Opinnäytetyö (AMK)

Tietojenkäsittelyn Ko.

Yrityksen tietoliikenne ja tietoturva

2013

Marko Mattila, Tuukka Henttonen & Tuure Suokas

TIETOTURVA-AUDITOINTI JA TOIMENPITEET TIETOTURVAN PARANTAMISEKSI YRITYKSELLE X

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Joulukuu 2013 | 31 sivua

Esko Vainikka

Marko Mattila, Tuukka Henttonen & Tuure Suokas

TIETOTURVA-AUDITOINTI JA TOIMENPITEET TIETOTURVAN PARANTAMISEKSI YRITYKSELLE X

Tämän opinnäytetyön tavoite on antaa perustietoa verkon rakenteesta, tietoturvasta sekä ylläpidosta.

Opinnäytetyön aihe on hyvin ajankohtainen. Suomesta löytyy paljon PK-yrityksiä joilla yrityksen verkko on täynnä tietoturvauhkia. Yritysten kasvaessa perinteinen työryhmämalli ei ole järkevä tapa hallinnoida verkkoa. Verkon ylläpitäjän on hyvä osata vähintään perusasiat Active Directoryn käytöstä.

Verkon ajan tasalla oleva dokumentaatio on kriittistä yrityksen verkon ylläpidon kannalta häiriötilanteissa.

Yritys X:n pyynnöstä yrityksen toimitiloissa suoritetut käytännön työt ja siitä syntynyt dokumentointi on salattu.

ASIASANAT:

Active Directory, palvelin, tietoturva, ylläpito, tietoturva-auditointi, lähiverkko

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communication

December 2013 | 31 pages

Esko Vainikka

Marko Mattila, Tuukka Henttonen & Tuure Suokas

INFORMATION SECURITY AUDIT AND MEASURES TO IMPROVE INFORMATION SECURITY FOR COMPANY X

The aim of the present bachelor's thesis is to provide basic information about the network structure, information security and network maintenance.

The present bachelor's thesis focuses on a very topical issue as Finland has a lot of small and medium sized companies whose networks are full of security threats. As companies grow, the traditional workgroup model is not a feasible way for administrating a network. The network administrator should have some basic knowledge of how to use Active Directory. The up-to-date documentation of the network is a critical part of maintaining the company's network.

By the request of the Company X, the practical work and the resulting documentation in this thesis is classified.

KEYWORDS:

Active Directory, server, information security, maintenance, information security audit, local area network

SISÄLTÖ

1 JOHDANTO **6**

2 TIETOVERKOT JA VERKON DOKUMENTOINTI **7**

2.1 Lähiverkon määritelmä 7

2.2 Verkkoympäristössä käytetyt yleiset käsitteet 8

2.2.1 ADSL-yhteys 8

2.2.2 Valokuitutekniikka 8

2.2.3 Reititin 9

2.2.4 Kytkin 9

2.2.5 Ethernet 10

2.2.6 IP-osoitteet 11

2.2.7 MAC-osoitteet 13

2.3 Verkon dokumentointi 14

2.3.1 Dokumentoinnin kohteet 15

2.3.2 Pääperiaatteet sekä toteutus 16

3 TIETOTURVA JA TIETOTURVALLISUUDEN TARKISTAMINEN **17**

3.1 Tietoturvallisuuden peruskäsitteitä 17

3.2 Tietoturvan osa-alueet 17

3.3 Salasanakäytännöt 19

3.4 Tietoturvahyökkäykset 20

3.5 Suojautuminen tietoturvahyökkäyksiltä 21

3.5.1 Virustorjuntaohjelmistot ja palomuuri 21

3.5.2 Sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne 22

4 ACTIVE DIRECTORY WINDOWS SERVER 2008 -YMPÄRISTÖSSÄ **23**

4.1 Active Directoryn hallintatyökalut 24

4.2 Käyttäjätilit 25

4.3 Ryhmäkäytännöt 26

5 YRITYS X:N TIETOTURVA-AUDITOINTI (SALATTU) **27**

6 YRITYS X:N AUDITOINNISSA ILMENNEIDEN PUUTTEIDEN KORJAUS (SALATTU) **28**

7 POHDINTA **29**

LÄHTEET **30**

LIITTEET (SALATTU)

KUVAT

Kuva 1. Esimerkki yksinkertaisesta lähiverkosta. 7
Kuva 2. IPv4-osoite komentokehotteessa. 12
Kuva 3. MAC- sekä langattoman verkkoyhteyden osoite komentokehotteessa. 14

TAULUKOT

Taulukko 1. Kaapeliluokat (i&iSolutions 2013). 11
Taulukko 2. Osoiteluokat (Hakala & Vainio, 2005). 13

1 JOHDANTO

Suomesta löytyy useita PK-yrityksiä, jotka kasvuvaiheessa ovat unohtaneet päivittää verkkonsa vastaamaan nykypäivän vaatimuksia. Verkon dokumentaatio ei ole ajan tasalla tai hallinta saattaa olla vaikeaa tai jopa mahdotonta, kun käytössä ei ole oikeita työkaluja.

Verkon dokumentointi on yrityksen toimivan tietoliikenneverkon ydin. Palveluiden siirtyessä verkkoon vika on helpompi paikantaa ja korjata, kun tiedetään mistä etsiä. Dokumentaatio tulee pitää ajan tasalla. Pienikin muutos, yhden työaseman lisääminen tai IP-osoitteen muuttaminen, tulisi kirjata välittömästi. Tällä parannetaan verkon vikasietoisuutta.

Käsitteenä tietoturva mielletään liian suppeasti. Moni ajattelee virustorjuntaohjelmiston riittävän. Tietoturva kuitenkin kattaa huomattavasti laajemman kokonaisuuden, joka tässä työssä on jaettu kolmeen osa-alueeseen: tekniseen, fyysiseen ja sosiaaliseen tietoturvaan.

Idea tälle opinnäytetyölle sai alkunsa, kun Yritys X:n toimitusjohtaja oli käynyt Turun ammattikorkeakoululla kuuntelemassa tietoturvapäivän seminaareja. Tästä seuranneena yrityksen johtohenkilöstö päätti uudistaa verkkonsa vastaamaan nykypäivän vaatimuksia. Toimitusjohtaja otti yhteyttä kouluun kysyäkseen, olisiko opiskelijoilla potentiaalia hoitaa yrityksen verkko kuntoon. Kolmen opiskelijan voimin päätimme ottaa haasteen vastaan.

Jokaiselle jaettiin oma vastuualue. Tuure otti vastuulleen tietoturvan, Tuukka keskittyi verkon dokumentointiin ja Marko toteutti verkon rakennemuutoksen. Jokainen kuitenkin osallistui kaikkiin työn osa-alueisiin. Kirjallinen dokumentointi tehtiin yhteisesti. Salassapitosopimusten vuoksi emme tässä opinnäytetyössä voi julkaista tietoa yrityksessä tehdystä tietoturva-auditoinnista, dokumentoinnista tai verkon rakennemuutoksesta.

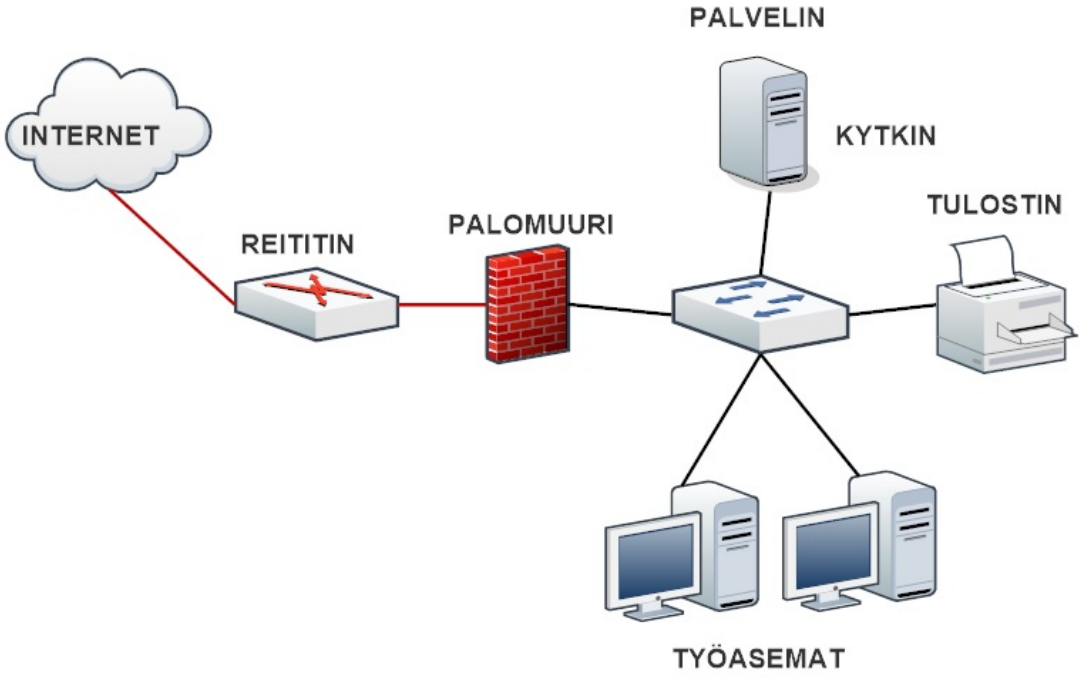
Lähteinä työssä on käytetty toimeksiantoyrityksen voimassaolevan verkon resursseja ja kirjallisina lähteinä ovat tietotekniikkaan liittyvä kirjallisuus sekä internet.

2 TIETOVERKOT JA VERKON DOKUMENTOINTI

Tämä osio selvittää ja täsmentää verkon yhteydessä käytettyjä laitteita. Tarkoituksena on selventää pintapuolisesti kaikenkokoisissa verkkoympäristöissä käytettyjä yleisempiä termejä, menetelmiä sekä laitteistoja. Tietoverkon ja sen dokumentoinnin kannalta nämä asiat on hyvä ymmärtää.

2.1 Lähiverkon määritelmä

Lähiverkko eli LAN (Local Area Network) on nopea tietoliikenneverkko, joka toimii maantieteellisesti rajatulla alueella. Useimmiten lähiverkko on yhden organisaation hallinnassa. Lähiverkon muodostavat työasemat, palvelimet, kytkimet, hubit, reitittimet ja niitä yhdistävät kaapelit (Kuva 1). Nykyisin lähiverkko voidaan myös toteuttaa langattomasti WLAN (Wireless Local Area Network) –tekniikalla. (Tuokko 2012, 11.)



Kuva 1. Esimerkki yksinkertaisesta lähiverkosta.

Lähiverkko toteutetaan nykyään useimmiten Ethernet-tekniikalla, joka on pakettipohjainen lähiverkkoratkaisu. Muita lähiverkkotekniikoita ovat Frame relay ja ATM (Asynchronous Transfer Mode).

Lähiverkon keskeisin tehtävä on jakaa resursseja. Palvelimet ja työasemat pystyvät helposti jakamaan muille verkon käyttäjille esimerkiksi tiedostoja. Tiedostojen jakamisesta huolehtivat tiedostopalvelimet. Lähiverkkoon liitetty tulostin mahdollistaa monelta työasemalta tulostamisen. (Hakala & Vainio 2005, 4-5.)

2.2 Verkkoympäristössä käytetyt yleiset käsitteet

2.2.1 ADSL-yhteys

ADSL on lyhennetty englannin kielen sanasta Asymmetric Digital Subscriber Line. ADSL verkkokytkintekniikka pystyy toimimaan vanhassa lankapuhelinverkossa ja tämän vuoksi se on yleisimmin käytetty internetliittymätyyppi kotitalouksissa. Uusin ADSL2+ -tekniikka mahdollistaa nopeimmillaan 24 Mbps yhteyden käyttäen lankapuhelinverkkoa, jossa tieto liikkuu kuparipareissa. Tämä tiedonsiirtotekniikka toimii niin, että liittymäntarjoajan laitekeskuksessa on operaattorin laitepaikka, josta liittymä lähtee. Data liikkuu vanhassa lankapuhelinverkossa epäsymmetrisen tiedonsiirtotekniikan avulla. Puhelinkeskuksen ja sieltä lähtevän laitepaikan sekä käyttäjän adsl-modeemin välinen etäisyys on verrannainen littymän nopeuteen. Pitkällä matkalla nopeus laskee. (D-Link 2013; FiCom 2013.)

2.2.2 Valokuitutekniikka

Valokuitutekniikan suurin etu on suurien datamäärien siirto ja tämän mahdollistaa suuri kaistanleveys. Valokuitutekniikan suuri kaistanleveys mahdollistaa nopeiden sekä uusien tiedonsiirtotekniikoiden käytön. Operaattoreiden nopeimmat valokuituyhteydet siirtävät dataa sisään sekä ulos nopeudella 100 Mbps. Valokuitu on myös täysin immuuni kaikenlaiselle häiriölle. Valokuidussa ei esiinny vuotoa eikä se reagoi esimerkiksi sähkömagneettisiin häiriöihin. Hyvänä puolena voidaan pitää myös sen nopeuden varmuutta pitkilläkin etäisyyksillä. Tämän takia valokuitutekniikka on yleisesti käytössä tehdasympäris-

töissä. Multi Mode Fiber eli monimuotokuitu sekä Single Mode Fiber eli yksimuotokuitu ovat kaksi valokaapelin päätyyppiä. Näistä päätyypeistä monimuotokuitua käytetään lähiverkkotyyppisissä ratkaisuissa kun taas yksimuotokuitua käytetetään pitkien matkojen etäisyyksiä vaativissa yhteyksissä. (Tallin university of technology 2007; Sonera 2013; Dna 2013.)

2.2.3 Reititin

Reititin on laite, jonka tarkoituksena on yhdistää ja jakaa verkon liikennettä. Reitittimen porttien oikea konfiguraatio on tärkeää. Verkon arkkitehtuurissa käytetyt protokollat keskustelevat vain keskenään. OSI-verkkomallin mukaan verkko voidaan jakaa seitsemään eri segmenttiin eli kerrokseen: fyysinen kerros, siirtoyhteyskerros, verkkokerros, kuljetuskerros, yhteysjaksokerros, esitystapakerros ja sovelluskerros. Reitittimen tarkoituksena on ohjata verkkokortilta lähetetty verkkosegmentti oikeaan liitäntään. Näin ollen reitittimen ansiosta oikeat verkkosegmentit keskustelevat keskenään ja verkossa työskentely onnistuu ja on yleensäkin mahdollista. Verkon rakenteessa esiintyvien reitittimien ja kytkimien välinen perusero on siinä, että kytkimeen yhdistetyt laitteet ovat samassa verkossa, kun taas reititin pystyy siirtämään tietoa eri verkkojen välillä. (Microsoft Windows 2013.)

2.2.4 Kytkin

Kytkin on laite, jonka tarkoituksena on ohjata verkossa tapahtuvaa liikennettä. Kytkimet ovat perusperiaatteeltaan yksinkertaisia laitteita. Perusoletuksena on, että niihin ei tarvitse tehdä mitään asetuksia manuaalisesti toimiakseen. Monissa kytkimissä on kuitenkin hallintaominaisuus, jonka avulla kytkintä voi konfiguroida tarpeiden mukaan. VLAN-määritykset ovat yleisimpiä määrityksiä, jotka tarvitsevat hallintaohjelman sekä ylläpitäjän täyden huomion toimiakseen oikein. Yleisimpiä kytkintyyppejä ovat seuraavat.

- Porttikohtaisella puskurilla varustetut kytkimet. Halvimmat ja vanhimmat kytkimet kuuluvat tähän ryhmään, jossa kytkin on varustettu porttikohtaisella puskurimuistilla. Tämä tarkoit-

taa, että jokaisella portilla on oma muisti. Tämä on ison datamäärän siirtämisessa huono ja kankea tekniikka. Yleisesti käytetään englanninkielistä nimitystä Cross Bar Switch.

- Jaetun muistin kytkimet. Kehitetty Cross Bar Switchien muistiongelmien takia. Niistä käytetään yleisesti nimitystä Shared Memory Switch, jossa kaikki portit käyttävät yhteistä keskusmuistia, jota ne käyttävät tarpeen mukaan.
- Suurnopeusväylällä varustetut kytkimet. Kutsutaan englanninkielisellä nimellä High Speed Bus Switch. Kytkimiä käytetään yleisesti eri nopeuksia käyttävien laitteiden verkossa. Suurnopeusväylällä varustetussa kytkimessä portteja yhdistää kytkentäväylä. Kytkentäväylä pystyy käsittelemään siihen lähetettyjä kehyksiä nopeammin kuin laitteet pystyvät tuottamaan niitä. (Hakala & Vainio 2005, 103-105.)

2.2.5 Ethernet

Ethernet-lähiverkkoteknologia on kehitetty 1970-luvulla Yhdysvalloissa. Lähes kaikissa Ethernet-ratkaisuissa käytetään parikaapelia siirtotienä laitteesta toiseen. Pienemmän luokan Ethernet-verkkoratkaisussa yhtenä tärkeimpänä komponenttinä toimii switch eli kytkin. Kytkin yhdistää verkossa olevat koneet toisiinsa ja ohjaa verkossa liikkuvaa dataa. Kaikki verkossa olevat koneet liitetään kytkimen portteihin. Koneet yhdistetään Ethernet-verkon kytkimeen erilaisilla kaapeliratkaisuilla. CAT-parikaapeleita on jo monia eri sukupolvia (Taulukko 1). Uusimpana on CAT-7 parikaapeli, jonka tiedonsiirtonopeus on 10 Gbps ja jossa maksimi etäisyys on kahden laitteen välillä 100 metriä. Ethernet-verkoissa mahdollinen tiedonsiirtonopeus vaihtelee verkon kuormittumisen mukaan. Mitä enemmän koneita käyttää samaan aikaan verkkoa, sitä hitaampi se on. Ethernet-verkoissa yleisimmin käytetty toimintamekanismi on CSMA/CD-access eli Carrier Sense Multiple Access with Collision Detect. Mekanismi toimii seuraavalla tavalla:

- Tietokone kuuntelee ensin onko verkko vapaa, kun tietoa haluttaisiin lähettää (Carrier Sense).
- Kone aloittaa datan lähettämisen, heti kun se on huomannut, että verkko on vapaa. Lähetettävillä paketeille on määritelty maksimikoko välttääkseen verkon tukkeutumisen liian pitkäksi aikaa.
- Datasignaalien törmäys johtuu siitä, että samaa väylää käyttää useampi kone, ja koneet lähettävät tietoa samanaikaisesti (Multiple Access).

- Törmäyksien estämiseksi datan lähettäjä "kuuntelee" väylää samalla, kun lähettää dataa. Datan lähettäjä reagoi häiriösignaaliin (Collision Detect).
- Kaikki datan lähettäjät ovat satunnaisen ajan hiljaa, kun törmäys on havaittu, ennen kun yrittävät lähettää uudestaan dataa. (Hämeen-Anttila 2003, 32-33.)

Taulukko 1. Kaapeliluokat (i&iSolutions 2013).

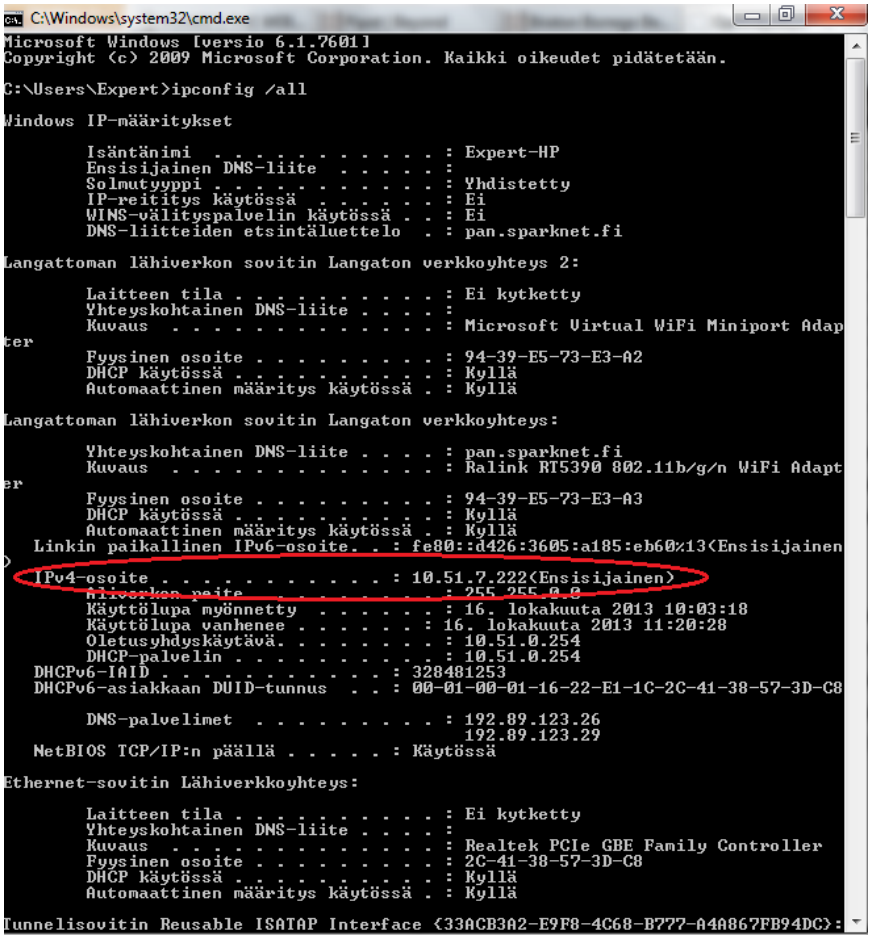
Kaapeliluokat	
Luokka	*Standardinopeus*
CAT 5	100 Mbps
CAT 5e	100 Mbps
CAT 6	1 Gbps
CAT 7	10 Gbps

2.2.6 IP-osoitteet

Jokaisella Internetiin kytketyllä tietokoneella pitää olla yksikäsitteinen tunniste eli osoite. Tämä on IP-osoite. Kansainvälisellä tasolla osoitteen jaosta vastaa IANA, kun taas kansallisella tasolla jokin teleoperaattori, Internet-palveluntarjoaja (Internet Service Provider, ISP), korkeakoulu tai jokin muu julkinen toimija. IP-osoite voidaan määritellä koneelle joko kiinteästi TCP/IP-protokollan asennuksen yhteydessä tai yhä yleisemmässä määrin verkkoon asennetun palvelimen kautta, josta organisaation palvelin antaa IP-osoitteen sitä tarvittaessa. IPv4-standardin osoitepulan johdosta on kehitetty NAT-palvelin (Network Address Translation). Tämän avulla organisaation sisällä voidaan käyttää niin sanottuja intranet-osoitteita. Näitä osoitteita ei rekisteröidä ja Internettiin kohdistuvassa liikenteessä sisäverkon osoitteet vaihdetaan joksikin rekisteröimättömäksi vapaaksi julkiseksi IP-osoitteeksi. (Hakala & Vainio 2005, 191-193.)

IPv4-standardin osoitteet koostuvat 32 bitistä ja osoitteet on jaettu neljään eri luokkaan A-E (Taulukko 2). Nämä osoitesarjaluokat on jaettu kokonsa mukaan. IPv4-standardin

osoitteiden loppumisesta on jo keskustelu pitkään. IANA jakoikin viimeiset IPv4-osoitteet alueellisille rekisteröintijärjestöille 3.2.2011. RIPE NCC alkoi taas jakaa viimeisiä osoitteitaan IPv4-poolistaan 14.9.2012. IPv4-osoitteita on yhteensä noin 4 miljardia kappaletta. IPv4-standardin osoitteiden loppumisen takia on kehitetty IPv6-standardin osoitteisto. IPv4- ja IPv6-standardin osoitteet eivät ole täysin keskenään yhteensopivia. Kuluttajan ei tarvitse huolehtia standardien siirtymisestä vaan verkkojen ja palvelujen tarjoajat huolehtivat siitä. Koneen IP-osoitteen saa vaivattomimmin selville komentokehotteen kautta komennolla ”ipconfig /all”. (Viestintävirasto 2013a). Kuvassa 2 käytössä oleva IP-osoite on rengastettu punaisella.



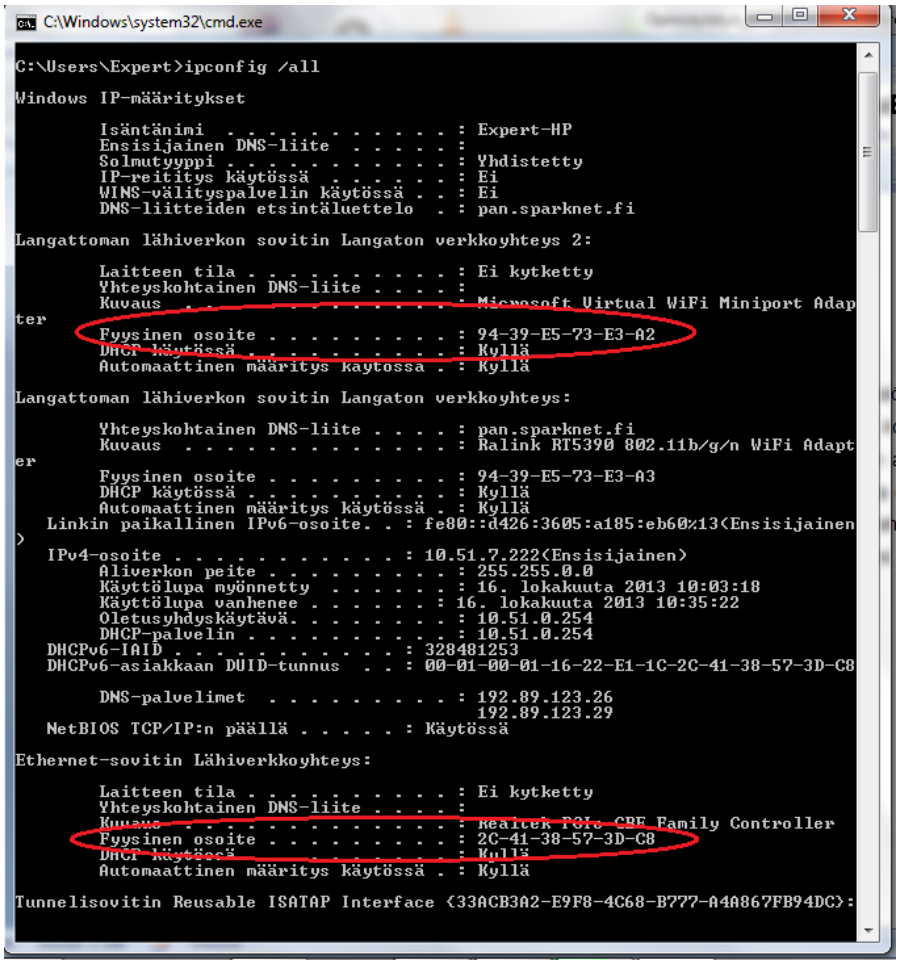
Kuva 2. IPv4-osoite komentokehotteessa.

Taulukko 2. Osoiteluokat (Hakala & Vainio, 2005).

Osoiteluokat		
Luokka	**Osoitealue**	**Koneiden määrä tai tarkoitus**
A	000.000.000.000-127.255.255.255	16 miljoonaa
B	128.000.000.000-191.255.255.255	65.534
C	192.000.000.000-223.255.255.255	254
D	224.000.000.000-239.255.255.255	Multicast-osoitteet
E	240.000.000.000-255.255.255.255	Kokeilut

2.2.7 MAC-osoitteet

Jokaisella eri verkkokortilla on oma yksilöllinen kiinteä osoitteensa. Tätä osoitetta kutsutaan MAC-osoitteeksi (Media Access Control). MAC-osoite eli fyysinen osoite toimii eräänlaisena koneen sormenjälkenä ja sen avulla pystytään varmistamaan ja jäljittämään Internet-käyttäjiä. MAC-osoitteella on tiivis kuuden heksadesimaalin esitysmuoto. Nämä kuusi tavua (48 bittiä) mahdollistavat 281 474 976 710 656 eri osoitetta. IEEE (Institute of Electronic and Electrical Engineers) toimii MAC-osoitealueiden jakelijana. Koneen MAC-osoitteen saa helpoiten selville Microsoft Windows –käyttöjärjestelmässä komentokehotteen kautta komennolla ”ipconfig /all”. Kuvassa 3 on ympyröitynä sekä langattoman verkkoyhteyden fyysinen osoite että ethernetin fyysinen osoite. (Mitchell 2013.)



Kuva 3. MAC- sekä langattoman verkkoyhteyden osoite komentokehotteessa.

2.3 Verkon dokumentointi

Organisaation hyvä dokumentaatio auttaa mahdollisissa verkon sekä tietojärjestelmien vikatilanteissa. On tyypillistä, että tietojärjestelmät sekä verkot muuttuvat jatkuvasti kehityksen myötä. Dokumentaatio auttaa ongelman paikallistamisessa. Vikatilanteiden sattuessa ongelmien rajaaminen ja paikallistaminen saattaa olla ilman hyvää dokumentaatiota työlästä ja aikaa vievää. Riittävä tieto organisaation järjestelmistä, verkosta ja käytettävissä olevista laitteista ovat pohja hyvälle ja tehokkaalle vika-analysoinnille. Tietojen määrä riippuu paljon organisaation koosta. Seuraavat asiat on hyvä olla tiedossa organisaation koosta riippumatta:

- dokumentaatio järjestelmän rakenteesta
- laitteiden ja ohjelmistojen valmistajien ja maahantuojien tiedot

- tiedot varaosien ja palveluiden saatavuudesta
- vikojen tunnistuksen ja korjauksen taito. (Jaakohuhta 2005, 325.)

2.3.1 Dokumentoinnin kohteet

Dokumentoinnin taso tulee päättää organisaation sisällä niiden henkilöiden kanssa, joilla on tietämystä organisaation järjestelmistä. Dokumentoitavat osat voivat vaihdella yrityksen koosta riippuen. Liiketoiminnan kannalta tärkeiden komponenttien on hyvä olla dokumentoinnissa, jotta ongelman paikallistaminen ja korjaaminen tapahtuisi mahdollisimman nopeasti ongelmatilanteen sattuessa. Yleisesti keskeisiä komponentteja yrityksen koosta riippumatta ovat

- verkon kaapelointi
- verkon johtotiet
- verkkoon liitoksissa olevat jakamot
- reitittimet
- kytkimet
- palomuurit
- palvelimet
- WLAN-tukiasemat
- verkossa olevien laitteiden konfiguraatiot
- sovellukset
- varmistukseen käytetyt menetelmät
- UPS-järjestelmät
- liitännät
- työasemat
- tulostimet.

Muita tärkeitä dokumentoitavia perustietoja aikaisemmin mainittujen komponenttien lisäksi ovat

- MAC - sekä IP-osoitteet
- työasemien käytössä olevien käyttöjärjestelmien versiot
- sovellusten versiot

- työasemien nimet
- laitetyypit, merkit ja mahdolliset versiot. (Jaakohuhta 2005, 325-327.)

2.3.2 Pääperiaatteet sekä toteutus

Dokumentaation toteutuksessa yleisimmin käytetyt kaksi kuvaustyyliä ovat looginen kuvaus sekä fyysinen kuvaus. Loogisen kuvauksen tavoitteena on hahmottaa organisaation järjestelmien ja verkkojen rakenne helposti laitteiden ja niiden liitäntöjen avulla. Fyysinen kuvaus selventää, miten verkko on fyysisesti rakennettu ja missä verkossa olevat komponentit todellisuudessa sijaitsevat. Verkon komponentteja ovat muun muassa kaapelit, työasemat ja tulostimet.

Dokumentointi toteutetaan pääsääntöisesti sähköisesti. CAD-ohjelmia tai korkeatasoisia piirrosohjelmia käytetään yleensä kuvaamaan kaapelointia. Näiden lisäksi on myös erityisesti verkon dokumentaatioon erikoistuneita ohjelmia, kuten esimerkiksi netViz tai Vision. Verkon dokumentointiin liittyy standardeja myös Suomessa. ST 681.41 on piirrosmerkkistandardi tietoverkkojen dokumentointiin. SFS-EN 50174-1 on standardi jossa määritellään yleiskaapeloinnin, hallinnon, korjauksen ja ylläpidon näkökohdat sekä vaatimukset. (Jaakohuhta 2005, 326-329.)

3 TIETOTURVA JA TIETOTURVALLISUUDEN TARKISTAMINEN

3.1 Tietoturvallisuuden peruskäsitteitä

Yleisesti käytetty jaottelu tietoturvallisuuden ominaisuuksista on niin sanottu CIA-malli, joka muodostuu englanninkielisistä sanoista Confidentiality, Integrity ja Availability. Nämä tunnetaan termein luottamuksellisuus, eheys ja saatavuus. Perinteiseen kolmijakoon on lisätty myös kiistämättömyys, todentaminen ja tunnistus.

Luottamuksellisuus tarkoittaa sitä, että tiedot ovat vain niihin oikeutettujen henkilöiden saatavissa ja asianomaisia tietoja ei paljasteta muille. Kukaan ei siis pääse käyttämään tietoa, jota ei ole hänelle tarkoitettu. Eheyden tarkoitus on taata tiedon virheetön käsittely. Tieto ei siis voi huomaamatta muuttua siirtämisen tai säilyttämisen aikana, eikä kukaan voi ilman lupaa muuttaa tiedostojen tai tiedon sisältöä saati poistaa sitä. Saatavuuden tarkoitus on saada tieto aina niiden käyttäjien käyttöön, jotka sitä tarvitsevat ja joille se on tarkoitettu. Saatavuuden turvaamiseen kuuluvat muun muassa tiedostojen suojaus tai varmuuskopiointi. (Viestintävirasto 2013b.)

Kiistämättömyydellä tarkoitetaan, ettei tiedon lähettäjä voi kiistää lähettäneensä tietoa tai olleensa osapuolena jossakin tapahtumassa. Kiistämättömyys on ehdoton edellytys esimerkiksi sähköisen kaupankäynnin toteuttamiselle tietoverkon kautta. Todennuksella voidaan luotettavasti varmistaa tietojärjestelmän käyttäjä oikeaksi lähettäjäksi tai vastaanottajaksi. Tunnistuksella varmistetaan osapuolen olevan oikeutettu tiedon tai palvelun käyttöön. Yleinen tunnistusmenetelmä on esimerkiksi kirjautuminen työasemalle käyttäjätunnuksella ja salasanalla. (Suomen internetopas 2013.)

3.2 Tietoturvan osa-alueet

Tietoturvasta puhuttaessa tarkoitetaan yleensä virustorjuntaohjelmistoa tai palomuuria. Tietoturva todellisuudessa käsittää huomattavasti suuremman kokonaisuuden joka on

tässä jaettu kolmeen osa-alueeseen: Tekninen tietoturva, sosiaalinen tietoturva ja fyysinen tietoturva. Tekninen tietoturva -osiossa keskitytään tietokoneen ohjelmalliseen tietoturvaan. Sosiaalinen tietoturva tuo mukaan käyttäjän osana tietoturvaa. Fyysisen tietoturvan osiossa on huomioitu muun muassa tietoturvalliset säilytystilat. (Turun Ammattikorkeakoulu 2013.)

Teknisellä tietoturvalla pyritään siihen, että käytetyissä laitteissa ja ohjelmistoissa ei ole tietoturvapuutteita. Tämä tulee ottaa huomioon jo laitteita tai ohjelmistoja hankittaessa. Teknisen tietoturvan takaamiseksi on tärkeää päivittää sekä käyttöjärjestelmä, erilaiset sovellusohjelmat että virustorjuntaohjemisto säännöllisesti.

Tärkeä osa tietoturvaa on käyttäjän tietoturva ja tähän voi jokainen itse myös helpoiten vaikuttaa. Välinpitämätön käyttäjä on tietokoneen pahin tietoturvauhka. Seuraavassa on lueteltu muutamia yleispäteviä ohjeita sosiaalisen tietoturvan parantamiseen:

- Kannettavalla tietokoneella työskentely julkisilla paikoilla: Pidä näytöllä kalvoa joka peittää näkyvyyden sivuille. Tämä estää mahdolliset urkinnat siitä, mitä koneella teet.
- Älä avaa sähköpostia ellet ole varma lähettäjästä. Liitetiedostot ovat pahimpia ”virus-pesäkkeitä”.
- Älä käytä yleisiä salasanoja kuten salasana, password tai password123.
- Älä kirjoita salasanoja paperille vaan opettele ne ulkoa. Eri tietoturvaohjelmistoilla on olemassa hyviä salasanojen säilytyssovelluksia, joihin pystyy yhden salasanan taakse tallentamaan kaikki itselleen tärkeät salasanat.
- Sosiaalisten medioiden yleistyessä on hyvä muistaa, mitä sinne kirjoittaa. Luottamuksellista tietoa ei tule jakaa ystävien kesken. (Tutkimusmedia 2013.)

Fyysiseen tietoturvaan kuuluvat olennaisesti käytössä olevat laitteet, mutta myös niiden turvallinen käyttö. Laitteistoon lukeutuvat niin ulkoiset tallennusvälineet (USB-muistit ja kiintolevyt, cd/dvd-levyt), tietokoneet, wlan-verkot kuin työhön käytettävät matkapuhelimetkin. Fyysisen tietoturvan on myös tarkoitus varmistaa, että tieto pysyy turvattuna ja tietoon ei ole pääsy kuin niillä joilla siihen on oikeus. Tällä tarkoitetaan esimerkiksi palvelinten sijoittamista paloturvalliseen huoneeseen, jonne sisäänpääsy on mahdollista ainoastaan oikeutetuilla henkilöillä. (Laaksonen ym. 2006, 125.)

3.3 Salasanakäytännöt

Tietokonetta käyttäessä tarvitsee nykyään monessa eri paikassa salasanoja. Ensimmäisenä niitä tarvitaan, kun kirjautuu käyttöjärjestelmään sisään. Sen jälkeen erilaisissa palveluissa, joita käyttäjä tarvitsee jokapäiväisessä elämässään. Näistä esimerkkeinä ovat verkkopankit, sosiaalinen media ja sähköposti. Käyttäjätunnus ja salasana ovat usein ainoa keino todentaa käyttäjä, joten salasana kannattaa suunnitella mahdollisimman turvalliseksi.

Salasanan pituuden pitäisi olla riittävä, ainakin kuusi kirjainta tai enemmän. Kannattaa myös käyttää isoja ja pieniä kirjaimia sekä numeroita. Salasanojen on hyvä olla pitkiä ja monimutkaisia, jotta hakkerit eivät voisi murtaa niitä ns. brute-force-hyökkäyksellä. Tämä tarkoittaa sitä, että hakkeri kokeilee kaikkia mahdollisia vaihtoehtoja, kunnes oikea salasana löytyy. Nopealla tietokoneella voi testata miljoonia kirjainyhdistelmiä sekunnissa. Jokainen lisäkirjain salasanan pituuteen kasvattaa murtamiseen kuluvan ajan 28-kertaiseksi, kun käytetään vain pieniä kirjaimia. Jos käytössä ovat myös isot kirjaimet sekä numerot, murtamisaika kasvaa 66-kertaiseksi. (Järvinen 2012, 115.)

Huonoja salasanoja ovat käyttäjän omat tiedot, esim. oma syntymäaika, oma lempinimi tai perheenjäsenen nimi. Jos murtautuja on tuttu, nämä asiat ovat helppoja arvata. Ei myöskään kannata käyttää omaa sähköpostiosoitettaan salasanana, sillä se on julkista tietoa. Ehdottomasti huonoin salasana on sama kuin käyttäjätunnus. Sitä murtautujat usein kokeilevat ensimmäisenä. Hakkerit käyttävät valmiita sanakirjoja salasanojen murtamiseen, joten mikään yksittäinen sana ei ole turvallinen. (Järvinen 2012, 118 – 119.)

Nykyään salasanoja tarvitaan moneen palveluun ja niiden olisi hyvä olla joka palvelussa erilaiset. Tämä auttaa lisäämään tietoturvaa, vaikka yhden palvelun salasana murrettaisiinkin. Toisaalta monen eri salasanan muistaminen on hankalaa. Silti olisi toivottavaa, ettei salasanoja kirjoitettaisi mihinkään muistiin varsinkaan työympäristössä. Työpaikoilla on usein ulkopuolisia, kuten siivoojat, jotka saattavat löytää salasanan sisältävän muistilapun näppäimistön alta.

Hyvä salasana muodostuu monesta sanasta. Sen on hyvä myös sisältää numeroita tai erikoismerkkejä ja isoja sekä pieniä kirjaimia. Hyvä tapa sisällyttää numeroita salasanaan

on korvata i-kirjain ykkösellä, e-kirjain kolmosella ja o-kirjain nollalla. Esimerkiksi sanasta erotuomari saa turvallisemman kirjoittamalla sen muotoon 3roTu0mar1.

Toinen hyvä tapa on poimia helposti muistettavasta lauseesta alkukirjaimet. Esimerkiksi ”Minä omistan kolme hassua kissaa” muuttuu salasanaksi MiOm3HaKi. (Järvinen 2012, 120.)

Salasana ja käyttäjätunnus on kannattavaa pitää aina henkilökohtaisina. Siten tietoturva pysyy parhaiten kunnossa. Jos joku yrittää puhelimitse tai sähköpostitse kysellä käyttäjältä salasanaa, on kyseessä aina huijaus. Internet-selaimeen ei kannata tallentaa salasanoja, sillä kuka tahansa samalle koneelle pääsevä voi lukea ne. (Iso riski 2013.)

Yritysten on hyvä luoda jokaiselle käyttäjälle oma käyttäjätunnus. Tämä ehkäisee tietomurtoja ja auttaa ottamaan selville, kenen käyttäjätunnuksella mahdolliset tietovuodot ovat tapahtuneet.

3.4 Tietoturvahyökkäykset

Tietoturvahyökkäykset voidaan jakaa neljään kategoriaan, joilla saadaan yhteys katkeamaan tiedon lähettäjän ja vastaanottajan välillä: Keskeytys (Interruption), Kaappaus (Interception), Muuttaminen (Modification) ja Väärentäminen (Fabrication). Keskeytyksessä hakkeri estää tiedon pääsyn vastaanottajalle. Kaappauksessa varas keskeyttää paketin perillemenon ja ottaa tiedon itselleen. Muuttamisessa hakkeri vaihtaa viestin sisältöä ennen kuin se tavoittaa vastaanottajan. Väärentämisessä ei lähettäjää välttämättä ole edes olemassa vaan varas esiintyy tiedon lähettäjänä. (Loula 2010.)

Tietoturvahyökkäyksen kohde saattaa liittyä käyttäjän identiteetin varastamiseen tai käyttäjän tietoihin. Internetissä toimivat varkaat, hakkerit, ovat kiinnostuneita pääasiassa kaikesta tiedosta, johon pääsevät käsiksi. Tieto on lähes aina arvokasta jollekin. Seuraavassa on mainittu yleisimpiä tietoturvahyökkäyksiä ja niiden toimintaperiaatteita:

- Mies välissä –hyökkäys (engl. Man-in-the-middle attack): hyökkääjä asettuu kahden osapuolen välisen tietoliikenteen välittäjäksi ja halutessaan muuttaa viestien sisältöä.
- Palvelunestohyökkäys (engl. Denial of Service, DoS): Tietyn verkkopalvelun lamauttaminen niin, että palvelu ei ole käytettävissä.

- Sähköpostihuijaukset, tietojen kalastelu (engl. phishing): Henkilökohtaisia tai yrityksen tietoja voidaan urkkia tekaistujen sähköpostiviestien tai verkkopalveluiden välityksellä. Sähköpostitse saattaa tulla aidolta vaikuttava kysely, jossa vastaanottajaa pyydetään ilmoittamaan verkkopalvelun toiminnan varmistamiseksi käyttäjätunnuksia, salasanoja ja muita henkilökohtaisia tietoja.

Tietoturvahyökkäyksiä on sekä passiivia että aktiivisia. Passiiviset hyökkäykset sisältävät mm. salakuuntelun ja monitoroinnin, jolloin tavoitteena on sisällön seuranta kuten puhelinkuuntelu tai sähköpostiseuranta. Aktiivisten hyökkäysten tavoitteena on viestin sisällön muuttaminen, esiintyminen vääränä palvelun tarjoajana, palvelun normaalin käytön tai hallinnan estäminen tai väärien viestien tuottaminen. (Loula 2010.)

3.5 Suojautuminen tietoturvahyökkäyksiltä

3.5.1 Virustorjuntaohjelmistot ja palomuuri

Virustorjunta käsittää sellaisia tietokoneohjelmia, joilla etsitään ja tuhotaan tietokoneessa olevia haitallisia ohjelmia tai tiedostoja. Virustorjunnan tehtäviin kuuluu tietokoneen puhdistamisen lisäksi estää virustartunnan leviäminen muille tietokoneille. Alla on lueteltu tunnettuja maksullisia sekä ilmaisia virustorjuntaohjelmia:

- **F-Secure Antivirus**: Maksullinen, vuonna 1988 perustettun suomalainen yrityksen virustorjuntaohjelmisto.
- **Norton Antivirus**: Maksullinen, Symantec Corporationin omistama tietoturvaohjelmisto.
- **McAfee Antivirus**: Maksullinen yhdysvaltalainen viruksentorjuntaohjelmisto.
- **Avast! Free Antivirus**: Ilmainen tšekkiläisen Avast Softwaren kehittämä virustorjuntaohjelmisto Windows- ja Linux-käyttöjärjestelmille. Saatavilla myös monipuolisempi maksullinen versio.
- **AVG Antivirus**: tsekkiläisen AVG Technologiesin valmistama virus- ja haittaohjelmien torjuntaohjelmisto. Ohjelman maksuton versio on yksityiskäyttöön tarkoitettu AVG Free, jossa on vähemmän ominaisuuksia kuin maksullisessa versiossa.
- **Avira free Antivirus**: Ohjelma on saksalaisen Avira GmbH:n valmistama virustorjuntaohjelma. Saatavilla on myös laajempi maksullinen versio.

Palomuuri on tietoverkoissa tapahtuvan tietokoneiden välisen tiedonsiirron hallintaan tarkoitettu työkalu. Palomuuri valvoo lävitseen verkosta toiseen kulkevaa tietoliikennettä ja rajoittaa tätä palomuuriin asetettujen sääntöjen mukaisesti. (Tietosuoja 2010.)

3.5.2 Sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne

Sähköisellä tunnistamisella tarkoitetaan henkilöllisyyden todentamista sähköisesti. Tällä tavoin voidaan vahvistaa henkilöllisyys erilaisissa sähköisissä palveluissa. Tunnistamisessa käytettyjä tunnistusvälineitä ovat:

- pankkien käyttämät verkkopankkitunnukset
- väestörekisterikeskuksen kansalaisvarmenne ja
- teleyritysten mobiilivarmenteet (Viestintävirasto 2013b).

Sähköistä allekirjoitusta käytetään allekirjoittajan henkilöllisyyden todentamiseen. Yksinkertaisimmillaan tämä tarkoittaa sähköpostin allekirjoittamista henkilön nimellä. Kehittyneemmässä sähköisessä allekirjoituksessa allekirjoittaja voidaan yksilöidä ja allekirjoitus liittää muuhun sähköiseen tietoon, kuten esimerkiksi sähköpostiviestiin, siten, että tiedon mahdolliset muutokset voidaan havaita. (Viestintävirasto 2013c.)

Varmenteita tarvitaan tietoverkkojen kautta tapahtuvassa tunnistamisessa, salauksessa ja sähköisen allekirjoituksen tekemisessä. Varmenteen myöntäjä allekirjoittaa sähköisesti myöntämänsä varmenteet ja siten vahvistaa niiden oikeellisuuden. (Viestintävirasto 2013c.)

4 ACTIVE DIRECTORY WINDOWS SERVER 2008 - YMPÄRISTÖSSÄ

Active Directory, suomeksi aktiivihakemisto, on Microsoftin Windows Server –käyttöjärjestelmien keskeinen palvelu. Active Directory sisältää tietoja verkon käyttäjistä, tietokoneista ja muista resursseista. Active Directoryn avulla niiden hallinta on helpompaa ja nopeampaa. Hakemistopalvelu toimii IP-osoitteiden ja DNS-protokollan avulla. Active Directoryn käyttäjät voivat etsiä resursseja verkon nimiavaruudesta. (Kivimäki 2009, 651.)

Järjestelmänvalvojan kannalta Active Directory auttaa keskittämään verkon hallintaa. Verkon käyttäjiä ja tietokoneita voidaan hallita yhdeltä tai useammalta palvelimelta erilaisilla hallintatyökaluilla. Tavalliselle verkon työaseman käyttäjälle Active Directory ei varsinaisesti näy. Käyttäjä voi kuitenkin käyttää aktiivihakemiston tarjoamia hakupalveluita. (Microsoft Technet 2013a.)

Tässä työssä keskitytään kuvaamaan lähinnä Active Directoryn Domain services –työkalua. Se mahdollistaa toimialueen luomisen ja käyttöönoton sekä hakemistopalvelut. Active Directoryssä on muitakin työkaluja, jotka eivät tässä työssä tule tarpeelliseksi. Niistä ei sen vuoksi ole tarpeen sen enempää kertoa. Tässä työssä Active Directorystä puhuttaessa viitataan juuri Active Directoryn Domain Services –työkaluun.

Active Directory mahdollistaa verkon resurssien järjestämisen hierarkiseksi rakenteeksi, jota kutsutaan loogiseksi rakenteeksi. Looginen rakenne tarjoaa monia etuja työryhmämalliseen verkkoon verrattuna. Yksi eduista on parempi tietoturva. Yksittäisille ryhmille ja käyttäjille voi jakaa erilaisia oikeuksia eri toimialueiden kesken. Muita etuja ovat yksinkertaistettu verkon hallinta, yksinkertaistettu resurssien jakaminen ja niiden ylläpidon myötä alennetut verkonhallinnan kustannukset. (Microsoft Technet 2013b.)

Loogisia rakenteita on yhteensä neljä, ja ne ovat hierarkkisessa järjestyksessä seuraavat: toimialuemetsät, toimialuepuut, toimialueet, organisaatioyksiköt. Toimialuemetsä on yhden tai useamman toimialueen muodostama kokonaisuus. Kaikilla samaan toimialuemetsään kuuluvilla toimialueilla on yhteisiä ominaisuuksia ja jokainen toimialueen käyttä-

jä pystyy kirjautumaan tarvittaessa mille tahansa metsän toimialueelle. Toimialuepuut koostuvat toimialueista, joista on muodostunut toiminnallisia rakenteita. Toimialuepuussa sijaitsevilla toimialueilla on yhteinen DNS -nimiavaruus. Toimialue on joukko työasemia, jotka jakavat yleisen hakemistotietokannan. Toimialueella on omat suojauskäytäntönsä ja luottosuhteensa muiden toimialueiden kanssa. Hierarkian alimpana on organisaatioyksikkö, joka on ryhmä toimialueen sisällä. Organisaatioyksiköiden tulisi heijastaa yrityksen organisaatiorakennetta. Niitä käyttämällä voidaan helpottaa ryhmien oikeuksien hallintaa ja ryhmäkäytäntöjä. (Microsoft Technet 2013b.)

4.1 Active Directoryn hallintatyökalut

Active Directoryn ensimmäisen ohjauspalvelimen eli Active Directory Domain Controllerin asennuksen jälkeen toimialueetta voidaan hallita keskitetysti. Hallinta tapahtuu hallintatyökaluilla, joita ovat:

- Active Directory Users and Computers
- Active Directory Domains and Trusts
- Active Directory Sites and Services
- Active Directory Group Policy Management.

Nämä työkalut löytyvät palvelimen Administrative tools –valikosta tai server manager -hallintakonsolista.

Active Directory Users and Computers –työkalulla hallitaan toimialueen ominaisuuksia. Sen tärkein ominaisuus on tehdä uusia käyttäjiä ja ryhmiä ja hallinnoida niitä. (Microsoft Technet 2013c.)

Active Directory Domains and Trusts –työkalu on tarkoitettu toimialueiden ja metsien hallintaa varten. Sillä voi määritellä toimialueiden keskinäisiä luottosuhteita sekä toimialueen ja metsän toiminnallisuustason määrittelemiseen. Toiminnallisuustaso määräytyy sen mukaan, mitä käyttöjärjestelmiä metsän tai toimialueen palvelimet käyttävät. Esimerkiksi toiminnallisuustason ollessa määriteltynä Windows Server 2008:aan, sitä vanhempia käyttöjärjestelmiä käyttäviä palvelimia ei voida järjestelmään lisätä. (Microsoft Technet 2013d.)

Active Directory Sites and Services –työkalulla voidaan hallinnoida toimipaikkoja ja aliverkkoja. Tällä työkalulla voidaan myös tarkastella hakemistopalveluita ja muokata palvelinten välistä replikointia. (Microsoft Technet 2013e.)

Active Directory Group Policy Management -konsolilla voidaan hallinnoida koko organisaation laajuisia ryhmäkäytäntöjä. Näitä voivat olla esimerkiksi salasanojen sääntöjen määrittely tai verkkolevyjen asentaminen käynnistyksen yhteydessä. (Microsoft Technet 2013f.)

4.2 Käyttäjätilit

Active Directoryn käyttäjätilit edustavat fyysisesti olemassa olevia ihmisiä. Käyttäjätilejä voi käyttää myös palvelevina tileinä joissain sovelluksissa. Käyttäjätilien avulla työaseman käyttäjä voi kirjautua toimialueelle ja käyttää organisaation verkon tarjoamia resursseja. Käyttäjä voi myös kirjautua paikalliseen koneeseen, jolloin hän käyttää tietokoneen resursseja. Käyttäjätilien pääasiallinen tarkoitus on todentaa käyttäjän identiteetti. Tarkoituksena on myös oikeuttaa tai estää käyttäjän pääsy toimialueelle tai paikallisen työaseman palveluihin.

Active Directoryn käyttäjätilit voidaan jakaa kolmeen eri pääryhmään, jotka ovat:

- järjestelmänvalvoja
- vieras
- käyttäjä.

Järjestelmänvalvojalla on täydet oikeudet kaikkiin osa-alueisiin toimialueella. Oikeuksiin kuuluu muun muassa käyttäjätilien lisääminen, käyttäjätilien muokkaaminen, verkkoasetuksien muuttaminen jne. Henkilöillä, jolla ei ole varsinaista käyttäjätiliä, voivat kirjautua toimialueelle tai koneelle vieraana eli guestina. Vierastili ei vaadi sisäänkirjautumisessa salasanaa. Vierastilin oikeuksien muokkaus tapahtuu samalla tavalla kuin normaalin käyttäjätilin. Käyttäjätili on tili, jonka järjestelmänvalvoja on luonut. Tilien määrän tarve vaihtelee organisaation koon ja tarpeen mukaan. Käyttäjätilien esisuunnittelu helpottaa huomattavasti tilien luomisprosessia. Active Directoryn käyttäjätilejä luodessa kannattaa ottaa huomioon

- tilien nimeämiskäytännöt (yhdenmukaiset käyttäjänimet)
- tilien voimassaolojat (tili voi vanheta tiettynä päivänä. esim. määräaikainen työsuhde)
- ryhmäjäsenyydet (oikeudet eri ryhmiin, joilla on eri oikeuksia)
- vahvat salasanat (mahdolliset salasanamurtautumiset)
- salasanojen vaihtokäytännöt (salasana pitää vaihtaa tietyin väliajoin)
- kirjautumisajat (mahdollisuus estää pääsy tiettyinä aikoina).

(Microsoft Technet 2013g.)

4.3 Ryhmäkäytännöt

Active Directory Group policy management -konsoli tarjoaa keskitetyn hallinnan lähes kaikkiin työaseman asetuksiin ja sovelluksiin. Ryhmäkäytännöt jakaantuvat päätasolla kahdenlaisiin asetuksiin: tietokoneasetuksiin (computer settings) ja käyttäjäasetuksiin (user settings). Käyttäjäasetukset kohdistuvat aktiivihakemistotasolla kirjautuvaan käyttäjään ja työasematasolla vastaavasti kaikkiin tietokoneisiin kirjautuviin käyttäjiin. Tietokoneasetukset sisältävät käyttäjäriippumattomia, laitteistoon ja sovelluksiin yleisellä tasolla liittyviä asetuksia. Aktiivihakemistotasolla ryhmäkäytännöt voidaan kohdistaa tarkemmin kuin työasematasolla, jolloin käytännöt vaikuttavat kaikkiin työasemaan kirjautuviin käyttäjiin. Active directoryn kanssa toteutettuna ryhmäkäytännöt mahdollistavat profiilien luomisen toimipaikka- (site), toimialue- (domain) tai organisaatioyksikkö- (Ou) tasolla. Group policy-asetukset tulevat voimaan työasemaan sen käynnistämisen (computer settings) tai käyttäjän verkkoonkirjautumisen (user settings) yhteydessä halutuin aikavälein automaattisesti. Oletusaikaväli on 90 minuuttia + 30 minuutin satunnainen viive. Jos tietokone on päällä 24 tuntia vuorokaudessa, se hakee uusimmat group policy -asetukset vähintään kahden tunnin välein. (Rousku 2005.)

5 YRITYS X:N TIETOTURVA-AUDITOINTI (SALATTU)

6 YRITYS X:N AUDITOINNISSA ILMENNEIDEN PUUTTEIDEN KORJAUS (SALATTU)

7 POHDINTA

Opinnäytetyön tavoitteena oli suorittaa tietoturva-auditointi yritykselle ja tehdä sen pohjalta parannusehdotuksia. Lisäksi osa parannusehdotuksista myös toteutettiin. Jokaisen parannusehdotuksen toteuttaminen olisi ollut liian laaja tehtävä jopa kolmen hengen opinnäytetyöksi. Tästä syystä valitsimme tehtäväksi muutokset, jotka oli järkevää toteuttaa ensimmäiseksi. Nämä muutokset olivat verkon dokumentointi, verkon rakennemuutos sekä virustorjunnan keskittäminen.

Tietoturva on viime vuosina paisunut niin laajaksi kokonaisuudeksi, että harva asiaan perehtymätön enää ymmärtää sen kaikkia osa-alueita. Tämä on avannut uusia liiketoimintamahdollisuuksia. Moni yritys myy nykyään tietoturva-auditointeja.

Opinnäytetyö onnistui ryhmältämme lopulta hyvin. Työn laajuuden vuoksi opimme asioita monelta osa-alueelta. Työn ansiosta meille on tullut tutuksi niin teoriassa kuin käytännössä Windows Server 2008 -käyttöjärjestelmän ominaisuudet, verkon oikeaoppinen dokumentointi sekä tietoturva-asiat. Ryhmämme jäsenten osaamistaso oli erilainen. Yksi tiesi enemmän tietoturvasta, toinen taas lähiverkoista. Tämän ansiosta jokainen pääsi jakamaan tietoaan ja ammentamaan toiselta uutta.

LÄHTEET

D-Link 2013. ADSL2+ Ethernet Modem. Viitattu 8.10.2013. http://www.dlink.com/fi/fi/home-solutions/connect/modems-and-gateways/dsl-320b-adsl-2-ethernet-modem.

Dna 2013. Liityntätekniikat. Viitattu 8.10.2013 http://www2.dna.fi/fi/yrityksille/yrityslaajakaista/liityntatekniikat.

FiCom 2013. ADSL. Viitattu 8.10.2013. http://www.ficom.fi/tietoa/tietoa_4_1.html?Id=1045051770.html.

Hakala, M & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo.

Hämeen-Anttila, T.2003. Tietoliikenteen perusteet. Jyväskylä: Docendo.

i&isolutions 2013. Lähiverkon tekniikka. Viitattu 10.10.2013. http://www.i-isolutions.fi/liitteet/ii/materiaalipankki/51.pdf.

Iso riski: Chrome ja Firefox tallentavat salasanat luettavina. Digitoday. 2013. Viitattu 25.9.2013 http://www.digitoday.fi/tietoturva/2013/08/07/iso-riski-chrome-ja-firefox-tallentavat-salasanat-luettavina/201310970/66.

Jaakkohuhta, J. 2005. Lähiverkot - Ethernet. Helsinki: IT Press.

Järvinen, P. 2012. Arjen tietoturva: vinkit & ratkaisut. Jyväskylä: Docendo.

Kivimäki, J. 2009. Windows Server 2008 R2, Tehokas hallinta. Hämeenlinna: readme.fi.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita.

Loula, P. 2010. Information security management. Pori: Tampereen teknillinen yliopisto. Viitattu 9.10.2013 http://www.pori.tut.fi/~loula/TLTP3110%20part%202.pdf.

Microsoft TechNet 2013a. Active Directory. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/bb742424.aspx.

Microsoft TechNet 2013b. Active Directory. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/cc759073%28v=WS.10%29.aspx.

Microsoft TechNet 2013c. Active Directory Users and Computers. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/cc754217.aspx.

Microsoft TechNet 2013d. Active Directory Domains and Trusts. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/cc770299.aspx.

Microsoft TechNet 2013e. Active Directory Sites and Services. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/cc730868.aspx.

Microsoft TechNet 2013f. Active Directory Group Policy Management Console. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/cc753298.aspx.

Microsoft TechNet 2013g. Understanding User Accounts. Viitattu 25.11.2013. http://technet.microsoft.com/en-us/library/dd861325.aspx.

Microsoft Windows 2013. Mitä eroa on keskittimellä, kytkimellä, reitittimellä ja tukiasemalla? Viitattu 11.12.2013. http://windows.microsoft.com/fi-fi/windows/hubs-switches-routers-access-points-differ#1TC=windows-7&section_3

Mitchell, B. 2013. Introduction to MAC addresses. About.com. Viitattu 11.12.2013. http://compnetworking.about.com/od/networkprotocols/a/introduction-to-mac-addresses.html.

Rousku, K. 2005. Työasemat ruotuun ryhmäkäytännöillä. MikroPC. Viitattu 26.11.2013. https://mikropc.net/nettilehti/pdf/0303200540.pdf.

Sonera 2013. Valokuidun etuja. Viitattu 8.10.2013. http://www.sonera.fi/nettiyhteydet/kotiin/ylivoimainen+valokuitu/.

Suomen Internetopas. 2013. Tietoturva. Viitattu 4.12.2013. http://www.internetopas.com/yleistietoa/tietoturva.

Tallin university of technology, 2007. Valokaapelien rakenne ja toiminta. Viitattu 8.10.2013. http://www.tlu.ee/~matsak/telecom/lasse/fibre_cables/valokaapelien_rakenne_ja_toiminta.html.

Tietosuoja 2010. Palomuuri, mikä se on? Viitattu 26.11.2013. http://www.tietosuoja.fi/uploads/khezzfmwctbvp.pdf.

Tuokko, M. 2012. Lähiverkon suunnittelu ja rakentaminen yksityiskäyttöön. Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turku: Turun ammattikorkeakoulu.

Turun Ammattikorkeakoulu 2013. Tietoturvapäivä. Viitattu 18.11.2013. http://www.tietoturvapaiva.fi/index.php?page=tietoturvainfo.

Tutkimusmedia 2013. Tietoturvaopas. Viitattu 18.11.2013. http://tutkimusmedia.fi/tietoturva.html#.

Viestintävirasto 2013a. Viitattu 11.10.2013. https://www.viestintavirasto.fi/internetpuhelin/internet/ip-osoitteet.html.

Viestintävirasto 2013b. Ohjeita viestinnän suojaamiseen. Viitattu 4.12.2013. https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeettulkinnatsuosituksetjaselvitykset/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohjeitaviestinnansuojaamiseen.html#yleisimminkaytetytpalvelutniidenkayttoonliittyvatuhatjaniiltasuojautuminen.

Viestintävirasto 2013c. Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne. Viitattu 16.11.2013. https://www.viestintavirasto.fi/tietoturva/sahkoinentunnistaminenjaallekirjoitus.html.