietoverkkoa. On silti mahdollista, että yrityksen sisällä työntekijä tahallisesti tai tahattomasti vuotaa salattuja tietoja yrityksen ulkopuolelle.

Työntekijältä voidaan kalastella tietoja fyysisesti hänen työskennellessään etänä tai henkilö voi osoittautua ennalta-arvaamattomasti tietorikolliseksi.

Skenaarion seuraukset voivat olla erittäin vakavat niin taloudellisesti kuin imagollisesti. Tähän on varauduttu tarkalla autentikoinnilla käyttäjä-tasoilla tietoverkossa ja määritellyillä hallinta-oikeuksilla tiedostoissa.

3.1 Toipumissuunnitelma onnettomuuksien varalle

Kustannusosakeyhtiö Sammakolle olen laatinut seuraavanlaisen toipumissuunnitelman onnettomuuksien varalle. Toipumissuunnitelmalla pyritään helpottamaan tietoverkon toiminnan palauttamista mahdollisen onnettomuuden jälkeen.

Onnettomuuden sattuessa kun kyseessä on tulipalo tai vesivahinko, yrityksen tietoverkko on avainasemassa koko liiketoiminnan kannalta. On erityisen tärkeää, että tilanteessa tehdään oikea arviointi ja toimintaa johtava henkilö on ajantasalla tilanteesta. Toipumissuunnitelma koskee Sammakon kaikkia toimipisteitä ja siitä tullaan tulostamaan kopioita, joita tullaan säilyttämään toimipisteiden seinällä työntekijöiden nähtävillä.

Toipumissuunnitelmaa johtaa *ylin työntekijä* onnettomuuden toteamisen aikana, joka toteaa tilanteen ja jakaa tehtävät toipumissuunnitelman mukaisesti.

Kun todetaan toteutunut onnettomuus joka uhkaa yrityksen tietoverkkoa tai tietoturvaa, edetään Kustannusosakeyhtiö Sammakossa seuraavasti.

1. Todetaan tilanne, jos tilanne vaatii - suoritetaan hätäilmoitus 112.

2. Todetaan mille alueelle onnettomuus on vaikuttanut.

3. Jaetaan vastuu-alueet työntekijöiden kesken (mitä kukin tekee?).

4. Suojataan/siirretään NAS-palvelin, jotta varmuuskopioinnit eivät tuhoudu.

5. Suojataan/siirretään muut tärkeät dokumentit koskien tietoverkkoa, jotta verkon elvyttäminen olisi helpompaa. Suojataan myös muut tärkeät dokumentit oman harkintakyvyn ja tilanteen vakavuuden mukaan.

6. Onnettomuuden ja mahdollisten korjausrakentamisen jälkeen aletaan korjaamaan tietoverkkoa tämän opinnäytteen mukaisen tai sen hetkisen tietoverkkorakenteen mukaan.

3.2 Yrityksen tietoturvan toteutus

Nykyaikana tietoturvallisuus korostuu yhä merkittävämmin jokaisesssa elämän tilanteessa. Yritysmaailmassa tietoturvan ylläpito ja kehitys on erittäin tärkeää. Riittävä tietoturvataso yritysmaailmassa palvelee yritystä ja asiakasta kaksisuuntaisesti. Riittävällä tietoturvalla turvataan yrityksen identiteetti ja ylläpidetään uskottavuutta liikekumppaneiden silmissä. Asiakkaat saavat hyödyn yrityksen tietoturvasta, kun he voivat luottaa siihen, miten asiakkaaseen liittyviä tietoja käsitellään ja säilytetään.

Tietoturvalla suojataan yrityksen tärkeät tiedot ulkopuolisilta. Tietoturva on siis sarja toimenpiteitä jotka takaavat yrityksen tietojen koskemattomuuden. Tietoturva on määritelty kattamaan ainakin seuraavat asiat: tietojen luottamuksellisuus, eheys, kiistämättömyys, pääsynvalvonta, saatavuus ja tarkastettavuus. [3]

Tietojen luottamuksellisuus

Kustannusosakeyhtiö Sammakossa tietojen luottamuksellisuus toteutetaan siten, että tietoihin (tiedostot,asiakirjat) pääsevät käsiksi vain ne, joilla siihen on oikeus. Tämä tullaan toteutetaan siten, että turvattavat asiakirjat säilytetään lukitussa tilassa yrityksen toimipisteissä. Tietoverkossa työntekijät kirjautuvat langattomaan verkkoon kayttämällä annettua salausavainta Service Set ID (SSID), lisäksi jokaisessa tietokoneessa on jokaiselle henkilölle luotu oma käyttäjätili, heille yksilöllisesti määritellyin käyttäjäoikeuksin.

Tiedon eheys

Yrityksessä pyritään jatkossa siihen, että tieto sitä käsiteltäessä ei muutu. Tämä toteutetaan siten, että jokainen sähköinen dokumentti allekirjoitetaan sähköisesti. Lisäksi otetaan käyttöön julkiset epäsymmetriset salausavaimet ja salaiset symmetriset salausavaimet.

Varmuuskopiointi tulee yrityksessä tapahtumaan täysin automaattisesti NAS-palvelimen avulla. Virustorjunnasta tulevaisuudessa tulee vastaamaan F-Securen pk-yrityksille suunnattu tietoturvaohjelmistopaketti.

Tietojen kiistämättömyys

Kustannusosakeyhtiö Sammakon tietoverkko tallentaa reitittimen, tukiasemien sekä muusta verkon toiminnasta lokimerkintöjä, jotka voidaan tarpeen tullessa todeta ja lukea

laitteistojen hallintapaneeleista. Niiden avulla pystytään todistamaan verkon tiedonsiirrossa tapahtuvat muutokset ja tapahtumat.

Pääsynvalvonta tietoturvassa

Yrityksen jokaisella työntekijällä on luotu oma käyttäjätili työaseman käyttöjärjestelmässä. Käyttäjätilien avulla voidaan asettaa tiettyjä tapauskohtaisia rajoituksia verkon ja tiedostojen käyttöön. Tietoverkon palvelimella oleville tiedostoille voidaan asettaa käyttäjärajoituksia (luku, kirjoitus, avaamisoikeus).

Tieturvan kannalta on myös tärkeää, että paperiset dokumentit ja muut asiakirjat tullaan säilyttämään huolellisuutta noudattaen, tarpeen vaatiessa lukitussa paikassa.

Tietojen saatavuus

Yrityksen toimitilojen sisäänkäynnit tullaan pitämään tarpeen vaatiessa lukittuna jotta vältytään mahdollisilta ulkopuolisilta tunkeutujilta. Kaikki tietoverkkoon kuuluvat laitteistot ovat vain yrityksen työntekijöiden käytössä, eikä niitä saa käyttää tai konfiguroida kukaan ulkopuolinen, pois lukien mahdollinen tietoverkon ulkoistettu ylläpito ja huolto.

Tietoverkon NAS-palvelin tullaan suojaamaan lyhyiden sähköverkon katkoksien varalta UPS-laitteella, jolla voidaan varakäyttää palvelinta n. 8-12 minuutin ajan sähkökatkon syntyessä.

Tarkastettavuus

Kustannusosakeyhtiö Sammakossa käsiteltävissä tiedoissa/tiedostoissa tulee pystyä selvittämään ja osoittamaan niiden oikeellisuus. Tämä tullaan toteuttamaan lokimerkintöjen avulla verkkolaitteista, työasemista ja paperisten dokumenttien tulosteiden kirjanpidolla.

Päätelaitteiden autentikointi

Langattomassa lähiverkossa, tarkemmin 802.11-standardeissa käytetään yksinkertaista laitetunnistusta. Yhteyspisteet eli tässä tapauksessa tukiasemat tunnistavat päätelaitteet (esim. tietokoneet) SSID- tunnuksen avulla.

Sammakon WLAN-verkkojen SSID-tunnukseksi valitaan jokin nimi esim. toimipaikan nimi. SSID- tunnus voidaan myös piilottaa reitittimen ja tukiasemien asetuksista, mutta tärkeämpää on valita käytettävä liikenteen salaus.

WLAN-verkon liikenteen salaamiseksi valitaan ne standardit joita tietoverkkoon suunniteltu laitteisto tukee. Tässä tapauksessa Sammakon WLAN-verkko tullaan salaamaan WPA (TKIP) –salauksella.

TKIP (Temporal Key Integrity Protocol) tarkoittaa joukkoa algoritmeja jotka sisältävältävät parannuksia aikaisempaan ja vanhentuneen WEP (Wired Equivalent Privacy) -salauksen tietoturvaan. Tärkeimpiä ominaisuuksia WPA (TKIP) salauksessa ovat 128-bittinen salausavain, alustusvektorien osoiteavaruus (48 bit), ryhmälähetys- ja levitysviestikehysten salausavaimen kierrätys (Broadcast Key Rotation) ja kryptograafisesti vahva sanoman eheyden tarkistus. [2]

Toimipisteiden välisessä tietoverkkojen suojauksessa käytetään laitteistojen ja ohjelmistojen tukemia tekniikoita. Yksi merkittävä tapa suojata langaton lähiverkko on VPN (Virtual Private Network) joka tarkoittaa toteutuksia salata IP-liikenne turvattoman verkon yli, tässä tapauksessa toimipisteiden välinen liikenne internetin yli (LAN-to-LAN).

Sammakon langattomissa verkoissa käytetään yllämainitussa tarkoituksessa IPSec-tekniikkaa (IP Security Architecture).

”VPN voi tarjota lähettäjän tunnistuksen, luottamuksellisuuden ja datan eheyden varmistuksen. IPSec jakaa luottamuksellisuuden, eheyden varmistuksen ja avainten hallinnan eri protokollille.” [2].

3.3 Ohjelmistojen turvallisuus

Yritysmaailmassa ohjelmistoturvallisuuden eräs tärkeä seikka on määritellä mitkä ohjelmistot ovat sallittuja ja mitkä eivät. Kustannusosakeyhtiö Sammakossa käytetään normaalien toimisto-ohjelmien lisäksi joitain lisensöityjä graafisia suunnitteluohjelmia.

Ohjelmistoissa on aina tietoturva-aukkoja, tässä tapauksessa emme voi vaikuttaa niihin, muuten kuin ohjelmien säännöllisellä päivittämisellä. Tärkeää olisi myös, että yrityksessä ei asennettaisi verkossa oleviin koneisiin mitään, mistä ei olla täysin varmoja. Tällä ehkäistään mahdollisten haittaohjelmien leviäminen yrityksen tietoverkon sisällä ja sitä kautta ongelmien syntyminen.

”Ohjelmistoturvallisuudella tarkoitetaan kaikkien käytettävien ohjelmistojen ja sovellusten tietoturvallisuusominaisuuksia ja sen osa-alueet voidaan luokitella aivan kuten laitteistoturvallisuudessa.” [4].

Kustannusosakeyhtio Sammakon ohjelmistoturvallisuus kattaa seuraavat asiat.

- Ohjelmistojen turvallisuus, tässä tapauksessa yrityksessä käytettävät työ-ohjelmat (mm. Photoshop, MS Office, Design-ohjelmat) ja web- selaimet.
- Käyttöjärjestelmien turvallisuus (Windows Vista, Windows 7) ja niiden sisältämät sovellukset.
- Virustorjunta ohjelmat, F-Secure.
- Ohjelmistojen salaportit ja niiden tukkiminen.

Ohjelmistojen turvallisuuden parantamiseksi Sammakossa tullaan käyttämään työasemien käyttöjärjestelmissä uusimpia tietoturvaominaisuuksia sekä laillisia lisensöityjä ohjelmia. Kaikkien sovellusten kohdalla tullaan jatkossa huolehtimaan, että ne ovat ajantasalla sekä tietoturvaohjelmisto on jokaisessa verkkoon kytketyssä tietokoneessa aktiivisena.

Virusuhka on sitä suurempi kun yrityksellä on toimintaa yrityksen ulkopuolisten laitteiden kanssa. Tämä tarkoittaa käytännössä sitä, että esimerkiksi asiakas vierailee yrityksen tiloissa omalla kannettavallaan tai ulkopuolisen USB-muistitikku kytketään johonkin yrityksen tietoverkon sisällä olevaan koneeseen.

Tietoturvan kannalta vaativin asia on ihmisen toiminnan suojaus, sillä harva haittaohjelma leviää ilman ihmisen toimenpiteitä.

4 TIETOVERKON TESTAUS

Tietoverkon testaus kuuluu olennaisena osana tietoverkon suunnittelua. Verkon toimintaa, vakautta ja turvallisuutta mitataan useilla välineillä, joiden antamia tuloksia dokumentoidaan ja verrataan. Koska kyseistä tietoverkkoa ei ole fyysisesti vielä rakennettu, testauksen pitää tapahtua simuloiden ja määrittää miten testaukset tapahtuvat. Testauksella varmistetaan, että verkko toimii halutulla tavalla.

4.1 Toiminnallinen testaus

Toiminnallisessa testauksessa testataan tietoverkon laitteistotason komponentit, joka pitää sisällään tietoverkon laitteet, kaapelit ja ohjelmistot. Toiminnallisessa testauksessa Kustannusosakeyhtiö Sammakon verkkoa kuormitetaan maksimitasolla joka vastaa kaikkien palveluiden samanaikaista käyttöä tietoverkon sisällä. Mittaustuloksista havaitaan verkon vakaus ja sen kyky toimia vaativissa toimintaolosuhteissa.

Verkkolaitteiden testaus tapahtuu tarkastamalla tukiasemien ja reitittimien IP-osoitteet niihin kytketyistä tietokoneista. Yhteyden tila tarkastetaan jokaisesta tietoverkkoon kytketystä tietokoneesta hyvin yksinkertaisella tavalla. Testaaja avaa Windows-käyttöjärjestämän komentorivin, ja lähettää ping-komennolla haluamansa määrän paketteja kohteeseen. Testaustulos on onnistunut jos laite vastaa kutsuun omalla echo reply –paketilla pienellä latenssilla (≥1 ms) ja 0% datamäärän hävikillä.

Tietoverkkoa tullaan testaamaan myös simuloimalla palvelunestohyökkäystä. Palvelunestohyökkäys on hyökkäys jolla aiheutetaan palvelun saannin katkeaminen tai estetään palvelun toiminta. Siinä missä kaikki muutkin tietoverkot, Sammakon tietoverkko kykenee siirtämään vain äärellisen määrän liikennettä tietyssä ajassa. Verkon kapasiteettia testataan simuloiden verkkokapasiteettihyökkäystä, joka on eräs tapa suorittaa palvelunestohyökkäys [1].

Testauksessa lähetetään edellä mainitulla tavalla suuria määriä dataa monesta eri työasemasta ping-komennolla kohdelaitteeseen. Yhteyslaite, esimerkiksi tietoverkon reitin saattaa lamautua, jos liikennetulva kasvaa liian suureksi. Testauksessa dokumentoidaan datamäärä, jolla tietoverkko saatiin lamautettua ja havainnoidaan miten testaustapahtuma vaikutti verkon muuhun toimintaan.

4.2 Määritystenmukaisuustestaus

Määritystenmukaisuustestauksessa verrataan suunniteltua tietoverkkoa sen vaatimusmäärittelyyn. Testauksessa todetaan onko tietoverkko haluttujen vaatimusten mukainen ja toteutuuko alkuperäiset tietoverkkoon asetetetut tavoitteet. Testaus voidaan toteuttaa yksinkertaisesti listaamalla vaatimukset ja tavoitteet, joihin vastataan kyllä tai ei –periaatteella.

5 YLLÄPITO JA DOKUMENTOINTI

Ylläpito Sammakon tietoverkoissa tullaan kehittämään riittävän helpoksi, jotta ylläpito ja ongelmien ratkaisut eivät aina vaadi asiantuntijan apua. Ylläpidon merkitys on erittäin suuri, kun ajatellaan tulevaisuutta ja kustannuksien säästämistä.

Varsinkin langattomissa tietoverkoissa merkittävä uhka on epäviralliset yhteyspisteet joiden määrittely on puutteellista tietoturvan kannalta. [2]

Sammakolla tämä merkitsee sitä, että jokin tietoverkon yhteyspiste käyttää vanhentunutta tekniikkaa, konfigurointi on jäänyt puutteelliseksi tai laite ei täytä tietoverkon tietoturvaominaisuuksia.

Edellä mainittujen ongelmien ehkäisemiseksi tulee paikallistaa ongelmaa aiheuttavat tekijät. Paikallistaminen tapahtuu seuraamalla radio-kanavia eri puolella rakennusta ja verrataan löydettyjen yhteyspisteiden MAC-osoitteita virallisiin laitteiden tietoihin. [2]

Järjestelmällisessä vianhaussa voidaan käyttää hyväksi OSI-mallia. Jolloin vikaa lähdetään ensin paikallistamaan fyysisistä yhteyksistä, jonka jlk. siirtokerroksen laitteiden toiminnasta ja määrittelyistä. Ellei edellä mainittu vianhaku tuota tulosta, edetään verkkokerroksiin, reititykseen ja pääsylistoihin. Liikennetilastot SNMP-verkonhallintaprotokollassa ovat myös erittäin hyödyllisiä vian paikantamisessa. [2]

Kustannusosakeyhtiö Sammakon tietoverkkojen dokumentointi rakennusvaiheessa tulee olemaan tärkeässä asemassa ja sen pitää kattaa ainakin seuraavat asiat.

- Jokaisen tietoverkkoa käyttävän laitteen MAC-osoitteet, tyypit, mallinumerot ja kuvaukset laitteen toimintatavasta
- Reitittimien laitetiedot ja konfiguroinnit, sähköisenä ja paperisena dokumenttina
- Tukiasemien laitetiedot ja konfiguroinnit, sähköisenä sekä paperisena dokumenttina
- NAS-palvelimen laitetiedot ja konfiguroinnit, hot-swap-kiintolevyjen sarjanumerot sekä ohjeet kuinka levyjä voidaan tarpeen tullen vaihtaa fyysisesti
- Helppolukuinen ohjeistus, jolla työntekijät voivat itse varmistaa tietoturvaohjelmiston ajantasaisuuden ja toiminnan.
- Toimitilojen pohjapiirrokset, joihin on merkitty tietoverkon laitteet ja kaapeloinnit

- Luodaan vikaraportti-pohja, johon työntekijä ongelman havaitessaan voi kirjata tietoja ongelmasta
- Jokaisen tietoverkon laitteen ostopaikat ja tiedot ja niiden alkuperäiset ohjekirjat
- Tiedot kehen ottaa yhteyttä ongelmien sattuessa

Kaikkia tietoverkkoihin koskevia dokumentteja tullaan säilyttämään kahtena kappaleena, joista toinen on lukitussa tilassa ja toinen yleisesti yrityksen sisällä nopeasti saatavana. Tietoverkkojen asennuksen ja suuren osan dokumentoinnista tulen tekemään henkilökohtaisesti, joten ulkopuolisia toimeksiantoja ei tarvitse yrityksen hankkia. Olen myös yrityksen käytettävissä mahdollisten ongelmatilanteiden varalta koskien tietotekniikkaa ja tietoturvaa.

6 YHTEENVETO

Opinnäytteeni tarkoituksena oli suunnitella Kustannusosakeyhtiö Sammakolle toimiva, turvallinen ja pääosin langaton tietoverkko eri toimipisteisiin. Tärkeänä asiana oli myös toimipisteiden yhdistäminen, joka toteutettiin tiedostojen jakamisella toimipisteiden kesken. Etätyöskentely sai myös uuden ulottuvuuden, kun tulevaisuudessa etätyöskentelijä pystyy käyttämään NAS-palvelimen toimintoja internetin välityksellä.

Suunniteluprojektini suurimpana tuloksena voidaan todeta, että tietoverkko vastaa siihen asetettuja vaatimuksia ja on toimeksiantajan tapauksessa ensimmäinen suunniteltu tietoverkko. Tietoturva, kuten työni alussa kerroin, ei ollut kovinkaan harkittua eikä tietoturvaan oltu paneuduttu kovinkaan syvällisesti.

Yrityksen tietoverkon rakennuskustannukset tulevat olemaan noin 1400-2000 € luokkaa. Kustannusarvioi perustuu tietoverkon laitteiden, ohjelmistojen ja tarvikkeiden listahintaan verkkokaupoissa. Tarvikkeiden ja varsinkin tietoturvaohjelmiston hankintakustannuksia voidaan vielä kilpailuttaa yrityksestä käsin, jolloin kustannusarvioita tullaan tarkastelemaan uudestaan.

Opinnäytteessä haastavinta oli oikean lähdemateriaalin löytäminen, koska tekniikka kehittyy valtavan nopeasti ja aihealue jota opinnäyte käsitteli oli kohtalaisen suuri. Haasteita aiheutti myös langattomien lähiverkkojen kirjava kokoelma standardeja, mikä aiheuttaa päänvaivaa monelle tietoverkkoa suunnittelevalle.

Opinnäytettä tarkasteltaessa voidaan todeta tietoturvan tärkeys, langattomien tietoverkkojen tietoturva on parantunut viime vuosina uusien tietoturvastandardien myötä. Onkin erittäin tärkeää huolehtia tietoverkkojen päivittämisessä siitä, että tietoturvastandardit ovat päivityksen jälkeen myös ajantasalla.

Tavoite oli myös kirjoittaa mahdollisimman tiivis ja käytännöllinen raportti tietoverkon suunnittelusta. Tekstin teoreettisuuden pyrin pitämään kohtalaisen helppolukuisena, jotta opinnäytteestäni olisi hyötyä mahdollisimman useaan käyttötarkoitukseen. Mielestäni onnistuin tavoitteessani hyvin ja opinnäyte täyttää tehtävänsä. Kuten edellä mainitsin tekniikka kehittyy, joten tätäkin opinnäytettä voidaan kehittää hyvin pitkälle tulevaisuuteen.

Tietoverkkoa ja sen tietoturvaa on jatkossa hyvä parantaa, etenkin tietoverkon tiedonsiirtokapasiteetin osalta. Seuraava kehitysaskel voisi olla nopeampaan 802.11 n-tekniikkaan siirtyminen, mikä tosin edellyttäisi joidenkin laitteiden uusimista.

Muita varteenotettavia kehityskohteita tulevaisuudessa ovat tiedostojaon tallennuskapasiteetin lisäys, verkon laajentaminen toimitilojen mahdollisissa laajennuksissa ja tietokannan luonti yrityksen omalle NAS-palvelimelle.

LÄHTEET

[1] Anonymous, Hakkerin käsikirja. Helsinki: Edita Publishing Oy, 2001.

[2] Puska Matti, Langattomat lähiverkot, Helsinki: Talentum Media Oy, 2005.

[3] [WWW-dokumentti] saatavilla: http://www.internetopas.com/yleistietoa/tietoturva/ (luettu 17.4.2011).

[4] Paavilainen Juhani, Tietoturva. Espoo: Suomen Atk-kustannus Oy, 1998.