Metropolia Ammattikorkeakoulu
Tietotekniikan koulutusohjelma

Anssi Teittinen

Infrastruktuurin, tietoturvan ja tietopalveluiden suunnittelu

Insinöörityö 1.6.2009

Ohjaaja: palvelujohtaja Karo Koskinen
Ohjaava opettaja: lehtori Erik Pätynen

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä	Anssi Teittinen
Otsikko	Infrastruktuurin, tietoturvan ja tietopalveluiden suunnittelu
Sivumäärä	66 sivua
Aika	1.6.2009
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaaja	palvelujohtaja Karo Koskinen
Ohjaava opettaja	lehtori Erik Pätynen

Insinöörityön tavoitteena oli suunnitella ratkaisut projektin asiakkaana toimineen konsultointiyrityksen infrastruktuurin, tietoturvan ja tietopalveluiden tehostamiselle. Tarkoituksena oli luoda näistä kolmesta asiasta kokonaisuus, jolla yrityksen prosessien toimintaa voitaisiin paremmin hallita ja tehostaa.

Suunnittelutyössä otettiin huomioon yrityksen yksilölliset tarpeet ja pyrittiin päätymään ratkaisuihin, jotka kykenevät laajenemaan sekä joustamaan yrityksen kasvun ja organisaatiomuutosten yhteydessä.

Insinöörityössä tutkittiin myös mahdollisuutta käyttää avoimen lähdekoodin tuotteita kustannussäästöjä tuovina tietopalveluratkaisuina. Tällaisia tietopalveluita olivat dokumenttienhallinta-, asiakkuuksienhallinta- sekä sisällönhallintajärjestelmät.

Työn lopputuloksena saatiin dokumentti, jota voidaan käyttää suunnitelmana tai ohjeistuksena asiakasyrityksen infrastruktuurin, tietoturvan sekä tietopalveluiden toteuttamisessa sekä nykyisten järjestelmien toiminnan arvioimisessa.

Hakusanat	tietoturva, infrastruktuuri, tietopalvelut, avoin lähdekoodi

Metropolia University of Applied Sciences **Abstract**

Author Name of Thesis Pages Time	Anssi Teittinen Infrastructure, information security and information systems planning 66 1 June 2009
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Instructor Supervisor	Karo Koskinen, Service Manager Erik Pätynen, Senior Lecturer

The objective of this thesis was to plan solutions for strengthening infrastructure, information security and information services for a consulting company that acted as the client in this project. The intention was to create an ensemble of these three parts, which can be used for strengthening and managing business processes.

In the planning, the client's individual needs were taken into consideration and solutions were pursued that could bend and expand with the growth of the business and during the organization's structural changes.

The thesis also examined the possibility of using open source products as information service solutions that would provide cost savings for the company. These information systems were document management, client relations management and content management systems.

As the outcome of this thesis a document was produced that can be used as a plan or as a set of instructions for implementing infrastructure, information security or information service solutions and for evaluating the functions of the current systems.

Keywords	information security, infrastructure, information services, open source

Sisällys

Lyhenteet

CIFS	Common Internet File System. Protokolla, jota käytetään resurssien jakamiseen lähiverkossa.
CRM	Customer Relationship Management. Asiakkuudenhallinta.
DDoS	Distributed Denial Of Service. Hajautettu palvelunestohyökkäys. Sama kuin DoS, mutta hyökkäys suoritetaan monesta eri lähteestä.
DMS	Document Management System. Sähköinen dokumenttienhallintajärjestelmä Dokumenttien hallintaan.
DoS	Denial Of Service. Palvelunestohyökkäys, jolla hyökkäyksen kohteen toiminta pyritään lamauttamaan.
GNU	GNU's Not Unix. Käyttöjärjestelmä, joka perustuu täysin vapaaseen ohjelmistoon.
GPL	General Public License. Vapaissa ohjelmistoissa käytetty lisenssi.
HTML	HyperText Markup Language. Internetsivustojen tekemiseen käytetty merkitsemiskieli.
IP	Internet Protocol. Protokolla, jota käytetään liikenteen kuljettamiseen pakettikytketyssä verkossa.
LAN	Local Area Network. Lähiverkko.
MAC	Media Access Control. Tietoverkoissa käytettävien laitteiden yksilöllinen tunniste.
MySQL	Avoimen lähdekoodin tietokantaohjelmisto.
OSI	Open Source Initiative. Voittoa tavoittelematon yhdistys, joka pyrkii parantamaan avoimen lähdekoodin näkyvyyttä.
SLA	Service Level Agreement. Palvelusopimus, jolla määritellään vaadittu palvelun taso.
SMB	Server Message Protocol. Protokolla, jota käytetään resurssien jakamiseen lähiverkossa.
SNMP	Simple Network Management Protocol. Verkkolaitteiden valvontaan käytetty protokolla.

SSID	Service Set Identifier. Langattomien lähiverkkojen mainostamiseen käytetty tunniste.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko, jolla voidaan pilkkoa fyysinen lähiverkko pienempiin loogisiin osiin.
VPN	Virtual Private Network. Virtuaalinen yksityisverkko, jolla voidaan turvallisesti yhdistää sisäverkkoja toisiinsa julkisen verkon yli.
WEP	Wired Equivalent Privacy. Langattoman lähiverkon suojaukseen käytetty protokolla.
WLAN	Wireless Local Area Network. Langaton lähiverkko.
WPA2	Wi-Fi Protected Access. Langattoman lähiverkon suojaamiseen käytetty protokolla.

1 Johdanto

Tässä insinöörityössä on tarkoituksena suunnitella tietojärjestelmäinfrastruktuuri ja tietoturvapolitiikka sekä valita toimintaa tukevat tietopalvelut pienelle, mutta nopeasti kasvavalle yritykselle. Keskeisenä tavoitteena on suunnitella tehokas ja joustava, mutta kustannuksiltaan edullinen ympäristö ja tutkia samalla avoimen lähdekoodin soveltuvuutta yrityksen tietopalveluissa.

Työn asiakkaana on kasvava pääkaupunkiseudulla toimiva IT-alan palveluyritys, jonka osaamisalueina ovat projektihallinta, konsultointi ja valmennus. Työ sai alkunsa vuoden 2008 loppupuolella, kun asiakasyritys muutti uusiin toimitiloihin. Työ päättyy tämän dokumentin valmistumiseen, joka toimii suunnitelmana sekä ohjeistuksena infrastruktuurin, tietoturvan ja tietopalveluiden kehittämiselle.

Monet organisaatiot kamppailevat päivittäin riittämättömien tietoteknisten ratkaisuiden kanssa. Aikaisemmin hyvät infrastruktuuriratkaisut ja tietopalvelut ovat organisaation sisällä tapahtuneiden muutosten tai kasvun takia muuttuneet riittämättömiksi ja kömpelöiksi käyttää. Tällainen tilanne voi olla yritykselle todella hankala: Organisaation koosta riippuen uusien järjestelmien suunnittelu, toteutus ja käyttöönotto on kallis ja aikaa vievä prosessi tuotannon ongelmineen sekä pitkine siirtymäaikoineen.

Tämän työn tavoitteena oli suunnitella asiakasyritykselle ympäristö, jossa edellä mainitut ongelmat on pyritty ottamaan huomioon. Työn päätavoitteet olivat seuraavat:

- parantaa infrastruktuurin kapasiteettia ja laajennettavuutta
- parantaa dokumenttien-, asiakkuuksien- ja sisäisen informaation hallintaa
- tutkia voidaanko kustannuksia pienentää sekä joustavuutta parantaa käyttämällä tietopalveluissa avoimeen lähdekoodin perustuvia palveluita sekä ohjelmistoja
- kehittää tietoturvaa.

Suunnittelutyön haasteena oli luoda tietoturvasta, infrastruktuurista ja tietopalveluista kokonaisuus, jolla yrityksen toimintaa voidaan tehostaa. Toiminnan tehostamisen lisäksi

uuden ympäristön tulisi myös kestää organisaation rakenteellisia muutoksia ja saavuttaa kohtalainen elinikä siedettävillä kustannuksilla.

2 Työn lähtökohdat

2.1 Asiakasyritys

Yrityksen liiketoiminta on hyvin asiakaspainotteista, joten suurin osa työstä tapahtuu suoraan asiakkaalle tehtävän työn muodossa.

Monet asiakasprojekteista tehdään yhteistyössä pääkaupunkiseudun ulkopuolelta toimivan tytäryrityksen kanssa. Tytäryrityksen liiketoiminta keskittyy avoimen lähdekoodin ohjelmistoihin, sillä on pääkaupunkiseudulla paljon työtehtäviä omissa asiakasprojekteissa tai emoyhtiön hankkeissa. Ollessaan työtehtävissä pääkaupunkiseudulla tytäryhtiön työntekijät työskentelevät emoyhtiön tiloissa.

Molemmilla yrityksillä työntekijöiden etätyöntarve on suuri. Työ on usein projektiluontoista eivätkä projektiryhmien jäsenet useinkaan työskentele yhtä aikaa samoissa tiloissa, mikä tekee informaation ja työn sujuvasta jakamisesta vaikeaa.

2.2 Tietoturvan jaottelu

Tietoturvalla tarkoitetaan tiedon ja tietojärjestelmien suojaamista erilaisilta uhkatilanteilta, kuten esimerkiksi luvattomalta käytöltä tai tuhoutumiselta [3].

Asiakasyrityksellä, kuten kaikilla yrityksillä, on paljon tärkeää informaatiota, joka tulee suojata asianmukaisesti. Tietoturvan merkitys on yrityksen toiminalle suuri: se ohjaa monia yrityksen sisäisiä toimintatapoja sekä takaa yrityksen toiminnan jatkuvuuden. Suuri tietomenetys voi olla kova paikka monelle yritykselle, sillä vain noin puolet vakavan tietomenetyksen kokevista yrityksistä ovat enää toiminnassa pari vuotta menetyksen jälkeen. [4.]

Asiakasyritykselle tulee luoda tietoturvapolitiikka, jossa otetaan huomioon yrityksen liiketoiminnalliset tarpeet. Tietoturvapolitiikka tulee määritellä tarvittavat

tietoturvamekanismit, joilla voidaan parantaa seuraavien asiakasyrityksen kohteiden turvallisuutta ja varmistaa yrityksen toiminnan jatkuvuus. Tietoturvan suunnittelussa voidaan käyttää seuraavaa jaottelua [5]:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- järjestelmien turvallisuus.

Asiakasyritykselle tulee luoda tietoturvapolitiikan määrittelyasiakirja, joka voi olla yksi tai kokoelma useampia asiakirjoja, joissa määritellään turvamekanismit edellä mainituille kohteille.

Tietoturvan toteuttamista ja määräysten noudattamista varten tulee määritellä valvontamekanismeja toteutettujen tietoturvamekanismien tehostamiseksi.

2.3 Tietopalveluiden jaottelu

Tietopalvelut koostuvat kaikista niistä organisaation järjestelmistä, joilla käsitellään organisaation informaatiota tai dataa. Yleensä näillä järjestelmillä tarkoitetaan sovelluksia, jotka tallentavat tietoa ja jollain asteella automatisoivat niiden prosessointia.

Asiakasyritys tarvitsee tietopalveluihinsa järjestelmät, joilla voidaan parantaa sähköisten dokumenttien, asiakkuuksien ja yrityksen sisäisen informaation hallintaa ja turvallisuutta.

Tietopalveluita tarvitaan pääasiassa asiakasyrityksen omassa tietoverkossa, mutta työntekijöiden on myös päästävä ulkoverkosta palveluihin käsiksi ilman tietoturvan vaarantamista.

Dokumenttien hallinta

Tarjousprosessien, markkinointimateriaalien, viralliset käyttöohjeiden ja dokumentaatioiden tekeminen tuottaa asiakasyritykselle paljon sähköisiä dokumentteja. Usein yhden dokumentin luomisessa saattaa olla mukana useita henkilöitä. Tämä aiheuttaa riskin päällekkäisestä työstä ja saattaa aiheuttaa dokumenttien eri versioiden sekaantumisen. Lisäksi tämänkaltainen työskentelytapa vaatii sähköisten dokumenttien hyvää saatavuutta.

Asiakasyritys tarvitsee järjestelmän, joka tuo parannusta sähköisten dokumenttien elinkaareen, hallittavuuteen, turvallisuuteen ja saatavuuteen.

Korjauksia tarvitaan etenkin seuraaviin ongelmiin:

- *Dokumenttien käyttöoikeuksien hallinta*, jolla varmistetaan, että kaikki työntekijät eivät saa päästä käsiksi kaikkiin yrityksen dokumentteihin.
- *Päällekkäisen työn estäminen*, jolla estetään kahden eri henkilön samaan dokumenttiin tekemän päällekkäinen työ.
- *Elinkaaren hallinta*, jonka avulla pystytään hallitsemaan dokumentin elinkaari luonnista aina poistamiseen saakka.
- *Web-käyttöliittymä*, jolla järjestelmään voidaan tallentaa ja sieltä ladata dokumentteja web-selaimen kautta.
- *Windows levyjako*, jolla järjestelmään voi tallentaa ja sieltä ladata dokumentteja samalla tavoin kuin windows-verkossa jaetulta levyltä.
- *Metatiedon tallennus*, jolla dokumentteihin voidaan liittää ja tallentaa dokumenttia kuvaavaa tietoa.

Järjestelmän tulee olla kapasiteetiltaan riittävä hallitsemaan jopa suuria määriä dokumentteja, lisäksi sen on tuettava ainakin yleisempiä tiedostoformaatteja.

Sisäisen informaation hallinta

Useiden projektien yhteydessä syntyy paljon informaatiota, jota ei tarvita projektin tai tuotteen virallisessa dokumentaatiossa. Tällainen informaatio saattaa silti olla hyödyllistä yrityksen sisällä, esimerkiksi tulevissa projekteissa.

Tällaista informaatiota ovat esimerkiksi asennusohjeet kehitysympäristöille, tieto tiettyihin teknologioihin liittyvistä ongelmatilanteista tai linkit hyödyllisille internet-sivustoille.

Myös projektiryhmät tarvitsevat tämänkaltaista järjestelmää informaation välittämiseen ja tallentamiseen projektien aikana.

Sisäisen informaation hallintaan asiakasyritys tarvitsee järjestelmän, jossa on seuraavanlaisia ominaisuuksia:

- *Web-pohjainen käyttöliittymä*, joka mahdollistaa järjestelmän käyttämisen web-selaimen kautta.
- *Käyttäjienhallinta*, jolla voidaan hallita ja rajoittaa palveluun pääseviä henkilöitä.
- *Oman sisällön ja sivujen luonti*, jolla mahdollistetaan uusien sivujen ja niiden sisällön luominen kaikille käyttäjille.

Asiakkuuden hallinta

Asiakkuuksien hallinnan parantamiseen tarvitaan asiakkuudenhallintajärjestelmä (Customer Relationship Management, CRM), jolla asiakaskontaktien hallintaa sekä myynnin toimintaa voidaan tehostaa.

Tarpeet asiakkuudenhallintajärjestelmän ominaisuuksille ovat seuraavat:

- *Asiakasrekisteri*, joka mahdollistaa asiakkaiden ja heidän kontaktitietojensa tallentaminen järjestelmään.
- *Jaettu kalenteri*, josta näkee henkilöiden sovitut tapaamiset ja menot, jotta vältyttäisiin päällekkäisiltä varauksilta.

2.4 Infrastruktuurin osat

Infrastruktuurilla tarkoitetaan kaikkia niitä asiakasyrityksen fyysisiä rakenteita, joita tarvitaan yrityksen toimintaan. Se on kokonaisuus, joka muodostuu yrityksen toimitiloista, sähköverkosta, tietoverkon kaapeloinnista, palvelimista ja työasemista. [1.]

Joustava ja kapasiteetiltaan riittävä infrastruktuuri tarjoaa vakaan pohjan organisaation toiminnalle.

Alla on esitelty infrastruktuurin eri osat.

Toimitilat ja sähköverkko

Toimitiloilla tarkoitetaan yrityksen toimistoa tai muuta yrityksen omistamaa kiinteistöä jota pääasiassa käytetään työskentelyyn henkilöstön toimesta. Toimitilat tarvitsevat myös sähkönsyötön, jotta siellä työskentely olisi mahdollista.

Toimitilojen ja sähkönsyötön osalta tulisi ainakin seuraavat asiat ottaa huomioon:

- toimitilan kunnossapito
- vakaa ja kapasiteetiltaan riittävä sähköverkko
- ovet ja lukitukset ulkopuolisten pääsyn estämiseksi
- sammutusjärjestelmä
- hätävalaistus sähkökatkosten varalta

Tietoverkko

Tietoverkkoa voidaan pitää organisaatioiden infrastruktuurissa erittäin tärkeänä osana. Tietoverkko koostuu kaapeloinneista, verkkolaitteista (kytkimet, reitittimet, palomuurit) sekä yhteyksistä ulkomaailmaan. Yrityksen tietoverkkoa voi olla hankala määritellä fyysisesti, koska virtuaalisten yksityisverkkojen (Virtual Private Network, VPN) ansiosta voi tietoverkko olla levinnyt suurellekin maantieteelliselle alueelle.

Asiakasyrityksen tiloissa tulee olla liitännät vähintään 40 kiinteälle työasemalle sekä suojattu langaton lähiverkko (Wireless Local Area Network, WLAN) kannettaville työasemille ja muille mobileille laitteille. Tietoverkkoon tarvitaan myös suojattu pääsy ulkoverkon puolelta, jotta liikkuvat työntekijät voivat toimitilojen ulkopuolelta päästä käsiksi resursseihin ja palveluihin.

Verkon liikenne koostuu pääasiassa sähköposti- ja www-liikenteestä, joten liikennemäärät ovat kohtuullisia. Tietoverkon kapasiteetin tulee siis olla riittävä tavanomaisten internet-palveluiden käyttämistä varten.

Työasemat

Työasemilla tarkoitetaan kaikkia niitä pöytäkoneita ja kannettavia tietokoneita, joita asiakasyrityksen työntekijät käyttävät työskentelyyn.

Työasemille tarvitaan selkeät normit, jotka niiden on täytettävä ennen kuin ne voidaan ottaa käyttöön. Työasemille tarvitaan myös selkeät standardit käyttöönottoon, hallintaan ja käytöstä poistamiseen.

Palvelimet

Palvelimet ovat tietokoneita, joiden pääasiallinen tehtävä on suorittaa palveluita muille tietokoneille. Tällaisia palveluita voivat esimerkiksi olla web-sivujen tarjoaminen tai tiedostojen varastointiin ja hallintaan liittyvät palvelut. [2.]

Asiakasyrityksen palvelimien tulee olla tehokkuudeltaan riittäviä tarjoamaan haluttuja tietopalveluita. Palvelimet tarvitsevat laitetilan, jossa niiden toiminta voidaan taata ja jossa niiden fyysinen turvallisuus on huomioitu.

Lisäksi on määriteltävä vaatimukset saatavuudelle, vikatilanteiden vasteajoille sekä varmuuskopiolle, jotka palvelinlaitteistojen on täytettävä.

3 Avoin lähdekoodi

3.1 Avoimen lähdekoodin historia

Ennen Open Source (avoin lähdekoodi) -käsitteen syntymistä vastaavia ohjelmistoja kutsuttiin vapaiksi ohjelmiksi (Free Software). Vapaan ohjelmiston määritelmän loi 1980-luvulla Richard Stallman. Stallman oli jo aikaisemmin käynnistänyt GNU (GNU's Not UNIX) -hankkeen, jonka tarkoituksena oli kehittää vapaa käyttöjärjestelmä joka on siirrettävissä konetyypistä toiseen. [6; 7. s. 8–9.]

Suojatakseen GNU -hankkeen ohjelmistoidensa vapauden, hän julkaisi Copyleft käyttäjänoikeudet, joissa kiellettiin ohjelmiston ehtojen muuttaminen. Copyleft:n keskeinen idea oli sallia ohjelmiston kopiointi, muuntelu ja muunnellun ohjelmiston levittäminen kaikille. [6; 7. s. 9.]

Vuonna 1985 GNU-projektin kasvaessa Stallman perusti Free Software Foundationin rahoittamaan sekä tukemaan GNU-projektin periaatteiden mukaisia käyttäjien oikeuksia. [6.]

Avoimen lähdekoodin käsite syntyi alkuvuodesta 1998, kun joukko avoimen lähdekoodin hakkereita kokoontui strategiakokoukseen Kaliforniassa, jossa keskusteltiin vapaan ohjelmiston tulevaisuudesta. [8.]

Netscape oli samaan aikaan julkaisemassa oman internet selaimensa lähdekoodia, joten hetki koettiin sopivaksi yrittää saada myytyä vapaan ohjelmiston ideaa myös yritysmaailmaan. Tätä varten tarvittiin uusi käsite, koska Richard Stallmanin kehittämä termi "Vapaa ohjelmisto" oli kerännyt itselleen jokseenkin moralisoivan ja välillä hiukan negatiivisenkin maineen, jota yritykset vieroksuivat. [8; 7. s. 11.]

Open Source -käsitettä tukemaan luotiin voittoa tavoittelematon Open Source Initiative, jonka tehtävänä on hallinnoida ja tuoda esille avoimen lähdekoodin määritelmää. [8.]

3.2 Avoimen lähdekoodin määritelmä

OSI kehitti avoimen lähdekoodin vaatimukset, jotka kaikkien avoin lähdekoodi -termiä käyttävien ohjelmien lisenssien tulee täyttää [9].

- Lisenssi ei saa rajoittaa mitään osapuolta myymästä tai antamasta ohjelmistoa useista eri lähteistä kootun ohjelmistokokonaisuuden komponenttina. Lisenssi ei saa vaatia myynnistä tekijänpalkkiota tai muuta maksua.
- Ohjelman täytyy sisältää lähdekoodi, ja sen levittäminen täytyy olla mahdollista lähdekoodina tai käännetyssä muodossa. Tilanteet, joissa ohjelman jotain muotoa levitetään ilman lähdekoodia, on lähdekoodi oltava saatavissa kohtuullisilla kustannuksilla, mieluiten ilmaiseksi ladattavissa internetistä. Lähdekoodi täytyy olla jossain suositellussa muodossa jotta ohjelmoija voi muokata ohjelmaa. Lähdekoodin tarkoituksellinen monimutkaistaminen ei ole sallittua.
- Lisenssin täytyy sallia muokkaukset sekä johdannaiset työt. Lisenssin täytyy myös sallia niiden levitys samoilla ehdoilla kuin alkuperäisen ohjelmiston lisenssin.
- Lisenssi voi rajoittaa lähdekoodin levitystä muokatussa muodossa vain silloin, mikäli lisenssi sallii korjaustiedostojen sekä niiden lähdekoodin levittämisen. Korjaustiedostojen tarkoituksena on alkuperäisen ohjelmiston muokkaaminen kääntämisen aikana.
- Lisenssi ei saa diskriminoida henkilöitä tai ryhmiä.
- Lisenssi ei saa kieltää ohjelman käyttämistä jollain tietyllä toimialalla.
- Ohjelmaan liitettyjen oikeuksien täytyy sopia kaikille, joille ohjelma on levitetty, ilman että heidän tarvitsee ottaa käyttöön mitään muuta lisenssiä.
- Ohjelmaan liitetyt oikeudet eivät saa olla riippuvaisia siitä, onko ohjelma osana jotain muuta ohjelmistokokonaisuutta. Mikäli ohjelma erotetaan kokonaisuudesta ja sitä käytetään sekä levitetään samojen lisenssitermien alla, kaikilla tahoilla, jotka ohjelmaa käyttävät, on samat oikeudet kuin niillä, jotka käyttävät ohjelmaa osana jotain muuta ohjelmakokonaisuutta.

- Lisenssi ei saa asettaa rajoituksia muille ohjelmille, joita levitetään lisensoidun ohjelmiston kanssa.
- Lisenssi ei saa ennalta rajoittaa käytettäviä teknologioita.

3.3 Avoimen lähdekoodin käyttö yritysmaailmassa

Avoimen lähdekoodin käyttö yritysmaailmassa on voimakkaasti lisääntymässä. Linux ja UNIX tosin ovat jo pitkään olleet yritysmaailmassa mukana lähinnä palvelinalustoina, mutta nykyisin useat avoimeen lähdekoodin perustuvat tietopalveluratkaisut ovat tekemässä läpimurtoa. Monet suuret yritykset ovat ottaneet avoimen lähdekoodin osaksi tietoteknisiä ratkaisujaan ja lisäksi monet muut harkitsevat vakavasti Open Source -tuotteiden käyttöönottoa.

Yksi merkittävimmistä eroista avoimen ja suljetun lähdekoodin välillä on se, että avoimen lähdekoodin tuotteen toimittaja ei usein omista toimittamaansa ratkaisua [10].

Yrityksille avoin lähdekoodi on aikaisemmin tarjonnut pääasiassa säästöjä lisenssikustannuksissa, koska ohjelmat ovat olleet ilmaisia tai maksaneet vain murto-osan verrattuna suljetun lähdekoodin kilpailijoihinsa.

Nykyään avoimen lähdekoodin ohjelmistot pystyvät kilpailemaan suljetun lähdekoodin kanssa myös ominaisuuksillaan [9]. Monet kaupalliset avoimen lähdekoodin projektit, kuten MySQL ja Red Hat ovat hyvin menestyneitä sekä kilpailevat täysiverisesti suljettujen kilpailijoidensa kanssa [11; 12].

3.4 Avoimen lähdekoodin kaupallisuus

Useiden avoimen lähdekoodin kaupallisten ratkaisujen tekijöillä on tuotteestaan kaksi eri versiota. Yhteisöversio (Community) on todellinen avoimen lähdekoodin tuote, jonka lähdekoodit ovat ilmaisesti jaossa ja jonka kehittäminen tapahtuu tuotteen ympärille kerääntyneen yhteisön ja yhteistyökumppaneiden voimin.

Kaupallisista toimintaa varten on maksullinen enterprise versio, joka eroaa community-versiosta lisenssiehtojensa ja ominaisuuksien puolesta [13, s.13]. Enterprise-version toiminnallisuudet valitaan jo yhteisöversioon hyväksytyistä ominaisuuksista. Valitut ominaisuudet ovat myös perusteellisemmin testattuja ja dokumentoituja valmistajan taholta. Tästä syystä tuotteen kaupallinen versio on yleensä ominaisuuksiltaan yhteisöversiota rajatumpi.

Maksullisessa enterprise-versiossa käytetään siis erilaista lisenssiä kuin ilmaisessa community versiossa. Enterprise-version lisenssimaksuun kuluu yleensä itse tuotteen lisäksi myös tuotteen tukipalveluilta lisenssin voimassaoloajaksi.

Vaikka community-versio onkin ilmainen ja ohjelmisto on todettu hyväksi, on enterprise version hankkiminen kannattavaa, sillä ilman kunnollista tukea voi community-version käyttöönotto tulla maksamaan saman verran tai enemmän enterprise-versioon nähden.

3.5 Avoimen lähdekoodin edut ja haitat

Avoimessa lähdekoodissa, kuten suljetussakin, on omat etunsa ja haittansa. Avoimen lähdekoodin etuihin voidaan laskea vahva yhteisöllisyys, halvemmat lisenssikustannukset, ohjelmiston vapaa muokattavuus sekä johdannaisten ohjelmistojen tekeminen. Tilanne, jossa tuotteen toimittaja ei omista tuotetta, antaa mahdollisuuden tuotteen jatkokehittämiselle jonkin toisen toimittajan toimesta.[7. s. 14; 10.]

Yhteisöllisellä kehittämisellä voidaan tuotteen kehittämiskustannuksia laskea. Mikäli tuote kasvattaa suosiotaan, sen ympärille rakentuu yhteisö ihmisistä, jotka muokkaavat ja tekevät ohjelmaan uusia ominaisuuksia omien tarpeidensa mukaan. Tekemänsä työn he jakavat muun yhteisön kanssa. Tuotteen omistaja voi lisätä näitä yhteisön tekemiä muutoksia tuotteen virallisiin versioihin. Tällä tavoin tuotteen valmistuskustannuksetkin ovat alhaisempia.

Lähdekoodien avoimella jakamisella voidaan myös välttyä yhteen tiettyyn valmistajaan tai toimittajaan lukkiutumisesta (Vendor Lock-in), koska lähdekoodit ovat kaikkien saatavilla ja ohjelmistoa käyttävä organisaatio voi jatkaa ostamansa tuotteen kehittämistä vaikka itse. [13. s. 12]

Ohjelmiston vapaa muokattavuus ja johdannaisten projektien salliminen tarkoittaa, että kuka tahansa voi ottaa olemassa olevan projektin lähdekoodit ja lähteä jalostamaan siitä kokonaan uutta tuotetta. Esimerkiksi ottamalla pohjaksi kaksi avoimen lähdekoodin tuotetta ja yhdistää ne yhdeksi isommaksi kokonaisuudeksi. Tämä helpottaa ja nopeuttaa uusien ratkaisuiden syntymistä, koska työtä ei aina tarvitse aloittaa alusta. [9.]

Etuna voidaan pitää myös avoimen lähdekoodin joustavuutta ja läpinäkyvyyttä. Hankittua ohjelmistoa tai järjestelmää voidaan tarpeen tullen muokata. Suljetun lähdekoodin tapauksessa tämä ei ole mahdollista ja siinä tapauksessa organisaatiolla on edessään uuden, korvaavan, ohjelmiston hankkiminen.

Avoimen lähdekoodin huonoihin puoliin voidaan lukea kunnollisen takuun ja tuen puute. Puutteellinen dokumentointi saattaa hidastaa käyttöönottoa ja käyttöä. Lisäksi monien lisenssien sisällössä on vielä paljon epäselvyyksiä ja tulkinnanvaraisuuksia. [7. s. 15.]

Puutteellinen dokumentointi saattaa kasvattaa ohjelmiston käyttöönottoon tarvittavaa aikaa ja näin ollen lisätä kustannuksia. Lisäksi dokumentoinnin puutteellisuus vaikuttaa suoraan myös käytettävyyteen [7. s. 16—18]. Ominaisuudet ovat yleensä usean eri tahon tekemiä, joten yhtenäistä, ohjelman kokonaisuutena kattavaa käyttöohjetta ei välttämättä ole [7. s. 17]. Kaupallisissa projekteissa nämä asiat ovat yleensä korjattu tarjoamalla jo edellä mainittua enterprise-versiota tuotteesta. Hintansa puolesta nämä maksulliset versiot ovat kuitenkin suljettuja ohjelmistoja halvempia.

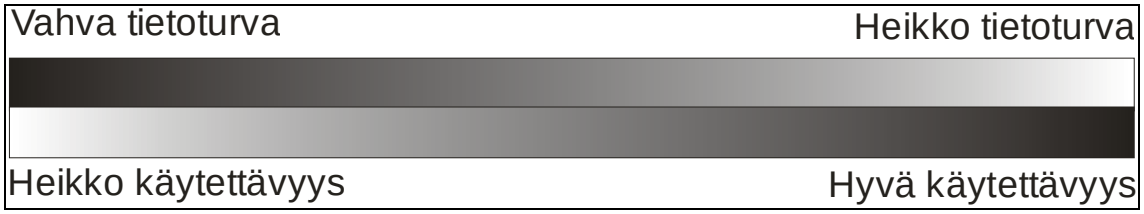
4 Tietoturva

Yksi organisaatioiden tärkeimmistä kohteista eri liiketoimintakohteiden tavoin on tieto. Tietoverkkojen kasvaessa tiedon välittäminen on helpompaa, mutta samalla se myös altistaa tiedon sekä yrityksen henkilöstön ja laitteiston useammille uhkille ja haavoittuvuuksille. Tietoturvalla pyritään suojaamaan nämä kohteet tarkoituksena varmistaa yrityksen toiminnan jatkuvuus. Tietoturvalla voidaan myös pyrkiä minimoimaan liiketoiminnallisia riskejä sekä maksimoimaan liiketoiminnan mahdollisuuksista saatu tuotto. [14. s. 4; 15. s. 14.]

Tietoturvallisuus saavutetaan suorittamalla toimenpiteitä ja mekanismeja, joilla on tarkoitus suojata organisaatiolle tärkeitä kohteita erilaisilta uhkatilanteilta. Näitä uhkatekijöitä voivat olla muun muassa onnettomuudet, sabotaasi, vakoilu, haittaohjelmat tai krakkerointi. Keskeisiä mekanismeja tietoturvalle ovat tietosuoja ja henkilötietojen yksityisyys, organisaation tallenteiden suojaaminen sekä aineettomat oikeudet. [15. s. 14.]

Vaikka organisaatioon kohdistuvia uhkia ei voida koskaan täysin poistaa, näillä tietoturvamekanismeilla pyritään uhkien aiheuttama riski minimoimaan hyväksyttävälle tasolle.

Tietoturva itsessään on yksi tämän suunnittelutyön tärkeimmistä osista, sillä se integroituu tiiviisti infrastruktuuriin ja suunniteltaviin tietopalveluihin. Tietopalvelut, työasemat, palvelimet, tietoverkot ja henkilöstö kuuluvat kaikki osaksi niitä yrityksen elimiä, jotka ovat asiallisesti suojattava mahdollisilta uhkilta. Lisäksi tietoturva vaikuttaa suorasti yritysten järjestelmien ja prosessien käytettävyyteen, kuten kuvassa 1 on esitelty: Tiukat tietoturvasäännöt vaikuttavat negatiivisesti käytettävyyteen ja helposti käytettävät järjestelmät eivät välttämättä ole niin tietoturvallisia. Esimerkiksi täysin suojaamattoman järjestelmän käyttö on helppoa, mutta kun järjestelmään lisätään vaatimukseksi käyttäjän tunnistaminen käyttäjätunnuksella ja salasanalla, tuo se välittömästi käytettävyyteen yhden mutkan lisää. [16. s. 49.]

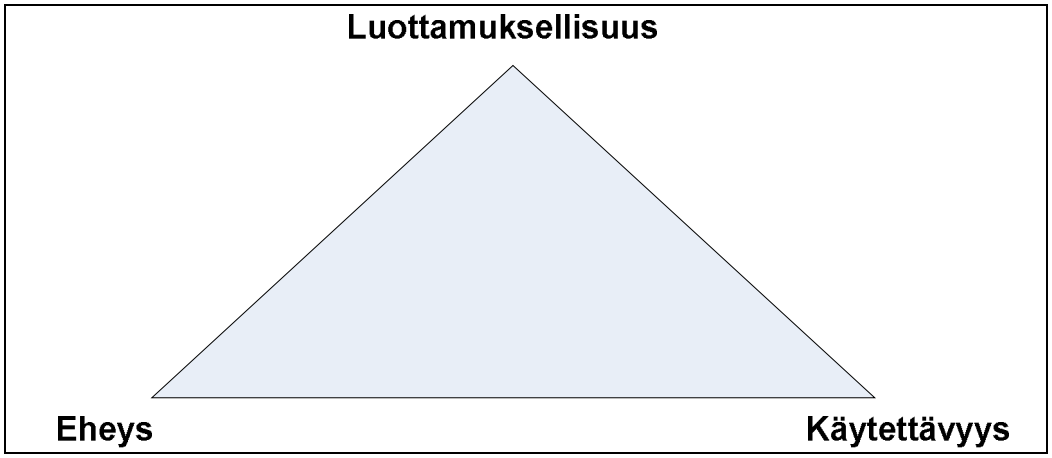


Kuva 1. Tietoturvan ja käytettävyyden välinen riippuvuus.

Tietoturva voidaan jakaa kolmeen perusperiaatteeseen. Kaikki valvonta- ja turvamekanismit sekä uhat ja haavoittuvuudet liittyvät näihin kolmeen asiaan [14. s. 3]:

- *Luottamuksellisuus t*arkoittaa tietojen tahallisen tai tahattoman paljastumisen ja muokkaamisen estämistä, sekä tietojen käsittelyoikeuksien hallintaa.
- Käsitteellä e*heys* taataan, että vain valtuutetut henkilöt tekevät tietoihin ainoastaan luvallisia muutoksia ja että tiedot ovat sisäisesti yhdenmukaisia eivätkä ristiriidassa keskenään. Myös tietojen ulkoinen eheys on taattava, eli sisäisten tietojen on oltava yhdenmukaisia ulkomaailman kanssa.
- *Käytettävyydellä* taataan, että informaatio ja resurssit ovat aina saatavilla niitä tarvitseville henkilöille.

Kuvassa 2 on esitelty luottamuksellisuuden, eheyden sekä käytettävyyden välinen riippuvuus.



Kuva 2. *Kolme suurta. Luottamuksellisuus, Eheys ja Käytettävyys [14,s.3].*

Tietoturva itsessään on prosessi, eikä sen kehittäminen ja toteuttaminen saa loppua, kun sen hetkiset määritelmät on saavutettu. Tietoturva ja erilaiset organisaatiota uhkaavat uhkatilanteet muuttuvat, poistuvat ja lisääntyvät kaiken aikaa, siksi yrityksen asiakasyrityksen tietoturva käytäntöjä ja mekanismeja on katselmoitava tasaisin väliajoin tietoturvan riittävyyden sekä kehittämisen kannalta.

4.1 Hallinnollinen turvallisuus

Hallinnollisella turvallisuudella tarkoitetaan organisaation hallinnon käytössä olevia välineitä riskien toteutumisen pienentämiseen sekä niiden käsittelyyn [5. s. 48].

Välineet, kuten riskianalyysi ja riskien käsittely, tietojen luokittelu, roolien sekä roolien ja vastuiden jakaminen, antaa hallinnolle enemmän ymmärrystä organisaatiota kohtaavista uhkatilanteista, niihin varautumisesta sekä tuo parempaa hallintaa haluttujen mekanismien toteuttamiselle ja ylläpidolle.

Perustana hallinnolliselle turvallisuudelle on tietoturvapolitiikka ja sen määrittelyasiakirja, jossa määritellään yllä mainitut asiat sekä erilaisten mekanismien toteuttaminen. [5. s. 48.]

Roolit ja vastuut

Yrityksen henkilöstölle tulee määritellä tietoturvaroolit ja näiden roolien vastuut tulee määritellä osaksi yrityksen tieturvaa [15. s. 58].

Asiakasyrityksellä tulee käyttää seuraavaa roolijakoa henkilöstön tietoturvavastuiden jakamiseksi [14. s. 15]:

- *Hallinto* vastaa viime kädessä tietoturvasta. Se tekee päätökset toimenpiteistä ja delegoi ne eteenpäin.
- *Tietoturva-ammattilaiset* vastaavat tietoturvan käytännön toteuttamisesta, ylläpidosta ja suunnittelemisesta.

- *Omistaja* on ensisijaisesti vastuussa omistamansa tiedon oikeasta luokittelusta sekä tiedon ulkoisesta ja sisäisestä eheydestä.
- *Käyttäjä v*astaa yrityksen tietoturvapolitiikassa esitettyjen määräysten noudattamisesta päivittäisessä työssään.

Tietojen luokittelu

Nykyaikana pienetkin yritykset omistavat suuret määrät informaatiota varastoituna eri formaateissa. Tietojen luokittelun tavoitteena on varmistaa, että näiden suojattavien tietojen suojaus on riittävä. Luokittelussa lähdetään liikkeelle siitä, että kaikki tiedot eivät ole organisaatiolle yhtä tärkeitä. Esimerkiksi organisaation pikkujoulujen järjestämistä käsittelevä muistio ei varmasti ole yhtä kriittistä tietoa kuin esimerkiksi asiakasrekisteri tai johtoryhmän pöytäkirjat. [14. s. 3; 15. s. 54.]

Luokittelemalla tiedot niiden tärkeyden sekä arvon mukaisesti voidaan tukea tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä. Luokittelulla myös saadaan suojaus- ja valvontamekanismeista kustannustehokkaampia. [14. s. 5.]

Asiakasyrityksen tietojen luokitteluun tullaan käyttämään CCISP-sertifikaattiin perustuvaa yksityisen sektorin luokittelua [14. s. 7]:

- *Julkinen*. Tiedot jotka eivät sovi muihin ryhmiin. Näiden tietojen paljastuminen ei ole haitallista yritykselle.
- *Arkaluontoinen.* Korkeampi luokittelu kuin tavallisella julkisella tiedolla. Tietojen luvaton muuttaminen ei aiheuta luottamuksellisuuden tai eheyden menettämistä.
- *Yksityinen*. Henkilökohtaisia tietoja pelkästään yrityksen sisäiseen käyttöön. Tietojen paljastuminen voi vahingoittaa yrityksen henkilökuntaa.
- *Luottamuksellinen.* Vain yrityksen sisäiseen käyttöön. Tietojen paljastaminen on kielletty tietosuojalailla. Tietojen paljastumisella voi olla vakava vaikutus yrityksen toimintaan.

Tietojen luokittelusta vastaa aina ensisijaisesti tiedon omistaja. Yrityksen hallinto hyväksyy tehdyt luokittelut, mutta voi myös muuttaa niitä, mikäli niin parhaakseen näkee. Tiedon luokittelua voidaan myös muuttaa jälkikäteen, joko ennalta määritetyn aikarajan jälkeen tai erikseen asiakasyrityksen hallinnon hyväksymänä.[14. s. 14–15.]

Tiedoille käytetään myös kriteereitä määrittelemään tietojen luokittelun tarve [14. s. 8]:

- *Arvo.* Tieto on luokiteltava, mikäli se on yritykselle jollain tavalla arvokasta.
- *Ikä.* Tietojen luokittelua voidaan alentaa, mikäli niiden arvo laskee ajan kuluessa.
- *Kelvollinen käyttöaika.* Tiedon luokitusta voidaan laskea, mikäli se vanhenee uudemman tiedon ilmestymisen takia.
- *Henkilökohtainen yhteys.* Tiedot on luokiteltava, mikäli ne liittyvät henkilökohtaisesti yhteen tai useampaan henkilöön.

Riskianalyysi

Riskianalyysillä pyritään systemaattisesti tunnistamaan sekä yksilöimään riskit sekä määrittelemään niiden suuruus. Analyysin tulisi ottaa huomioon yrityksen olennaiset tavoitteet ja asettaa riskit tärkeysjärjestykseen suhteessa näihin tavoitteisiin. Analyysin perusteella toteutettavilla turvamekanismeilla voidaan kustannustehokkaasti laskea riskien toteutumisen todennäköisyyttä hyväksyttävälle tasolle. [14. s. 18; 14. s. 26.]

Riskianalyysillä pyritään siis parhaan mukaan ennustamaan tulevaisuutta. Analyysin perusteella tunnistettuihin riskeihin voidaan näin varautua etukäteen ja estää yritykseen kohdistuvien uhkien toteutumista tai vähentää niiden vaikutusta yrityksen toimintaan. [14. s. 15; 15. s. 26.]

Kaikkia uhkia ei tietenkään ole mahdollista ottaa huomioon. Eikä kaikkia uhkia vastaan edes kannata varautua etukäteen, mikäli sen toteutumisen todennäköisyys on hyvin pieni eikä se uhkaa yrityksen tärkeitä omaisuuseriä tai toimintoja. Analyysin osana tulisi

suorittaa myös kustannus-hyötyanalyysiä, jolla voidaan arvioida uhkan toteutumisen sekä uhalta suojautumisen aiheuttamat kustannukset. [14. s. 15.]

Riskien käsittely

Tunnistetun riskin osalta on arvioinnin yhteydessä päätettävä riskin käsittelystä. Mahdollisia riskien käsittelytapoja ovat seuraavat [15. s. 26]:

- riskien pienentäminen asianmukaisilla tietoturvamekanismeilla
- riskien tietoinen hyväksyminen, mikäli ne täysin täyttävät organisaation riskien hyväksymiskriteerit
- riskin minimoiminen tai välttäminen kieltämällä riskin mahdollistavat toimenpiteet
- riskin siirtäminen ulkopuoliselle taholle, kuten vakuutusyhtiölle, alihankkijalle tai palveluntarjoajalle.

Tietoturvapolitiikka

Tietoturvapolitiikka on käytännöistä, standardeista, suosituksista ja menetelmistä koostuva kokoelma, jonka tarkoitus on luoda kestävä perusta tietoturvan toteuttamiselle [14. s. 10]. Se on myös väline hallinnolle asettaa selkeä linjaus ja osoittaa sitoutumisensa tietoturvaan luomalla koko organisaatiota koskettava tietoturvapolitiikka [15. s. 29].

Tietoturvapolitiikasta tulisi käydä ilmi ne mekanismit, käytännöt ja säännökset tietoturvasta, joihin yrityksen työntekijät ja hallinnon jäsenet sitoutuvat. Tietoturvapolitiikka tulisi erikseen määritellä tietoturvapolitiikan määrittelyasiakirjaan, joka julkaistaan ja josta tulisi tiedottaa yrityksen työntekijöille. [15. s. 29.]

Tietoturvapolitiikan määrittelyasiakirjaa tulisi katselmoida tasaisin väliajoin tai suurien organisaation muutosten yhteydessä. Mikäli katselmusten yhteydessä politiikassa havaitaan puutteellisia tai organisaation nykytilanteeseen sopimattomia kohteita, tulee

määrittelyasiakirjaa muuttaa niiden kohtien osalta ja muutoksista tulee tiedottaa organisaation henkilöstölle. [15. s. 30.]

4.2 Henkilöstön turvallisuus

Henkilöstön turvallisuuden tarkoituksena on varmistaa, että työntekijät, alihankkijat ja kolmannen osapuolen käyttäjät ymmärtävät vastuunsa ja ovat kykeneviä täyttämään roolinsa, joihin heitä harkitaan. Lisäksi sillä pyritään vähentämään varkauksien, väärennöksien ja resurssien väärinkäytön aiheuttamia uhkia. [15. s. 57.]

Asiakasyrityksessä kaikki uudet työntekijät ja alihankkijat tulisi tarkastaa perusteellisesti, etenkin jos kyseessä on arkaluonteinen työ. Jokaisen työntekijän ja yrityksen projekteissa työskentelevän alihankkijan tulisi allekirjoittaa sopimus, josta käy ilmi heidän roolinsa ja vastuunsa tietoturvan osalta. [15. s. 57.]

Työsuhteen aikana työntekijöille tulisi tarjota riittävä tietoturvallisuuden valmennuksen ja kouluttamisen taso, jotta he ovat kykeneviä suoriutumaan vastuistaan tietoturvan osalta. Koulutukset ja tieturvatietoisuuden lisääminen ovat yksi tapa vähentää henkilöstön aiheuttamia tietoturvariskejä. Mahdollisten suorien tietoturvamenettelyjen rikkomisesta tulisi laatia viralliset sanktiomenettelyt. [15. s. 58.]

Työsuhteen päättymisen varalta tulisi asiakasyrityksellä olla vastuut ja käytännöt, joilla työtekijän, aliurakoitsijan tai muun kolmannen osapuolen poistuminen yrityksestä voidaan hoitaa hallitusti. Sopimuksen päättyessä tulee poistuvan henkilön palauttaa kaikki yrityksen suojattavat kohteet, kuten laitteisto, arkaluonteinen materiaali tai yrityksen toiminnan kannalta kriittinen informaatio. Yrityksen hallinnon vastuulla on poistumisen järjestäminen niin, että yritys ei menetä kriittistä tietoa sekä tiedottaa muille työntekijöille toimintajärjestelyjen muutoksista. [15. s. 65–66.]

4.3 Fyysinen tietoturva

Fyysisellä turvallisuudella tarkoitetaan toimitilojen, henkilöstön ja laitteiden, kuten palvelimien ja verkkolaitteiden turvallisuutta ja suojaamista erilaisia fyysisiä uhkia vastaan. [14. s. 325; 15. s. 68.]

Mahdollisia tällaisia riskejä asiakasyritykselle ovat [14. s. 326]:

- varkaus
- vaaratilanteet, kuten tulipalo, vesivahinko tai sähkökatko
- luonnonkatastrofit
- ihmisen aiheuttama sabotaasi tai ilkivalta.

Asiakasyrityksen toimitilojen turvallisuutta suunniteltaessa on otettava huomioon tilojen fyysinen sijainti. Toimitilat sijaitsevat suuren yrityspuiston katutasossa, ja ne on varustettu suurilla ikkunoilla. Tämä lisää etenkin murtovarkauksien ja ilkivallan riskiä huomattavasti. Riskiä pienentää huomattavasti yrityspuiston puolesta tuleva vartiointi ja hälytysjärjestelmät, mutta näistäkin huolimatta yrityksen tilat ja irtaimistot tulee olla vakuutettuina murtojen ja ilkivallan varalta. Kaikki yrityksen kriittiset laitteet ja informaatio tulisi säilyttää erillisessä lukitussa tilassa tai kokonaan poissa toimistolta.

Tulipalot ja vesivahingot ovat aina vakavasti otettava riski. Toimitiloissa on aina paljon dokumentteja ja laitteistoa, joiden tuhoutuminen tulipalossa tai vesivahingon toimesta keskeyttää liiketoiminnan väliaikaisesti tai kokonaan. Toimitiloissa on automaattinen sammutusjärjestelmä, mutta sen käynnistymisestä todennäköisemmin seuraa kaikkien esillä olevien laitteiden dokumenttien tuhoutuminen. Tästä syystä kaikki sähköisessä muodossa oleva informaatio tulisi säilyttää tai ainakin varmistaa palvelimille, jotka eivät sijaitse asiakasyrityksen toimitiloissa, vaan kunnolla palosuojatussa palvelintilassa.

Suuret luonnonkatastrofit alueella, missä toimitilat sijaitsevat, ovat epätodennäköisiä. Suurimpana uhkana voidaan pitää voimakkaita ukonilmoja, joissa voimakas salamointi

saattaa sytyttää tulipaloja. Salamointi voi myös aiheuttaa voimakkaita virtapiikkejä tai sähkökatkoksia, jotka voivat vioittaa yrityksen laitteistoa tai heikentää palveluiden saatavuutta. Erityisesti yrityksen kriittiset laitteet ja palvelut tulee suojata näiltä sähkönjakelun häiriöiltä. Palvelimet tulee sijoittaa tilaan, jossa on tarvittavat suojaukset sähkösyötön häiriöiden varalta. Muiden salamoiden ja sateiden aiheuttamien vahinkojen varalta tulee yrityksellä olla ne kattava vakuutus.

Ilkivallalla ja sabotaasilla tarkoitetaan kaikkea tahallisesti toimitiloille ja omaisuudelle tehtyä haittaa. Ilkivalta on yleensä hetken mielijohteesta tehtyä eikä sillä ole mitään varsinaista motiivia. Sabotaasilla tarkoitetaan kriittisten laitteiden tai informaation vahingoittamista tai tuhoamista tarkoituksena aiheuttaa taloudellista vahinkoa organisaatiolle. Tästä syystä kaikki asiakasyrityksen kriittiset ja mahdollisesti mielenkiintoiseksi sabotaasin kohteeksi luokitellut kohteet täytyy suojata ja niiden koskemattomuutta tulee valvoa.

Fyysisellä turvallisuudella pyritään näin estämään suurien aineellisten vahinkojen toteutuminen tai minimoimaan niiden vaikutukset ja niistä aiheutuneet kustannukset.

Päävastuussa fyysisestä turvallisuudesta on aina viime kädessä yrityksen hallinto. Vaikkakin hallinto voi delegoida mekanismien suunnittelun, toteutuksen ja valvonnan muulle henkilöstölle, on viimeinen päätösvastuu toteutettavista mekanismeista aina hallinnolla.

4.4 Järjestelmien tietoturva

Kriittisten tietojenkäsittelyjärjestelmien tulisi sijaita turvallisilla alueilla, joiden kulunvalvonta, paloturvallisuus, verkkoyhteydet ja sähkönsyöttö on turvattu. Järjestelmiä ajavien laitteiden tulisi olla fyysisesti suojattuja luvattomalta pääsyltä, vahingonteolta sekä häirinnältä. [15. s. 69.]

Järjestelmien tiedoista tulee ottaa varmuuskopiot, ja otettuja varmuuskopioita tulee testata säännöllisesti, jotta niihin voidaan hätätilanteessa luottaa. Varmuuskopioiden

osalta tulee kopioiden taso sekä varmuuskopioinnin ajallinen tiheys määritellä. Varmuuskopioinnista ja palautusmenetelmistä tulee olla täydellinen dokumentaatio, jossa on esitelty varmuuskopiointiprosessi ja sen työkalut sekä ohjeistus tietojen palauttamiselle. [15. s. 95.]

Otetut varmuuskopiot tulee säilyttää erillään varmistetuista tietojärjestelmistä, jotta tiedonkäsittelyjärjestelmiin vaikuttanut ongelmatilanne ei pääse vaikuttamaan varmuuskopioiden saattavuuteen tai eheyteen. [15. s. 95.]

4.5 Poikkeustilanteisiin varautuminen ja niiden käsittely

Poikkeustilanteilla tarkoitetaan tilannetta, jossa normaalitoiminnon ulkopuolinen tekijä voi vaikuttaa palveluiden tai informaation käytettävyyteen. Tällaisia poikkeamia voivat olla organisaation ulkopuoliset voimat, tekniset virheet sekä inhimilliset tekijät.

Asiakasyrityksen toimintaan vaikuttavia poikkeamia on esitelty alla.

Fyysiset murrot

Fyysisillä murroilla tarkoitetaan kaikkea luvatonta tunkeutumista asiakasyrityksen tiloihin.

Asiakasyrityksen tilat sijaitsevat katutasossa ja suuret ikkunat entisestään korostavat fyysisen murron aiheuttamaa riskiä. Murrosta aiheutuneet tietovuodot ja tietojen menetykset ehkäistään kieltämällä tärkeiden tietojen säilytys työasemilla ja määräämällä ne talletettavaksi keskitettyyn järjestelmään, joka ei sijaitse yrityksen omissa tiloissa. Murrosta aiheutuneet taloudellisista vahingoista aiheutuneet riskit pienennetään siirtämällä pääosa riskistä vakuutusyhtiölle hankkimalla vakuutus, joka korvaa murrosta aiheutuneet vahingot.

Laitteistoviat

Laitteistovikoihin kuuluvat kaikki työasemien, verkkolaitteiden ja palvelimien teknilliset ongelmat, kuten esimerkiksi kovalevyjen hajoamiset tai jonkin muun laitteen osan rikkoutuminen. Vika voi johtua laitteen huonolaatuisesta osasta tai olla suoraan käyttäjän toimien aiheuttama.

Koska asiakasyrityksen ydinosaaminen on ohjelmistokehityksessä ja konsultoinnissa, ei sillä itsellään ole varsinaisia laitetiloja. Kaikki palvelinkapasiteetti tai tarvittava laitetila ostetaan palveluntarjoajalta. Näin tekemällä saadaan palvelinlaitteistoihin ja varmuuskopiointiin liittyvät riskit helposti siirrettyä palveluntarjoajalle ja asiakasyritys voi keskittyä omaan ydinosaamiseensa.

Kuitenkin jotain pieniä kehitys- ja testipalvelimia sijaitsee yrityksen omissa tiloissa sijaitsevassa pienessä lukitussa laitetilassa. Näille laitteille ei ole olemassa mitään varalaitteita, eikä niistä oteta varmuuskopioita, koska laitteen hajoamisen aiheuttama riski yritykselle on erittäin pieni.

Palvelukapasiteetin ja tietoliikenneyhteyksien tarjoajien sekä työasemien ja kriittisten verkkolaitteiden toimittajien kanssa on solmittava palvelutasosopimus (Service Level Agreement, SLA), jossa tulee huomioitava seuraavat asiat [17]:

- prosenttiosuus ajasta jolloin palvelu on oltava saatavilla
- teknisen tuen reagointi vikatilanteisiin arkisin ja viikonloppuisin.
- palveluiden ja laitteiden riittävä suorituskyky ennalta määritetylle käyttäjämäärälle
- aika, jota ennen palveluntarjoajan on ilmoitettava suunnitelluista käyttökatkoksista ja huoltotoimenpiteistä
- toimenpiteet, mikäli palvelusopimuksessa määriteltyjä ehtoja ei kyetä täyttämään

Työasemille ja verkkolaitteille voidaan yrityksen tiloissa säilyttää muutamaa varalaitetta äkillisten vikatilanteiden varalta niin sanottuna hätävarana, kunnes korvaava laite saapuu. Tällaiseksi varalaitteeksi kelpaa vanha, aikaisemmin käytöstä poistettu laite.

Kriittisten laitteiden asetustiedostot on talletettava erikseen turvalliseen paikkaan, jotta rikkoutuneen laitteen asetukset voidaan nopeasti palauttaa korvaavaan laitteeseen.

Tietomurrot

Tietomurroilla tarkoitetaan kaikkea sellaista tietojärjestelmien käyttöä, joka tapahtuu ilman järjestelmän omistajan lupaa. Tietomurtoa suorittava hyökkääjä pyrkii pääsemään järjestelmän sisältämiin tietoihin käsiksi joko jollakin olemassa olevalla tunnuksella, pyrkimällä luomaan itse itselleen käyttäjätunnuksen tai käyttämällä hyväkseen järjestelmästä löytyvää aukkoa. [18.]

Tietomurrot ovat hyvin dynaamisia riskejä yrityksille. Uusia tietomurtoihin tähtäävien hyökkäyksien mahdollistavia aukkoja löydetään erilaisista järjestelmistä jatkuvasti. Näitä aukkoja on jokaisessa järjestelmässä, eikä niiltä kaikilta voi mitenkään suojautua.[14. s. 73.]

Tietomurtoihin tähtäävät hyökkäykset ovat tietoturvauhkien nopeimmin muuttuva osa. Niiden tavoitteena on tunkeutua yrityksen sisäisiin järjestelmiin ja pystyä kopioimaan, muokkaamaan tai tuhoamaan yrityksen omistamaa tietoa.

Hyökkääjä voi myös pyrkiä aiheuttamaan yritykselle taloudellisia tappioita häiritsemällä sen kriittisten järjestelmien toimintaa [14. s. 75]. Tällaisia hyökkäyksiä ovat esimerkiksi palvelunestohyökkäykset DoS (Denial Of Service) tai DDoS (Distributed Denial of Service), joiden tarkoituksena on lamauttaa hyökkäyksen kohteena oleva palvelu ruuhkauttamalla se suurella määrällä palvelupyyntöjä. Tällainen hyökkäys voi tehdä palvelusta käyttökelvottoman tai jopa kaataa sen kokonaan. [19. s. 89]

Hyökkäykset eivät välttämättä kohdistu pelkästään yrityksen tietojärjestelmiin, vaan yritys saattaa joutua myös perinteisempien tapojen kohteiksi. Tällöin hyökkäysten kohteena ovat yleensä yrityksen työntekijät, joiden tietämättömyyttä ja hyväuskoisuutta pyritään hyväksikäyttämään halutun informaation saamiseksi.

Kaikki yritykselle kriittinen tai luottamuksellinen tieto tulisi säilyttää keskitetyssä järjestelmässä, jossa sen hallinta ja valvonta on helpompaa. Vaikkakin yksi keskitetty järjestelmä on hyökkääjälle herkullisempi kohde, on sen suojaaminen ja hallitseminen silti helpompaa kuin tuhansien informaation palasten hallinta hajautettuna useille työasemille ja palvelimille.

Tietomurtoja tekevän hyökkääjän toimintaa voidaan hankaloittaa esimerkiksi käyttämällä riittävän turvallisia salasanoja, siksi tietoturvapolitiikassa tuleekin määritellä salasanan minimipituus ja muoto. Esimerkiksi salasanan on oltava vähintään kahdeksan merkkiä pitkä, se ei saa perustua sanakirjasta löytyvään sanaan, ja siinä täytyy olla vähintään kolme numeroa. [20.]

Erilaisia teknillisiä järjestelmiä hyökkäyksiltä suojautumiselle ovat palomuurit, tunkeutumisenhavaitsemisjärjestelmät (IDS, Intrusion Detection System) ja tunkeutumiseniestämisjärjestelmät (IPS, Intrusion Prevention System). Näillä järjestelmillä pyritään estämään pääsyä yrityksen resursseihin, havaitsemaan verkon kautta tapahtuvia hyökkäyksiä sekä suorittamaan toimenpiteitä hyökkäysten pysäyttämiseksi. Tietoturvapolitiikassa tuleekin tarkasti määritellä tietoverkkoa koskevat säännöt siitä, minkälainen liikenne on sallittua.

Henkilöstön aiheuttamia riskejä voidaan vähentää tietoturvatietoisuutta lisäämällä esimerkiksi kouluttamalla sekä asianmukaista ohjeistusta parantamalla. Valvontaa tulisi myös lisätä velvoittamalla käyttäjät raportoimaan epäilyttävistä tiedusteluista, puheluista tai sähköposteista yrityksen hallinnolle tai tietoturvasta vastaaville henkilöille.[15. s. 62.]

Lopullinen vastuu hyökkäyksiä vastaan suojautumisesta on yrityksen hallinnolla, jonka tehtävänä on päättää toimenpiteet suojautumiselle. Tietoturva-ammattilaisten vastuulle jää käytännön toteuttaminen, ylläpito ja valvonta. Erilaisten tietoturvaa käsittelevien julkaisujen aktiivinen seuranta uusien löydettyjen aukkojen varalta kuuluu myös tietoturvahenkilöstön tehtäviin. Näihin löytyneisiin riskeihin on reagoitava ja niiden vaikutus yrityksen toimintaan on arvioitava.

Haittaohjelmat

Haittaohjelmiksi kutsutaan ohjelmia, jotka on tarkoituksellisesti suunniteltu soluttautumaan tietokoneisiin ja tietojärjestelmiin tai aiheuttamaan näille vahinkoa esimerkiksi poistamalla informaatiota tai suorittamalla ei-toivottuja tapahtumia [21].

Haittaohjelmat leviävät useimmiten sähköpostin tai erilaisten pikaviestimien kautta. Sähköpostin liitetiedostona voi olla tietokoneen saastuttava tiedosto tai linkki, joka johtaa käyttäjän www-sivulle, josta haittaohjelma lataantuu käyttäjän koneelle käyttämällä hyväksi esimerkiksi internet-selaimen haavoittuvuutta. [22.]

Haittaohjelmat voidaan jakaa eri ryhmiin seuraavasti [20; 23]:

- *Virukset* ovat parhaiten tunnettu haittaohjelmatyyppi. Ne levittävät itseään tietyntyyppisistä tiedostoista toisiin. Mahdollisesti virus saattaa sisältää muutakin haitallista koodia, joka saattaa esimerkiksi korruptoida osan tai kaiken kovalevyn sisällöstä.
- *Madot* ovat periaatteeltaan hyvin samanlainen kuin virus, mutta koneen sisäisten tiedostojen sijaan ne saastuttavat muita tietokoneita esimerkiksi tietoverkkojen yli.
- *Troijalaiset* ovat haittaohjelma jotka naamioivat itsensä esimerkiksi peliksi tai joksikin hyötyohjelmaksi
- *Vakoiluohjelmat* keräävät tietoa koneessa tehtävistä tapahtumista tai vaikkapa näppäinpainalluksista. Keräämänsä tiedon ohjelma saattaa lähettää internetin välityksellä ohjelman tekijälle.

- *Mainosohjelmat* esittävät mainoksia tai lataavat mainoksia tietokoneelle.
- *Rootkitit* ovat ohjelmia, jotka kykenevät piilottamaan toimintansa täysin käyttäjältä tai virustorjuntaohjelmistoilta.

Haittaohjelmilta suojautumiseen tulee käyttää viruksentorjuntaohjelmia, joiden päivittämisestä on huolehdittava ja joiden lisenssien tulee olla voimassa. Käyttöjärjestelmät ja käytettävät ohjelmat on myös säännöllisesti päivitettävä. Palomuurilaitteen ohjelmistot ovat myös pidettävä ajan tasalla. [24.]

Käyttäjät tulee ohjeistaa olemaan asentamatta tai avaamatta epäilyttäviä tiedostoja, ohjelmia, sähköposteja tai pikaviestimien kautta kulkevia epäilyttäviä linkkejä.

Virustorjuntaohjelmistojen, käyttöjärjestelmien ja muiden ohjelmistojen päivittämisestä vastaa yrityksen tietoturvahenkilöstö. Lisäksi yrityksen verkkoliikennettä tulisi tietoturvahenkilöstön puolesta valvoa, sillä monet madot ja haittaohjelmat voidaan havaita epäilyttävän verkkoliikenteen perusteella.

4.6 Valvonta

Tietoturvan yhteydessä valvonnalla pystytään entisestään tehostamaan tietojen luetettavuutta, eheyttä ja käytettävyyttä. Valvonnalla pystytään varmistamaan, että kukaan ei pysty huomaamatta tekemään luvattomia muutoksia organisaation omistamaan informaatioon. Lisäksi pystytään havaitsemaan ongelmat tietojen ulkoisen eheyden kanssa. [14. s. 31.]

Oikeanlaisilla valvontamekanismeilla voidaan saada tietoa esimerkiksi informaatiota tarjoavien palveluiden tilasta ja mahdollisista häiriötilanteista. Nopeasti saatavan valvontainformaation ansiosta voidaan ongelmatilanteisiin ja väärinkäytöksiin puuttua välittömästi ja näin parantaa suoraan informaation käytettävyyttä. [14. s. 32.]

Valvontamekanismit voidaan jakaa kolmeen luokkaan ja jokaiseen luokkaan mahtuu kolmea eri tyyppiä mekanismeja: ennaltaehkäisevät, havaitsevat ja korjaavat

mekanismit. Ennaltaehkäisevien valvontamekanismien tarkoituksena on estää riskien toteutuminen, havaitsevilla mekanismeilla voidaan havaita riskit ja korjaavilla mekanismeilla voidaan järjestelmät palauttaa ja suojausta tehostaa riskien toteutumisen jälkeen. [14. s. 32–33.]

Valvontamekanismien kolme eri luokkaa ovat [14. s. 32]:

- *hallinnolliset mekanismit*, kuten standardoidut käytännöt ja työtavat sekä käyttäjäkoulutus
- *tekniset mekanismit* eli kaikki tekniset mekanismit, kuten pääsynvalvonta, järjestelmien lokitiedostot ja erilliset järjestelmien valvontatyökalut
- *fyysiset mekanismit,* kuten rakennusten turvallisuus, vartiointi, lukitukset, laitetilojen ja mobiilien laitteiden varmistaminen sekä varmuuskopiot.

Valvontamekanismien luokkia voidaan yhdistellä eri tyyppien kanssa [14. s. 34]. Esimerkiksi havaitsevalla ja teknillisellä mekanismilla voidaan tarkoittaa IDS-järjestelmää (Intrusion Detection System), jolla väärinkäyttö pyritään havaitsemaan teknisin välinein. Ennaltaehkäisevällä ja fyysisellä mekanismilla voidaan tarkoittaa vaikka toimitilan ovessa olevaa lukitusta.

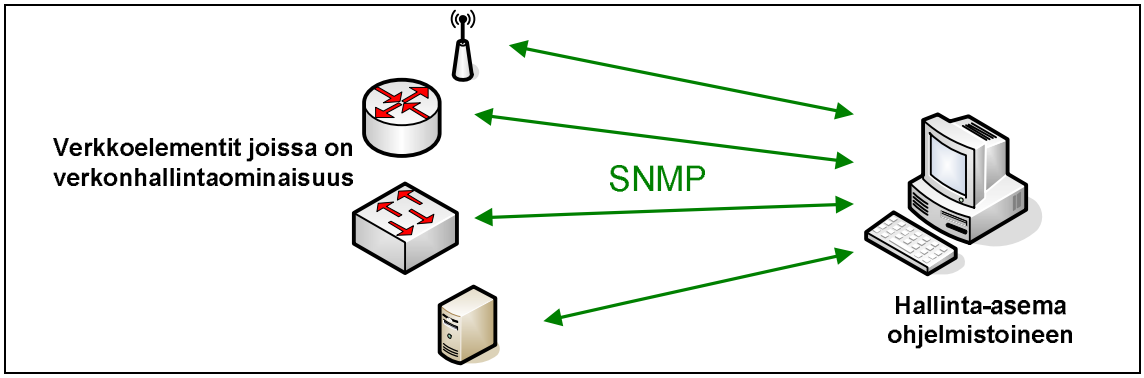
Asiakasyrityksen hallinnolla on vastuu sekä hallinnollisista että fyysistä mekanismeista. Vastuu teknisten järjestelmien ja työasemien valvonnasta on yrityksen tietoturvahenkilöstöllä. Näiden järjestelmien valvontaan voidaan käyttää työkaluina erilaisia sähköisiä valvontajärjestelmiä.

Markkinoilla on lukuisia avoimen ja suljetun lähdekoodin tuotteita, joilla voidaan valvoa tietoverkkojen, palvelimien sekä käyttäjien toimintaa. Valvontatyökaluilla voidaan tehostaa valvonnan laatua automatisoimalla monia tehtäviä, kuten valvontatiedon analysointia tai muita tehtäviä, joita valvova henkilöstö joutuisi muuten suorittamaan käsin. Kaiken laitteiden tuottaman valvontatiedon tarkastaminen manuaalisesti on äärimmäisen hidasta ja virhealtista puuhaa, joten automaattisella järjestelmällä voidaan valvonnan tehoa huomattavasti parantaa.

Seuraavassa esitellään muutamia teknisiä ratkaisuja valvonnan tehostamiseksi.

Simple Network Management Protocol

SNMP eli Simple Network Management Protocol on RFC-standardoitu (RFC 2574) protokolla internetin verkonhallintapalveluille [25; 26]. Sen arkkitehtuurimalli koostuu joukosta verkonhallinta-asemista ja verkkoelementeistä kuvan 3 mukaisesti. Verkonhallinta-asemat suorittavat verkonhallintaohjelmistoja, joilla valvontaan ja hallitaan verkkoelementtejä. Verkkoelementit taas ovat verkkoon kytkettyjä laitteita, kuten palvelimia, kytkimiä ja reitittimiä, joihin on asennettu verkonhallintaominaisuus, joka kykenee suorittamaan hallintaohjelmistoilta saatuja komentoja. SNMP:tä käytetään näiden kahden osapuolen välisessä kommunikaatiossa. [27.]



Kuva 3. SNMP:n toiminnan kuvaus

Syslog

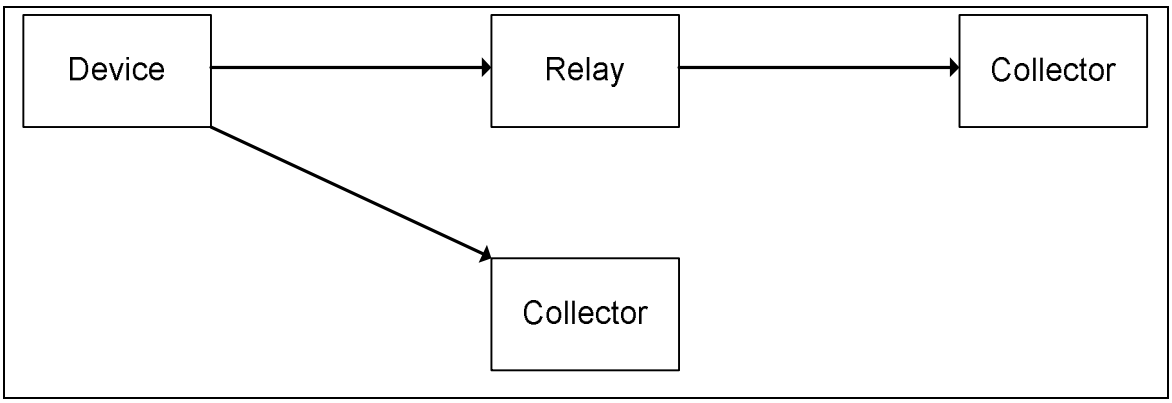
Termiä syslog voidaan käyttää kuvaamaan protokollaa tai sovelluksia, joita käytetään viestien välittämiseen. Termillä voidaan myös tarkoittaa lokiviestejä itsessään. Syslog on tapa välittää lokitietoja lähettäjältä vastaanottajalle. [28.]

Lokiviestit ovat viestejä laitteelta tai järjestelmältä, jotka kuvaavat laitteen tai järjestelmän tilaa tai tapahtumaa.

Syslog-palvelu tukee kolmea roolia: Laite (device), välittäjä (relay) ja kerääjä (collector). Device-roolin laitteet toimivat lähteinä ja collector-roolin laitteet varastoina syslog viesteille. Relay-roolin laitteet toimivat esimerkiksi välityspalvelimena tai suodattimina device- ja collector-roolin laitteiden välissä. [29. s. 3.]

Device- ja collector-roolin laitteiden välissä voi toimia monesta moneen -suhde. Collector-laitteet voivat kerätä viestejä usealta device-roolin laitteelta ja device-roolin omaava laite voi taas lähettää tietojaan usealle eri collector-roolin laitteelle. [29. s. 3.]

Syslog-palvelun roolit on esitetty kuvassa 4.



Kuva 4. Esimerkki Syslog-palvelun mallista.[30,s.6.]

Syslog on hyvin yleinen ja tehokas järjestelmä eri järjestelmien lokiviestien keskitettyyn hallintaan. Siitä on ajan kuluessa muodostunut standardi lokiratkaisu Unix- ja Linux-järjestelmille. Syslog-ratkaisuja ja -sovelluksia on olemassa myös muille käyttöjärjestelmille, ja monet verkkolaitteetkin tukevat sitä.

Keskitetyllä lokiviestien hallintaan tarkoitetulla järjestelmällä voidaan tehostaa yritysten kriittisten laitteiden ylläpidettävyyttä sekä valvontaa. Syslog-palvelut tarjoavat mahdollisuutta suodattaa lokiviesteistä vain tärkeimmät ja kiinnostavimmat ylläpitäjien nähtäväksi. Näin saadaan vähennettyä vika- ja väärinkäyttötilanteiden havaitsemiseen ja analysointiin käytettyä aikaa.

Nagios

Nagios on palkittu avoimen lähdekoodin pohjautuva valvontajärjestelmä [31], jota voidaan käyttää monenlaisten palveluiden ja laitteiden valvontaan. Reitittimet, HTTP-palvelimet (HyperText Transfer Protocol) ja sähköpostipalvelimet, kaikkien valvontatiedot voidaan keskittää yhteen järjestelmään valvonnan tehostamiseksi. [32.]

Koska tuote on avoimen lähdekoodin lisenssin alla, sen saa käyttöönsä pelkillä käyttöönottokustannuksilla, mitään lisenssikustannuksia sen käytöstä ei tule. Sen ympärillä on erittäin aktiivinen kehittäjäyhteisö ja liitännäisiäkin on tehty erittäin suurelle joukolle laitteita ja ohjelmistoja, joten sen soveltuvuus kirjavaan ympäristöön on parempi kuin monilla yhden valmistajan tuotteisiin keskittyneillä järjestelmillä. [32.]

Nagios voi käyttää SNMP-protokollaa laitteiden väliseen kommunikointiin. Se tarkkailee valvottavia laitteita ja palveluita, ja mikäli jokin laite ilmoittaa ongelmasta, lähettää se hälytyksen tai tiedotteen asiasta niitä koskeville henkilöille, joko sähköpostitse tai jopa tekstiviestillä. [32.]

Nagios on yksi esimerkki Syslogin tapaan keskitetystä valvonta ja hallintajärjestelmästä, jolla voidaan helpottaa ja tehostaa teknistä valvontaa suorittavien henkilöiden työskentelyä. Työntekijöiden ei enää tarvitse tarkkailla jokaisen palvelun ja laitteen tilaa erikseen vaan kaikki on nähtävissä yhden web-pohjaisen käyttöliittymän kautta.

5 Tietopalvelut

5.1 Dokumenttienhallintajärjestelmä

Dokumentit, niin sähköiset ja paperisetkin, ovat tärkeitä organisaatioille, sillä ne usein sisältävät liiketoiminnalle kriittistä informaatiota. Suurin osa projekteista ja prosesseista alkavat dokumentilla ja päättyvät dokumenttiin. Työ usein alkaa aloitteen tekevällä dokumentilla, joka voi olla tarjous tai esimerkiksi määrittelyasiakirjan luonnos ja päättyy yleensä projektin dokumentaatioon tai loppuraporttiin. Ensimmäisen ja viimeisen dokumentin väliin mahtuu iso joukko muita dokumentteja, joita yleensä päivitetään projektin aikana lukuisia kertoja. [33.]

Tämä aiheuttaa usein ongelmatilanteita organisaatioissa, joissa ei ole kunnollista ratkaisua dokumenttien hallintaan: dokumentit katoavat käyttäjien virheiden takia, yhdestä dokumentista saattaa olla liikkeellä useita verisoita, jotka eivät ole yhdenmukaisia keskenään. Lisäksi dokumenttien saatavuus juuri sillä hetkellä, kun niitä tarvitaan, saattaa olla kyseenalaista.

Dokumenttienhallintajärjestelmät ovat teknisiä ratkaisuja, joilla pyritään korjaamaan ja vähentämään dokumenttien hallintaan liittyviä ongelmia. Ottamalla käyttöön yksi keskitetty järjestelmä, johon kaikki yrityksen dokumentit tallennetaan, voidaan varmistaa dokumenttien säilyvyys, saatavuus ja eheys.

Metatiedot, tallennus ja hakutoiminnot, työjonot sekä versiointi ovat dokumenttienhallintajärjestelmien yleisimpiä ominaisuuksia. Metatiedoilla tarkoitetaan dokumentteihin liitettävää tietoa, joka kuvaa dokumenttien sisältämää tietoa. Tallennus ja hakutoiminnoilla taataan tiedon säilyttäminen järjestelmässä sekä sen löytyminen ja saatavuus tarvittaessa. Työjonoilla voidaan luoda automaatiota dokumenttien hallintaan, esimerkiksi lajittelua dokumentin nimen, luontipäivän tai siihen liitetyn metatiedon perusteella. Versiointi mahdollistaa paluun takaisin mihin tahansa hetkeen dokumentin elinkaaren aikana, kun uusi versio dokumentista tallennetaan järjestelmään, se ei

suinkaan tallennu entisen version päälle vaan uudeksi versioksi samasta dokumentista. Näin esimerkiksi tiedoston turmeltuminen tai virheelliset muutokset eivät tee dokumentista käyttökelvotonta, koska vanhempaan versioon palaaminen on aina mahdollista.

Asiakasyrityksen tulisikin ottaa käyttöönsä järjestelmä sähköisten dokumenttien hallintaan parantaakseen informaationsa luottamuksellisuutta, käytettävyyttä ja eheyttä.

Alfresco

Dokumenttienhallintajärjestelmiä on lukuisia. Markkinoilla on suuri joukko suljetun lähdekoodin tuotteita, joiden lisensointi on monimutkaista ja hinnakasta. Avoimen lähdekoodin puolelta johtava tuote dokumenttien hallinnassa on Alfresco Software Inc.:n valmistama ja yhtiön nimeä kantava tuote: Alfresco.

Alfresco on Documentumin perustajan John Newtonin sekä Business Objectsin Operatiivisen johtajan John Powelin vuonna 2005 perustama avoimen lähdekoodin sisällönhallintaratkaisuihin erikoistunut yritys [34]. Sen keihäänkärkituotteena on Alfresco-dokumenttienhallintajärjestelmä (Document Management System, DMS), joka kilpailee suoraan Microsoftin SharePointin kanssa. Alfrescon ympärillä on vahva kehittäjäympäristö ja siitä löytyy sekä kaupallinen ja tuettu Alfresco Enterprise versio sekä GPL-lisenssin (General Public License) alla toimiva yhteisöllinen versio, Alfresco Community. [35.]

Alfrescon DMS:n tärkeimpiin ominaisuuksiin kuuluvat seuraavat: Microsoft Office integraatio, joka mahdollistaa Alfrescon toimintojen käyttämisen Office-tuoteperheen ohjelmistoista käsin ja täten tekee Alfrescosta vaihtoehdon Microsoft SharePointin korvikkeena. Windowsin levyjakojen tapaan CIFS (Common Internet File System) -protokollaa käyttävä jaettu levy tarjoaa parempaa käytettävyyttä ja tukee muun muassa kansiokohtaisesti määriteltyjä työjonoja. Jaetun levyn lisäksi Alfrescossa on web-pohjainen käyttöliittymä, jonka kautta tietojen lataus ja tallennus on mahdollista. Muita

ominaisuuksia ovat jo aikaisemmin mainitut metatiedon tallennus, dokumenttien versiointi sekä työjonot. [35.]

CIFS on protokolla, joka on aikaisemmin tunnettu nimellä Server Message Block (SMB). Sen pääasiallinen käyttötarkoitus on mahdollistaa tiedostojen ja laitteiden, kuten tulostimien, jakaminen lähiverkossa. Microsoft tukee CIFS:iä laajasti ja onkin implementoinut sen Windows käyttöjärjestelmiinsä. Tämän takia sen tukeminen on dokumenttienhallintajärjestelmien ominaisuuksissa tärkeää.

Lisenssikustannuksiltaan Alfresco on kilpailijoitaan, kuten SharePointia ja Documentumia huomattavasti halvempi ja hinnoittelultaan yksinkertaisempi. Mikä tekee siitä houkuttelevan vaihtoehdon yrityksen dokumenttienhallintajärjestelmäksi. [liite 1].

5.2 Sisällönhallintajärjestelmä

Sisällönhallinta (Content Management) tai pikemminkin sisällönhallintajärjestelmä on työkalu, jolla voidaan hallita palvelun, kuten web-sivuston, sisältöä. Se sallii sellaisten henkilöiden tehdä muutoksia web-sivustoille, joilla ei ole varsinaista osaamista HTML-kielestä. (Hyper Text Markup Language). [36.]

Sisällönhallintajärjestelmä voi olla tehokas työkalu yrityksen sisäisessä käytössä monenlaisen tiedon jakamiseen ja tallentamiseen. Yrityksen käytännöt, henkilöstön yhteystiedot ja esimerkiksi käyttöohjeet voidaan tallentaa yhteen järjestelmään, josta ne ovat helposti kaikkien saatavilla. Myös projektiryhmien kommunikointia voidaan tehostaa antamalla heille käyttöön sivusto, johon ryhmien jäsenet voivat jakaa projekteihin ja teknologioihin liittyvää tietoa.

Perinteisiä ominaisuuksia sisällönhallintajärjestelmissä ovat mm. Web-julkaisu, sivujen versionhallinta, hakutoiminnot sekä indeksointi [36].

Web-julkaisu sallii käyttäjien käyttää valmiita pohjia tai työkaluja web-sisällön luomiseen tai muokkaamiseen. Versionhallinnalla voidaan tietty sivu päivittää uudempaan versioon tai palauttaa sille vanhemman version sisältö. Tämä helposti estää virheellisen sisällön säilymisen sivustolla. Versionhallinta pitää myös lukua siitä, milloin mikäkin päivitys on tehty ja kenen toimesta. Versionhallinta myös indeksoi siihen talletettua tietoa ja mahdollistaa tiedon hakemisen avainsanoilla. [36.]

Sisällönhallintajärjestelmän käyttöönotolla asiakasyritys voisi parantaa sisäistä kommunikointiaan huomattavasti. Pitkät sähköpostiketjut, joissa puidaan projektiin tai muuhun yrityksen sisäiseen tehtävään liittyviä asioita, ovat usein vaikeaselkoisia eivätkä ne välttämättä tavoita kaikkia. Yhdellä sisällönhallintajärjestelmällä tieto saadaan helposti kaikkien ulottuville ja jokainen pystyy ottamaan osaa tietojen jakamiseen.

Sisällönhallintajärjestelmiä on olemassa lukuisia ja etenkin avoimen lähdekoodin puolella valikoima on suuri ja niiden läpi käyminen tässä työssä olisi täysin mahdotonta, siksi tässä työssä käytetään esimerkkinä MediaWiki-sisällönhallintajärjestelmää, johon suosittu tietosanakirjapalvelu Wikipedia pohjautuu.

MediaWiki

MediaWiki on ilmainen GPL-lisenssin alla toimiva palvelinpuolen ohjelmisto, jonka on kehittänyt voittoa tavoittelematon Wikimedia Foundation ja jota käytetään kaikissa säätiön projekteissa kuten Wikipediassa ja Wictionaryssa. [37.]

MediaWiki on toimintaperiaatteeltaan web-pohjainen wiki-ohjelmisto. Wiki-ohjelmistot ovat sovelluksia, jotka tarjoavat mahdollisuuden etsiä, lisätä ja muokata informaatiota, joka voi olla esimerkiksi web-sivujen muodossa [36]. MediaWikissä informaatio tarjotaan siis web-sivujen muodossa. Ohjelmisto tarjoaa työkalut sivujen lisäämiseen, muokkaamiseen ja poistamiseen, joten sivuston käyttäjän ei tarvitse varsinaisesti osata mitään web-julkaisuun tarkoitettua teknologiaa, kuten esimerkiksi HTML-kieltä.

MediaWiki käyttää sivujen muokkaamiseen omaa Wikitext-kieltä, se on yksinkertaistettu vaihtoehto HTML-kielelle ja sillä toteutetaan kaikki muotoilu wikiin kirjoitettavalle sisällölle. MediaWiki -ohjelmisto lukee tekstistä muotoiluun tarkoitetut merkit, muuttaa merkit oikeiksi muotoiluiksi ja tämän jälkeen tuo sivun käyttäjän näkyviin. Taulukossa 1 on muutama esimerkki Wikitext-syntaksista.

Taulukko 1: Wikitext muotoiluja [38]

Wikitext muotoilu	Lopputulos
[[Uusi sivu]]	Luo wikin sisäisen linkin sivulle nimeltään ”Uusi Sivu”
’’’Lihavoitu teksti’’’	**Lihavoitu teksti**
’’Kursivoitu teksti’’	*Kursivoitu teksti*

Nykyään MediaWikiä käytetään myös monissa yrityksissä sisäisen tiedon välittämiseen sekä sisällönhallintajärjestelmänä.

MediaWikin ominaisuuksiin kuuluvat sivujen muokkauksen, lisäämisen ja poistamisen lisäksi revisionti eli sivujen versionhallinta, jolla voidaan nähdä, kuka on milloinkin tehnyt tietylle sivulle muutoksia. Sivun tila voidaan myös palauttaa mihin tahansa näistä revisioista milloin tahansa. Ohjelmisto tukee myös matemaattisten kaavojen esittämistä sen mukana tulevalla lisäosalla. Lisäosat ovatkin yksi MediaWikin vahvuuksista, sillä niitä kehittämässä on suuri joukko ihmisiä, jotka jakavat niitä yleensä ilmaiseksi. [37.]

5.3 Asiakkuuden hallintajärjestelmä

Asiakasyrityksellä on lukuisia asiakaskontakteja, joiden hallintaa voidaan tehostaa asiakkuudenhallintajärjestelmällä. Käytännössä se on järjestelmä, johon syötetään asiakkaan tiedot, kuten yhteyshenkilön nimi, puhelinnumero, osoite ja sähköpostiosoite. Lisäksi voidaan syöttää tietoja, kuten milloin asiakkaaseen on otettu edellisen kerran yhteyttä, miten yhteydenotto tapahtui ja mikä oli lopputulos. Näitä tietoja soveltamalla voidaan asiakasyrityksen myynnin ja kontaktoinnin toimintaa tehostaa.

Asiakkuudenhallinta- eli CRM-järjestelmät (Customer Relationship Management) tarjoavat usein monipuolisia työkaluja yrityksen hallinnolle ja myyntityötä tekevälle henkilöstölle. Sen kautta myyjät ja muu asiakkaiden kanssa toimiva henkilökunta saa käsiinsä yhteystietoja sekä muuta informaatiota liittyen tiettyyn asiakkaaseen. Yrityksen hallinto taas pystyy käyttämään sitä myynnin ja muun asiakastoiminnan valvomiseen, sillä useat CRM-järjestelmät tarjoavat työkalut asioiden tilastolliseen tarkkailuun. Monesti myös CRM-järjestelmät kykenevät luomaan ennusteita myyntityön edistymisestä perustuen aikaisemmin kerättyyn dataan myynnin edistymisestä.

SugarCRM

SugarCRM on markkinajohtaja avoimen lähdekoodin CRM-järjestelmissä. Se sai alkunsa puhtaana avoimen lähdekoodin projektina vuonna 2004, ja sittemmin siitä on kehittynyt varteenotettava vaihtoehto organisaation CRM-järjestelmänä. [39.]

SugarCRM tarjoaa muun muassa seuraavia ominaisuuksia [40]:

- *asiakasprofiilit*, joilla voi profiloida asiakkaan tiettyyn toimialaan tai maantieteelliseen alueeseen ja näin saada parempaa ymmärrystä asiakaskannasta
- *myynnin automaatio*, jolla myyjät ja asiakkaiden kanssa toimivat henkilöt voivat jakaa kontaktejaan ja tarkastella asiakaan edellisiä tapahtumia asiakashistorian kautta
- *raportointi*, jolla voidaan luoda myynneistä ja asiakaskontaktoinneista raportteja esimerkiksi yrityksen hallinnon nähtäväksi.

Kaiken kaikkiaan SugarCRM on monipuolinen työkalu, jossa on paljon ominaisuuksia kattamaan asiakkuuden- ja myynninhallinnan tarpeet. Tuotteesta on olemassa Community-, Pro- ja Enterprise-versiot, joiden erot ovat hinnassa ja ominaisuuksissa. Pro- ja Enterprise versiot ovat kaupallisia ja maksullisia tuotteita, joiden kehittämisestä, testaamisesta ja tuesta vastaa SugarCRM yhdessä kehittäjäyhteisönsä kanssa. Ne on tarkoitettu erikokoisille organisaatioille, joten ne myös tarjoavat hiukan erilaisia ominaisuuksia. Tuotteista Pro on tarkoitettu pienille

ja keskikokoisille yrityksille ja Enterprise taas suurille yrityksille. Community-versio on SugarCRM:n ylläpitämä avoimen lähdekoodin tuote, jonka saa käyttöönsä ilmaiseksi. [41] Sen lisenssi perustuu Mozilla Public Licenseen, jota on muokattu SugarCRM:lle sopivaksi [42].

Erikoiseksi community-version tekee se, että se ei tarjoa kaikkia samoja ominaisuuksia kuin Pro- tai Enterprise versiot. SugarCRM siis ole täysin puhdas avoimen lähdekoodin järjestelmä, mutta siitä on silti saatavissa ilmainen versio, jonka ominaisuudet on mitoitettu riittäväksi pienen yrityksen tarpeisiin. [43.]

6 Infrastruktuuri

6.1 Toimitilat ja sähköverkko

Asiakasyrityksen toimitilat sijaitsevat yrityspuistossa, joka vuokraa tilojaan ja palveluitaan yrityksille. Toimitiloihin kuuluu kaapeloinnit tietoliikenneyhteyksille, sähköverkko, jonka kapasiteetti on määritelty riittäväksi toimitilojen kokoon nähden, sekä sammutusjärjestelmä tulipalojen varalta.

Ulkopuolisten pääsy toimitiloihin on myös estetty sähköisellä lukituksella. Yrityksen henkilöstöllä on jokaisella yksilöllinen avainkortti, jonka avulla he pääsevät sisälle yrityksen toimitiloihin. Virka-aikojen ulkopuolella myös yrityspuiston ovet ovat lukittuna, jolloin sinne pääsee samaisella avainkortilla. Kynti asiakasyrityksen tiloihin tapahtuu aina yrityspuiston tilojen kautta.

Sähkökatkosten varalta toimistossa on hätävalaistus ja selkeästi merkityt varauloskäynnit. Minkäänlaiselle varavirtajärjestelmälle asiakasyrityksellä ei ole tarvetta, koska mitään kriittisiä järjestelmiä ei tulisi ylläpitää yrityksen tiloissa. Pääosalla työntekijöistä on kannettavat tietokoneet, joilla työskentely on väliaikaisesti mahdollista ilman sähköverkkoakin.

Toimitilojen, tietoverkon kaapelointien ja sähköverkon ylläpito on siis yrityspuiston vastuulla, eikä niiden parantaminen vaadi mitään toimenpiteitä.

6.2 Tietoverkko

Tietoverkko on joukko yhteyksiä, joko langallisia langattomia, joilla yhdistetään organisaation työasemat, palvelimet ja muut verkkolaitteet toisiinsa. Sen tärkeimpänä tarkoituksena on jakaa käyttäjille resursseja ja tarjota yhteyspalveluita.[43. s. 4.]

Erilaisten tietopalveluiden, kuten aikaisemmin tässä työssä mainittujen palveluiden, käyttö tapahtuu myös aina asiakasyrityksen tietoverkkoa pitkin. Asiakasyrityksessä tullaan käyttämään ns. verkkokeskeistä tietojärjestelmää, jossa tiedot ja dokumentit säilytetään keskitetyissä palveluissa erillisillä palvelimilla, jotka ovat kytkettyinä asiakaan tietoverkkoon. [43. s. 24.]

Laitteet

Tietoverkko koostuu monista fyysisistä osista, kuten kaapeloinneista sekä laitteista, jotka mahdollistavat liikenteen välityksen jonkin median yli. Tällaisia laitteita ovat esimerkiksi reitittimet, kytkimet ja langattoman lähiverkon tukiasemat.

Reitittimiä käytetään yhdistämään erillisiä verkkoja toisiinsa sekä tarjoamaan yhteyksiä Internetiin. Reitittimet tarjoavat liikenteen päästä päähän reitittämistä välittämällä datapaketteja eri verkkoihin protokollan ja verkkokerroksen tietojen perusteella. Reitittimet erottelevat eri levitysalueet toisistaan. [44. s. 42.] Moniin reitittimiin on myös liitetty erilaisia palomuuritoimintoja sekä muita teknillisiä tietoturvamekanismeja.

Kytkimet ovat oppivia laitteita: ne kykenevät oppimaan informaatiota datapaketeista, joita verkon eri tietokoneet lähettävät. Ne käyttävät tätä informaatiota rakentaakseen välitystauluja, jonka avulla ne kykenevät päättelemään jonkin verkon tietokoneen lähettämän datapaketin kohteen ja näin pystyvät tarjoamaan nopean välityksen lähdeportista kohdeporttiin. [45. s. 219.]

Langattoman lähiverkon tukiasema on käytännössä radiolähetin ja vastaanotin. Se toimii yhteyspisteenä, jonka avulla langattomat tilaajat voidaan liittää organisaation lähiverkkoon. Tukiasema voi toimia joko yksinäisenä langattoman lähiverkon keskuspisteenä tai langattoman ja langallisen lähiverkon välisenä yhteyspisteenä. Osa tukiasemista voi myös toimia toistimina, jotka kasvattavat langattoman lähiverkon kantoaluetta. [46. s. 29.]

Virtual Private Network

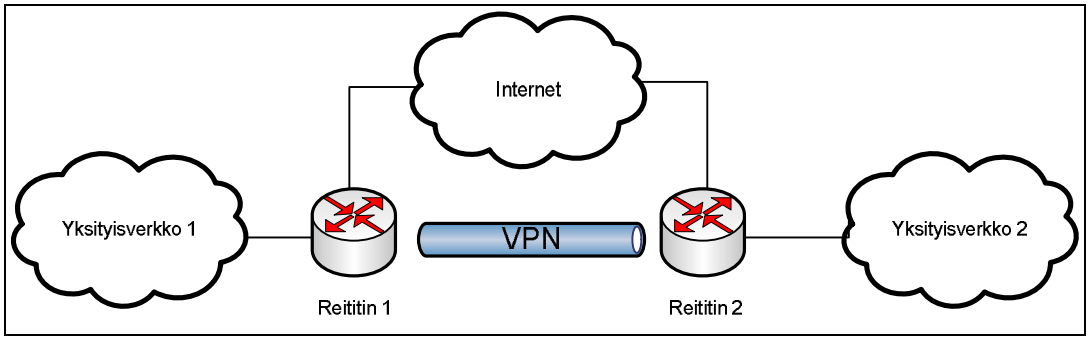
Organisaatioiden sisäisen liikenteen kuljettaminen internetin tai muun julkisen verkon kautta suojaamatta on merkittävä tietoturvariski. Sisäinen informaatio voidaan suojata rakentamalla julkiseen verkoon niin sanottuja tunneleita, jotka ovat suojattuja yhteyksiä kahden pisteen välillä. Näistä suojatuista yhteyksistä käytetään nimitystä Virtual Private Network (VPN). [43. s. 381.]

VPN-tunneli voidaan muodostaa kahden eri laitteen tai usean eri verkon välille. Sen aiheuttaa pienempiä kustannuksia kuin suuret fyysiset yksityisverkot. VPN tarjoaa myös enemmän joustavuutta ja skaalautuvuutta kuin perinteiset laajaverkot. Tämä mahdollistaa organisaatioille nopean ja kustannustehokkaan tavan laajentaa omaa yksityisverkkoaan sivukonttoreille, yhteistyökumppaneille, etätyöntekijöille sekä muille liikkuville käyttäjille. [47. s. 454.]

VPN-tunneli siis tarjoaa kahden pisteen välisiä yhteyksiä yhteydettömässä IP-verkossa (Internet Protocol). Tämä mahdollistaa kehittyneiden turvallisuusominaisuuksien käytön. VPN-tunnelit käyttävät salausta, jolla estetään luvattomia osapuolia näkemästä liikenteen sisältöä, kun se kulkee julkisessa verkossa. Salauksessa viestin lähettäjä salaa viestin sisällön muodostamalla siitä koodia, joka ei ole mitenkään luettavassa muodossa. Tunnelin toisessa päässä viestin vastaanottaja purkaa salauksen ja muuntaa viestin jälleen luettavaan muotoon. [47. s. 456.]

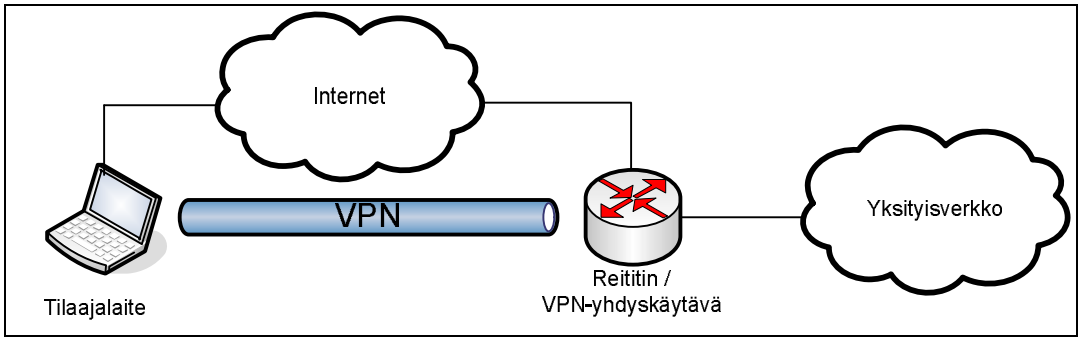
VPN-tunneleita voidaan pääasiassa muodostaa kahdella eri tavalla [47. s. 457]:

Yhteys voidaan muodostaa kahden reitittimen välille kuvan 5 mukaisesti. Yhteyden on tarkoitus olla kiinteä, sitä yleensä käytetään kahden tai useamman sisäverkon yhdistämiseen, esimerkiksi yhdistämään sivukonttorin ja pääkonttorin sisäverkot.



Kuva 5. Kahden reitittimen välinen VPN yhteys

Yhteys voidaan luoda myös tilaajalaitteen ja reitittimen tai VPN-yhdyskäytävän välille kuvan 6 mukaisesti. Yhteys on luonteeltaan väliaikainen, sitä käytetään pääasiassa liikkuvien käyttäjien tai etätyöntekijöiden liittämiseen organisaation sisäverkkoon. Tilaajalaite voi olla esimerkiksi tietokone tai matkapuhelin.



Kuva 6. Tilaajalaitteen sekä reitittimen tai VPN yhdyskäytävän välinen yhteys.

Asiakasyrityksessä tulisi pääsy sisäverkkoon ja sen resursseihin sallia ainoastaan VPN-tunnelin kautta. Mitään arkaluontoista tai yrityksen sisäistä tietoa ei saa välittää tai käsitellä julkisen verkon kautta ilman yhteyksien suojaamista.

Päästäkseen käsiksi sisäisiin resursseihin on liikkuvien käyttäjien otettava luotava VPN-yhteys asiakasyrityksen VPN-yhdyskäytävän kanssa. Yhdyskäytävässä tulee olla määritelty, mihin resursseihin tunneloidun yhteyden kautta voi päästä.

Mikäli asiakasyrityksen ja tytäryrityksen välistä luottamuksellista informaatiota tullaan välittämään julkisessa verkossa, esimerkiksi tietopalveluita käyttämällä, tulee toimistojen välille luoda staattisempi kahden reitittimen välinen VPN-yhteys. Koska

yritysten tietoliikenne on hyvin purskeista, ei VPN-yhteyden tarvitse kyetä suuriin siirtonopeuksiin.

VPN yhteyksien välisen tiedonsiirron tulisi silti yhteensä päästä nopeuksiin, jotka lähentelevät 1–2 megabittiä sekunnissa.

Virtual Local Area Network

Virtual Local Area Network (VLAN) tuo lähiverkkojen hallintaan ja suunnitteluun joustavuutta. Se laajentaa normaalit reitittimien rajaamat yhteislähetysalueet VLAN-sidottuihin yhteislähetysalueisiin. VLAN mahdollistaa yhteislähetysalueiden muovaamiseen mihin tahansa muotoon, joka pystytään verkon kytkimissä määrittämään. [48. s. 122.]

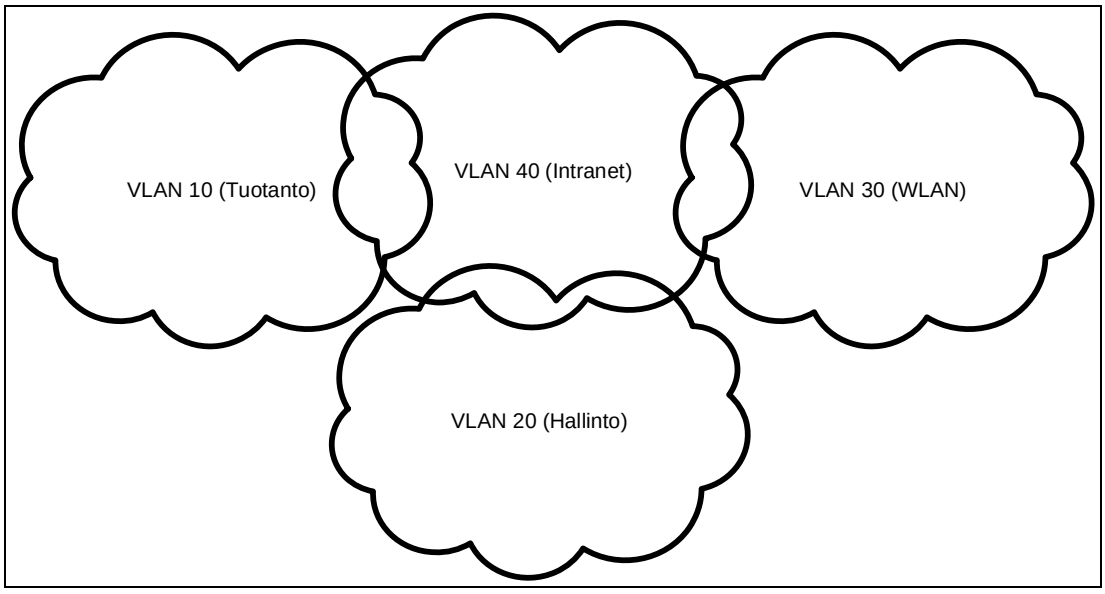
VLAN on loogisesti erillinen aliverkko. Sen avulla voidaan sallia useiden eri aliverkkojen olemassaolo yhdessä fyysisessä kytketyssä verkossa. Saman VLAN:n sisällä sijaitsevien tietokoneiden IP-osoitteiden ja aliverkon tunnuksien täytyy olla yhdenmukaisia kyseisen VLAN:n kanssa. Näiden VLAN:ien täytyy myös olla konfiguroituna kytkimeen. Lisäksi jokaisen kytkimen portin täytyy olla asetettu osaksi jotain VLAN:a. [48. s. 122.]

VLAN-teknologian käyttöönotto tuo yrityksen tietoverkolle enemmän joustavuutta ja kykyä tukea yrityksen tavoitteita. Suurimpia hyötyjä VLAN:n käyttöönotossa ovat seuraavat ominaisuudet [48. s. 125]:

- *Turvallisuus.* Organisaation osat, joilla on käsiteltävänä arkaluontoista informaatiota, voidaan eristää muusta verkosta ja näin estää luvaton pääsy kyseiseen informaatioon.
- *Kustannustehokkuus.* VLAN vähentää tarvetta kalliille verkkopäivityksille. Olemassa olevien laitteiden toimintaa saadaan tehostettua jakamalla yksi suuri verkko pienempiin osiin ja näin vähentämällä turhaa liikennettä verkossa.

- *Yhteislähetysviestien rajoittaminen.* Verkon jakaminen VLAN:eilla rajoittaa aliverkon laitteiden määrää, jotka osallistuvat levitysviestien lähettämiseen. Tämä estää yhteislähetysviestimyrskyn (Broadcast Storm) leviämisen koko verkkoon.
- *Pienempi kuormitus teknilliseen henkilökuntaan.* VLAN:eilla voidaan helpottaa verkon hallintaa, koska niillä saadaan jaettua samanlaiset verkonkäyttötarpeet omaavat käyttäjät samaan aliverkkoon. Tämä helpottaa muun muassa pääsylistojen ja muiden tietoturvamekanismien suunnittelua, toteutusta ja hallintaa. VLAN:t helpottavat myös eri verkon osien tunnistamista, sillä VLAN:t voidaan nimetä kuvaamaan jotain tiettyä verkon tai organisaation osaa.

Asiakasyrityksessä tulee organisaation yksityisverkko pilkkoa pienempiin loogisiin osiin hallittavuuden ja tietoturvan kasvattamiseksi. Hallinto, tuotanto ja tietopalvelut tulisi eristää omiin loogisiin aliverkkoihinsa, jotta niiden välistä liikennettä voitaisiin paremmin hallita sekä vähentää levitysviestien verkolle aiheuttamaa kuormaa.



Kuva 7. Esimerkki verkon jakamisesta eri VLAN:eihin.

Kuvassa 7 on esimerkki verkon jakamisesta loogisiin osiin ja siitä, kuinka ne on eristetty toisistaan. Kuvassa näkyvät aliverkot samalla myös heijastavat osittain yrityksen organisaatiorakennetta. Tuotantoaliverkko sisältää kaikki yrityksen tuotannon

henkilöt, hallintoaliverkossa sijaitsevat kaikki asiakasyrityksen hallinnon henkilöt, intranet-aliverkko sisältää kaikki yrityksen tietopalvelut ja WLAN-aliverkko on verkko, jonka kautta kaikki asiakasyrityksen langattoman lähiverkon yhteydet kulkevat.

Tuotannon, hallinnon ja WLAN-aliverkkojen käyttäjien ei ole tarvetta päästä käsiksi toistensa verkkoihin ja resursseihin. Jokaisesta verkosta kuitenkin tarvitaan yhteys Intranet-aliverkkoon, jotta tietopalvelut olisivat kaikille saatavilla.

Wireless Local Area Network

Organisaatioiden tietoverkkojen tarvitsee nykyisin entistä paremmin tukea työntekijöitä, jotka ovat liikkeessä. Kannettavat tietokoneet ja matkapuhelimet tarjoavat ominaisuuksia, joilla ne voidaan liittää organisaation tietoverkkoon langattomasti. Tärkein ja eniten käytetty langaton verkkoteknologia on Wireless Local Area Network (WLAN). [48. s. 379.]

Nykyiset organisaatioiden tietoverkot ovat riippuvaisia kytkinpohjaisista lähiverkoista toimistojen päivittäisissä toiminnoissa. Työntekijät ovat entistä liikkuvia eikä töitä nykyään tehdä ainoastaan oman työpöydän ääressä, mutta jatkuvaa pääsyä organisaation tietoverkkoon tarvitaan. Tällaisissa tapauksissa langallisen verkon käyttö on erittäin epäkäytännöllistä. [48. s. 380.]

Kuten muutkin verkot, langattomat verkot välittävät informaatiota verkkomedian kautta. Tässä tapauksessa käytetty media on sähkömagneetista säteilyä, eli radioaaltoja. Liikkuville verkoille on tärkeää, että käytetty media pystyy kattamaan laajan alueen, jotta sitä käyttävät asiakkaat voivat vapaasti liikkua kantoalueen sisällä. Radioaallot voivat helposti läpäistä seiniä ja muista toimistoista löytyviä esteitä, näin ne kykenevät tarjoamaan laajan kantoalueen. Näistä radioaaltoja käyttävistä teknologioista onnistunein on ollut 802.11. [49. s. 5.]

802.11 kuuluu IEEE 802 -perheeseen, joka on kokoelma määritelmiä LAN-teknologioille. Siitä käytetään montaa eri nimeä riippuen siitä, ketkä siitä puhuvat.

Jotkut käyttävät siitä nimitystä langaton Ethernet korostaakseen sen jaettuja sukujuuria langallisen Ethernet-verkon kanssa. WIFI Alliance on yrittänyt voimakkaasti tuoda esiin heidän Wireless Fidelity (Wi-FI) sertifikaattiohjelmaansa, jolla pyritään saavuttamaan yhteensopivuus kaikkein 802.11-standardeja käyttävien laitteiden välillä. [46. s. 6.]

802.11 on itse asiassa kokoelma standardeja, joita käytetään langattomien lähiverkkoyhteyksien toteuttamiseen taulukon 2 mukaisesti.

Taulukko 2: 802.11 standardit. [50]

Standardi	Toimintataajuus	Maksiminopeus megabitteinä sekunnissa (Mbit/s)
802.11b	2,4 GHz	11
802.11g	2,4 GHz	54
802.11a	5 GHz	54
802.11n	2,4 GHz & 5 GHz	248

Alkuperäisessä 802.11-standardissa esiteltiin kahdentyyppisiä tunnistusmenetelmiä: avoimen ja jaettuun WEP-avaimeen (Wired Equivalent Privacy) perustuva tunnistus. Avoin tunnistus ei ole kuitenkaan varsinainen tunnistusmenetelmä. Jaettuun WEP-avaimeen perustuvan tunnistuksen tarkoitus oli tarjota suojausta radiolinkille ja tehdä siitä lähes yhtä turvallinen kuin langallisesta lähiverkkoyhteydestäkin. Tässä teknologiassa on kuitenkin havaittu suuria vajavaisuuksia ja siihen perustuva suojaus on helposti murrettavissa. [48. s. 406.]

Nykyään yritysverkoissa pääosin tunnistamiseen käytetty standardi on 802.11i, joka on samankaltainen WiFi Alliancen Wi-Fi Protected Access (WPA2) -standardin kanssa. Ennen WPA2:n käyttöönottoa monet yritykset yrittivät suojata WEP-tunnistuksen puutteita käyttämällä fyysisiä laitteita yksilöivien Media Access Control (MAC) -osoitteiden suodatusta tai olemalla mainostamatta verkkojensa Service Set Identifier (SSID) -tunnisteita. Kummatkaan näistä menetelmistä eivät tosin ole riittäviä suojausmenetelmiä sillä laitteen MAC-osoite on väärennettävissä ja SSID-tunnisteen voi saada selville radioliikennettä luotaamalla. [48. s. 406.]

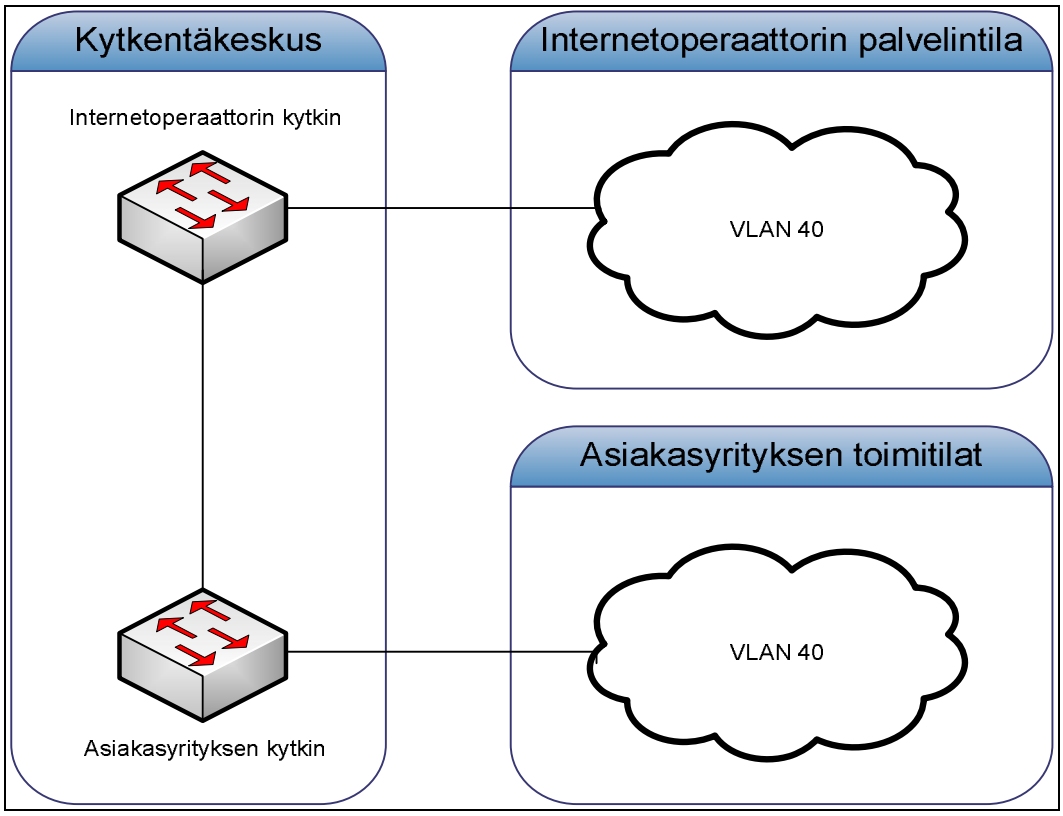
Asiakasyrityksen tulisikin käyttää WLAN:a liikkuvien käyttäjien liittämiseksi yrityksen lähiverkkoon. Langattoman verkon käyttöönotolla saadaan myös tarjottua käyttäjien muille laitteille, kuten matkapuhelimille mahdollisuus päästä käsiksi yrityksen tietoverkkoon.

Koska WLAN on jaettu media ja se käyttää radioaaltoja tiedon välitykseen, voivat yrityksen ulkopuoliset henkilöt liittää itsensä verkkoon, mikäli sitä ei ole suojattu. Ottaen huomioon jaetun WEP-avaimen heikkoudet yrityksen langaton lähiverkko tulisikin suojata käyttäen WPA2-tunnistusta informaation luottamuksellisuuden ja eheyden säilyttämiseksi.

6.3 Palvelimet

Asiakasyrityksellä ei ole mitään omia palvelimien ylläpitoon sopivia tiloja, joten palvelinylläpito joudutaan hankkimaan palveluna internetoperaattorilta tai muulta palveluntarjoajalta.

Asiakasyrityksen internetoperaattorin toimiessa samassa rakennuksessa on mahdollista eristää palvelimet omaan virtuaalisen lähiverkkoonsa ja kytkeä tämä verkko suoraan asiakasyrityksen kytkimeen kuvan 8 mukaisesti. Näin palvelimet kuuluisivat asiakasyrityksen sisäverkkoon ilman VPN-yhteyksiä, vaikka fyysisesti palvelimet sijaitsisivat toimitilojen ulkopuolella. Palvelimiin voidaan lisätä toinen verkkokortti, joka olisi taas kytketty internetoperaattorin omaan aliverkkoon ja jota kautta palvelinten yhteydet ulkoverkkoon kulkisivat. Tällä voidaan minimoida toimiston reitittimen kautta kulkevaa liikennettä ja täten saavuttaa kustannussäästöjä laitehankinnoissa.



Kuva 8. Kahden eri fyysisen sijainnin liittäminen yhteen virtuaalisella lähiverkolla.

Ylläpitopalveluista palveluntarjoajan kanssa on tehtävä palvelusopimus, jossa määritellään suorituskykyä, saatavuutta sekä vikatapahtumien vasteaikoja koskevat minimivaatimukset. Vaatimuksissa tulee ottaa kantaa verkkoyhteyksiin ja sähkönsyöttöön. Lisäksi, mikäli palveluntarjoajalta ostetaan tai vuokrataan ylläpitopalveluiden lisäksi palvelinlaitteistoa, tulee näiden laitteiden saatavuudelle ja suorituskyvylle tehdä omat vaatimuksensa.

6.4 Työasemat

Asiakasyrityksellä voidaan ajatella olevan kahdentyyppisiä työasemia: kiinteitä ja kannettavia. Kiinteillä työasemilla tarkoitetaan pöytäkoneita, joita ei ole tarkoitettu liikutettavaksi. Kannettavat työasemat ovat kannettavia tietokoneita, joita yrityksen liikkuvat työntekijät käyttävät.

Kaikille työasemille tulee määritellä tietyt kriteerit, jotka niiden on täytettävä. Näiden määrittelyjen pohjalta luodaan työasemastandardin määrittelydokumentti, jonka avulla voidaan taata eri työasemien yhtenäinen kokoonpano ja riittävä suorituskyky.

Laitteistokokoonpanojen, ohjelmistojen ja yleisten käytäntöjen yhtenäistämisellä voidaan helpottaa työasemien hallintaa ja huoltotoimenpiteitä. Määrittelydokumentti tulee tarkastaa tasaisin väliajoin, mikäli määritelty kokoonpano ei ole riittävä, täytyy määritelmää päivittää, jonka jälkeen uudet laitehankinnat tulee tehdä tämän päivitellyn määritelmän mukaisesti.

7 Yhteenveto

Kokonaisuudessaan tämä työ oli prosessina hyvin opettavainen, se antoi minulle hyvän mahdollisuuden tutustua siihen, mistä osista organisaation tietojärjestelmät koostuvat ja mitä niiden suunniteluun kuuluu. Työn sisältämä aiheet muodostivat kokonaisuuden, joka suuruudessaan ei antanut mahdollisuutta pureutua tässä työssä kaikkiin asioihin niin syvällisesti kuin olisin halunnut. Asioiden pilkkominen pienemmiksi osiksi ennen suunnittelutyön aloittamista olisi ehkä auttanut rajamaan aihepiiriä paremmin.

Suunnittelutyön suurimmaksi teemaksi osoittautui tietoturva, joka tuntui integroituvan erittäin tiukasti muihin työssä käsiteltyihin aiheisiin. Käytännössä muutosten tekeminen tietoturvaan aiheutti aina jotain muutoksia joko infrastruktuurissa tai tietopalveluissa. Tietoturvalla hyvin usein luodaankin ne säännöt ja käytännöt, joiden päälle organisaation prosessit ja tietopalveluiden toiminnot pystytetään.

Avoimen lähdekoodin ohjelmistojen sekä palveluiden ominaisuudet ovat kasvaneet kypsien kaupallisten ohjelmistojen suuntaan ja siihen perustuvien sovellusten ympärille on perustettu kunnollista ja vakavaa liiketoimintaa. Ominaisuuksiensa puolesta monet avoimen lähdekoodin ohjelmistot kilpailevat täysiverisesti suljetun lähdekoodin kilpailijoidensa kanssa. Vaikkakin vielä monet yrityksen ja organisaatiot vierastavat ajatusta avoimen lähdekoodin käytöstä omassa liiketoiminnassaan, on tulevaisuudessa mielenkiintoista nähdä, voiko sen ympärille kasvaa yhtä suurta liiketoimintaa kuin suljetun lähdekoodin.

Avoimen lähdekoodin suurimmat ongelmat ovat liian tulkinnanvaraiset lisenssit, jotka ovat mahdollistaneet monien avoimeen lähdekoodiin perustuneiden kaupallisten tuotteiden synnyn. On ollut paljon keskustelua, voidaanko monien projektien enterprise-tason maksullisia ohjelmistoja varsinaisina avoimen lähdekoodin ohjelmistoina lisensseistä löytyvien vapaan levityksen ja muokkauksen estävien pykälien takia.

Asiakasyrityksen tietopalveluihin avoin lähdekoodi tarjoaa riittävät ominaisuudet, halvemmat kustannukset sekä joustavuutta tulevaisuuden muutoksia varten. Työssä

mainitut tietopalvelut kasvattavat yrityksen prosessien hallittavuutta ja parantavat viestintää, mikä on tärkeää yrityksessä, jossa työntekijät harvoin työskentelevät saman katon alla.

Työskennellessäni tämän työn parissa sain hyvän kuvan tietoturvan, infrastruktuurin sekä tietopalveluiden suunniteluun ja valintaan liittyvistä prosesseista sekä erilaisista liiketoiminnan prosesseista, joita tukemaan suunnitelma laadittiin. Asetetut tavoitteet saavutettiin mielestäni hyvin. Asiakasyritykselle kyettiin löytämään ne ratkaisut, joilla toimintojen kehittäminen tulevaisuudessa on mahdollista.

Tämän työn valmistuttua syntynyttä dokumentaatiota voidaan käyttää myöhemmin tukena asiakasyrityksen infrastruktuurin, tietoturvan ja tietopalveluiden auditoinnissa sekä suunnittelussa. Seuraavat vaiheet, kuten suunnittelu ja toteutustyöt, tullaan tekemään omina projekteinaan, sitä mukaa kuin asiakasyrityksessä se nähdään tarpeelliseksi.

Lähteet

1 Infrastructure. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/Infrastructure>. 24.4.2009. Luettu 26.5.2009.

2 Server (computing). (WWW-dokumentti.) Wikipedia .<http://en.wikipedia.org/wiki/Server_(computing)>. 26.4.2009. Luettu 26.4.2009.

3 Information security. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/Information_security>. 13.3.2009. Luettu 16.3.2009.

4 Kotilainen, Samuli. Iscsi uudistaa tallennuksen. (WWW-dokumentti.) Tietokone. <http://www.tietokone.fi/lukusali/artikkelit/2005tk02/ISKASI.HTM>. 1.2.2005. Luettu 10.2.2009.

5 Tietoturvallisuuden arviointi valtionhallinnossa. (WWW-dokumentti.) Valtionvarainministeriö. <http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf>. 1.8.2006. Luettu 29.5.2009.

6 Free Software. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/Free_software>. 17.3.2009. Luettu 17.3.2009.

7 Saastamoinen, Matti. Avoimen lähdekoodin lisenssit kaupallisessa liiketoiminnassa. (WWW-dokumentti.). <http://tutkielmat.uta.fi/pdf/gradu01157.pdf>. 1.3.2006. Luettu 17.3.2009.

8 Tiemann, Michael. History of The OSI. (WWW-dokumentti.) <http://www.opensource.org/history>. 19.9.2006. Luettu 20.3.2009.

9 Coar, Ken. The Open Source Definition. (WWW-dokumentti.) <http://www.opensource.org/docs/osd>. 7.7.2006. Luettu 20.3.2009.

10 Lahti, Jarmo. Kuka kantaa vastuun avoimen koodin laadusta? (WWW-dokumentti.) <http://m.digitoday.fi/?page=showSingleNews&newsID=20097929> 25.3.2009. Luettu 7.4.2009.

11 MySQL Success Stories. (WWW-dokumentti.) MySQL. <http://www.mysql.com/customers/>. Luettu 1.4.2009.

12 Success Stories. (WWW-dokumentti.) RedHat. <http://www.redhat.com/solutions/info/casestudies/>. Luettu 1.4.2009.

13 JUHTA. Avoimen lähdekoodin ohjelmien käyttö julkisessa hallinnossa. (WWW-dokumentti.) <http://docs.jhs-suositukset.fi/jhs-suositukset/JHS169/JHS169.odt>. 23.2.2009. Luettu 1.4.2009.

14 Kruzt, Ronald L. Vines, Russel Dean. Tietoturvasertifikaatti CISSP. Helsinki: Edita Publishing oy. 2003.

15 ISO/IEC 17799:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje.

16 Verkkopalveluarkkitehtuuri. (WWW-dokumentti.) <http://matwww.ee.tut.fi/hmopetus/hm-ohj/2007/pruju/hmohj2007-041-052-4sivulla.pdf>. Luettu 2.4.2009.

17 The SLA Training Guide. (WWW-dokumentti.) <http://www.service-level-agreement.net/sla-intro.htm>. Luettu 2.4.2009.

18 Kommonen, Mats. Suojatoimenpiteet tietomurtotapauksissa. (WWW-dokumentti.). http://www.cc.utu.fi/tietoturva/tietomurtotapauksissa.html>. 1.7.2008. Luettu 6.4.2009.

19 Kizza, Joseph Migga. Computer Network Security. New York: Springer Science+Business Media Inc. 2005.

20 Salasanatiedosto julkaistu useilla www-sivustoilla - vaihda salasana riittävän usein. (WWW-dokumentti.) <http://www.ficora.fi/index/viestintavirasto/uutiset/2007/P_80.html>. 15.10.2007. Luettu 6.4.2009.

21 Malware. (WWW-dokumentti.) <http://en.wikipedia.org/wiki/Malware>. 7.4.2009. Luettu 8.4.2009.

22 Haittaohjelmat. (WWW-dokumentti.) <http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/haittaohjelmat.html>. 27.9.2007. Luettu 9.4.2009.

23 Haittaohjelmat. (WWW-dokumentti.). Tietoturvaopas. <http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html>. 12.11.2008. Luettu 9.4.2009.

24 Suojautuminen haittaohjelmilta. (WWW-dokumentti.) Ficora. <http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/haittaohjelmat/suojautuminenhaittaohjelmilta.html>. 27.9.2007. Luettu 14.4.2009.

25 Simple Network Management Protocol – FAQ. (WWW-dokumentti.) <http://www.snmp.com/FAQs/snmp-faq-part1.txt>. 2.7.2003. Luettu 20.4.2009.

26 Blumenthal,Wijnen. Simple Network Management Protocol (SNMPv3). (WWW-dokumentti.). <http://www.ietf.org/rfc/rfc2574.txt>. 1.4.1999. Luettu 23.4.2009.

27 Case. Fedor. Schoffstall. Davin. RFC 1157: SNMP. (WWW-dokumentti.) <http://www.ietf.org/rfc/rfc1157.txt?number=1157>. 1.5.2009. Luettu 20.4.2009.

28 Syslog. (WWW-dokumentti.) Syslog. <http://www.syslog.org/wiki/Main/Syslog>. 26.10.2007. Luettu 21.4.2009.

29 New. Rose. RFC 3195: Reliable Delivery for syslog. (WWW-dokumentti.) <http://www.syslog.org/syslog/rfc3195.txt>. 2001. Luettu 21.4.2009.

30 Lonvick. RFC 3164: The BSD syslog Protocol. (WWW-dokumentti.) <http://www.syslog.org/syslog/rfc3164.txt>. 2001. Luettu 21.4.2009.

31 Venezia, Paul. Killer open source monitoring tools. (WWW-dokumentti.) <http://www.infoworld.com/t/networking/killer-open-source-monitoring-tools-860>. 24.11.2008. Luettu 23.4.2009.

32 Millard, Elizabeth. Managing Your Network. (WWW-dokumentti.) <http://www.processor.com/editorial/article.asp?Article=articles/p2931/20p31/20p31.asp&GUID=>. 2.8.2008. Luettu 23.4.2009.

33 Designing a Document Strategy. (WWW-dokumentti.) <http://www.document-strategy.com>. Luettu 24.3.2009.

34 About Alfresco. (WWW-dokumentti.) Alfresco. <http://www.alfresco.com/about/>. Luettu 27.4.2009.

35 Open Source Document Management. (WWW-dokumentti.) Alfresco. <http://www.alfresco.com/products/dm/>. Luettu 27.4.2009.

36 Svarre, Klaus. Content Management System. (WWW-dokumentti.). <http://searchsoa.techtarget.com/sDefinition/0,,sid26_gci508916,00.html>. 22.9.2006. Luettu 27.4.2009.

37 MediaWiki. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/Mediawiki>. 24.4.2009. Luettu 28.4.2009.

38 Wikipedia: How to edit a page. (WWW-dokumentti.) Wikipedia. <http://en.wikipedia.org/wiki/Wikipedia:Formatting#Wiki_Markup>. 17.5.2009. Luettu 19.5.2009.

39 SugarCRM. (WWW-dokumentti.) SugarCRM. <http://en.wikipedia.org/wiki/SugarCRM>. 30.4.2009. Luettu 5.5.2009.

40 Sugar Features. (WWW-dokumentti.) SugarCRM. <http://www.sugarcrm.com/crm/products/sugar-suite/components.html>. Luettu 5.5.2009.

41 Sugar Editions. (WWW-dokumentti.) SugarCRM. <http://www.sugarcrm.com/crm/products/editions.html>. Luettu 5.5.2009.

42 Farber, Dan. Commercial open source, a misnomer? (WWW-dokumentti.) 29.8.2006. Luettu 5.5.2009.

43 Hakala, Mika. Vainio, Mika. Tietoverkon Rakentaminen. Jyväskylä: Docento Finland Oy. 2005.

44 Cisco Systems Networking Academy: First-Year Companion Guide. Indianapolis: Cisco Press. 1999.

45 Cisco Networking Academy Program: CCNA1 and CCNA2 Companion Guide. Indianapolis: Cisco Press. 2005.

46 Cisco Networking Academy Program: Fundamentals of Wireless LANs. Indianapolis: Cisco Press. 2004

47 Cisco System Inc. CCNP2: Remote Access. Companion Guide. Indianapolis: Cisco Press 2005.

48 Lewis, Wayne. Lan Switching and Wireless. CCNA Exploration Companion Guide. Indianapolis: Cisco Press. 2008

49 Gast, Matthew S. 802.11 Wireless Networks. California: O'Reilly & Associates. 2002

50 IEEE 802.11 Standards, Facts & Channels. (WWW-dokumentti.) <http://www.air802.com/ieee-802.11-standards-facts-amp-channels.html >. 2005. Luettu 18.5.2009.

51 Alfresco. Total Cost of Ownership for Enterprise Content Management. Alfresco Content Community Site (WWW-dokumentti.) Alfresco. (Vaatii rekisteröitymisen.). <http://share.alfresco.com/>. Luettu 27.3.2009.

Liite 1: Dokumenttienhallintajärjestelmien linsessikustannuksia

Alla on käsitelty SharePointin, Documentumin ja Alfrescon lisensoinnin ja kustannuksien eroja Alfrescon tekemän tutkimuksen perusteella. [50]

Dokumentum

- kokoonpanolle 1032 erilaista vaihtoehtoa
- hinnoittelumalli, joka hinnoitellaan aina erikseen mm. käyttäjämäärä ja käytettävän asiakasohjelman perusteella.

Alla Documentumin lisenssien hintoja ylläpitokustannuksineen suositetulla kokoonpanolla:

Käyttäjämäärä	Lisenssimaksu	Ylläpitokustannukset	Yhteensä
100	$100664,73	$18414,25	$129078,98
1000	$764982,73	$116955,25	$863937,98

Taulukko 1: Documentumin hinnoittelu

SharePoint

- tukee vain Microsoftin tuotteita ja teknologioita
- Vendor Lock-in täysin Microsoftin tuotteisiin ja toimituksiin.

Alla Microsoft SharePoint lisenssien hintoja suositellulla kokoonpanolla:

Käyttäjämäärä	Lisenssimaksu	Ensimmäisen vuoden todelliset kulut
100	$20918,00	$24669,00
1000	$263168,00	$318738,00

Taulukko 2: SharePointin hinnoittelu

Liite 1: Dokumenttienhallintajärjestelmien lisenssikustannuksia

Alfresco

- Kaikki tuotteen osat ja ominaisuudet yhden hinnoittelun alla. Ei monimutkaisia lisenssejä.
- Ei per käyttäjä hinnoittelua eikä lisämaksuja käytetyn asiakasohjelman takia.
- Maksetaan vain yhdestä tilauksesta, johon kaikki ominaisuudet ja palvelut kuuluvat.

Alla Alfrescon hinnoittelu:

Käyttäjämäärä	Lisenssimaksu	Yhden vuoden tilausmaksu	Ensimmäisen vuoden todelliset kulut
100	$0	$18,500	$18,500
1000	$0	$33,500	$33,500

Taulukko 3: Alfrescon hinnoittelu