OPINNÄYTETYÖ

JUHANI JOENSUU 2012

PALVELINTURVALLISUUS PK-YRITYKSEN NÄKÖKULMASTA

Rovaniemen
ammattikorkeakoulu
University of Applied Sciences
LUC

TIETOTEKNIIKKA

Rovaniemen
ammattikorkeakoulu
University of Applied Sciences
LUC

ROVANIEMEN AMMATTIKORKEAKOULU

TEKNIIKAN JA LIIKENTEEN ALA

Tietotekniikka

Opinnäytetyö

PALVELINTURVALLISUUS PK-YRITYKSEN NÄKÖ-KULMASTA

Juhani Joensuu

2012

Toimeksiantaja Rovaniemen ammattikorkeakoulu

Ohjaaja Kenneth Karlsson

Hyväksytty __/__2012

Rovaniemen
ammattikorkeakoulu
University of Applied Sciences
LUC

Tekniikka ja liikenne
Tietotekniikka

Opinnäytetyön
tiivistelmä

Tekijä Juhani Joensuu Vuosi 2012

Toimeksiantaja
Työn nimi Palvelinturvallisuus PK-yrityksen näkökulmasta
Sivu- ja liitemäärä 42

Opinnäytetyön tavoitteena oli syventää asiantuntemusta Windows-palvelimista ja perehtyä turvallisen palvelinympäristön rakentamiseen liittyviin asioihin. Työ keskittyi Windows Server 2008 R2 -palvelimen turvallisiin konfigurointiasetuksiin ja palvelimen tietoturvatasoa mittaaviin ohjelmiin.

Opinnäytetyössä kerrotaan käytännönläheisesti ja tietoturvallisuutta painottaen, mitä asioita pitää ottaa huomioon palvelimen asennuksessa ja perusasetusten määrittelyssä, sekä selvitetään koventamisprosessin vaiheita. Työtä varten asennettiin ja määritettiin toimintavalmiiksi Windows Server 2008 R2 -palvelinkäyttöjärjestelmä.

Koventamisprosessin jälkeen palvelimen tietoturvataso mitattiin analysointiohjelmien avulla. Työhön käytettiin Microsoft Baseline Security Analyzer- ja GFI LanGuard -tietoturvan mittausohjelmaa. Tarkistukset tehtiin järjestelmällisesti useita kertoja molemmilla ohjelmilla. Analysointiohjelmien asennus ja niiden käyttö kuvataan opinnäytetyössä. Mittaustulokset esiteltiin ja analysoitiin opinnäytetyössä avoimesti, koska kyseessä ei ollut varsinaisesti käytössä oleva palvelin.

Opinnäytetyö saavutti sille asetetut tavoitteet ja työ lisäsi tietämystä palvelimista paljon. Opinnäytetyön tuloksena syntyi opasmainen selvitys turvallisen Windows-pohjaisen palvelinympäristön rakentamisesta.

Avainsanat Windows-palvelin, Microsoft Baseline Security Analyzer, GFI LanGuard, haittaohjelmat, tietoturva

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

School of Technology Abstract of Thesis
Information Technology Programme

Author Juhani Joensuu Year 2012

Commissioned by
Subject of thesis Server Security in a Small and Medium-sized Enterprise
Number of pages 42

The goal of this thesis was to acquire knowledge about the Windows-based servers and to become familiar with the construction of a secure server environment. The thesis focused on the secure configuration settings for the Windows Server 2008 R2 and also the programs that scan the data security level of the server.

This thesis discussed what should be considered in the installation of the server and the basic setting. The emphasis was on the practical aspects and the security issues. The thesis also discussed the steps in server hardening. The Windows Server 2008 R2 operating system was installed and configured.

After the process of the server hardening, the level of the server data security was scanned by analysis programs. The Microsoft Baseline Security Analyzer and the GFI LanGuard security scanner programs were used for this work. Checks were done systematically several times with both the programs. The analysis programs installation and use were describes in the thesis. The results were openly displayed and analysed in the thesis, because the server was not actually in use.

The goals of the thesis were achieved and knowledge of servers was increased. Finally, the result of this thesis was a guide for the construction of a Windows-based server environment.

Key words Windows server, Microsoft Baseline Security Analyzer, GFI LanGuard, malware, data security

SISÄLTÖ

KUVIOLUETTELO

1 JOHDANTO

Opinnäytetyön tavoitteena oli tutustua turvallisen palvelinympäristön rakentamiseen ja perehtyä palvelinkäyttöjärjestelmien tietoturvatasoa mittaaviin ohjelmiin. Opinnäytetyö voi myös toimia ohjeena yrityksille ja organisaatioille palvelinympäristön tietoturvallisuuden parantamisessa.

Opinnäytetyön asiasisältö jakautuu kolmeen lukuun. Ensimmäisessä luvussa käsittelen tietoturvallisuutta yleisellä teoriatasolla. Esittelen yleisimpiä haittaohjelmia ja kerron, kuinka tietoturvauhkia pystytään torjumaan. Toisessa luvussa alkaa käytännöntyön osuus. Käytännön osuudessa kerron tietoturvallisuusnäkökulma huomioonottaen Windows-palvelinkäyttöjärjestelmän asennuksesta ja käyttöönotosta sekä selvitän palvelimen koventamisprosessin vaiheita. Kolmannessa luvussa tutkin palvelimen tietoturvan analysointiohjelmia. Esittelen analysointiohjelmien toimintaa ja käyn läpi niiden tarkistustuloksia.

Opinnäytetyö esittää, mitä asioita palvelinympäristön turvaamisessa pitää ottaa huomioon ja kuinka Windows Server 2008 R2 -käyttöjärjestelmä asennetaan ja määritetään tietoturvalliseksi. Windows-palvelin sisältää erittäin paljon eri asetuksia ja ominaisuuksia, joten olen keskittynyt vain tärkeimpinä katsomieni asetusten määrittämiseen. Käyttöjärjestelmäksi valitsin Windows Server 2008 R2 -käyttöjärjestelmän, koska se on yrityksissä ja organisaatioissa laajasti käytetty. Palvelimen tietoturvamittaukset tein ilmaisella Microsoft Baseline Security Analyzer -ohjelmalla sekä maksullisella, mutta ilmaisen kokeiluversion sisältävällä GFI LanGuard -ohjelmalla.

Opinnäytetyön toimeksiantajana toimi Rovaniemen ammattikorkeakoulu ja ohjaajana Kenneth Karlsson. Idea opinnäytetyöhön kehitettiin yhdessä ohjaavan opettajan kanssa. Tavoitteena oli laajentaa ja syventää tietämystäni palvelinympäristöstä ja palvelimiin liittyvistä tietoturva-asioista. Aiheen ajankohtaisuutta ja kiinnostavuutta lisäsivät viimeaikaiset tietomurrot eri organisaatioiden palvelimille ja näiden tapahtumien pohjalta syntyneet keskustelut aiheesta, onko yritysten palvelinturvallisuuteen keskitytty sen edellyttämällä tärkeydellä.

2 TIETOTURVAUHKAT

2.1 Tietoturvallisuus yleisesti

Tietoturvallisuudesta huolehtiminen on yksi tärkeä osa yritysten ja organisaatioiden toimintaa. Tietomurtohyökkäyksiä kohdistetaan kasvavassa määrin yrityksiä ja yhteisöjä vastaan. Hyökkäyksillä hakkerit yrittävät esimerkiksi kaataa organisaatioiden internet-sivustoja tai varastaa verkkokaupan käyttäjien salasanoja ja käyttäjätunnuksia. Varastettuja tietoja hakkerit saattavat myöhemmin levittää luvattomasti internetissä. Tällaisten tekojen jälkeen yritysten maine ja tulevaisuus voi olla vakavasti vaakalaudalla. Tietomurron jälkeen yritys saattaa myös joutua maksamaan suuriakin rahallisia korvauksia eri tahoille.

Tietoturvallisuus muodostuu yleisesti tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä. Tämä jako pohjautuu tiedon klassiseen arvoon perustuvaan luokitukseen. Luottamuksellisuudella tarkoitetaan, että tiedot ja järjestelmät ovat saatavilla vain niille käyttäjille, joille ne ovat tarkoitettu, eivätkä ulkopuoliset pysty niitä käyttämään. Tietojen eheys tarkoittaa tietojen ajantasaisuutta, oikeellisuutta ja luotettavuutta. Käytettävyydellä tarkoitetaan, että tietojen pitää olla niihin oikeutettujen käyttäjien saatavilla. Tietoturvallisuuden määritelmää on myöhemmin täydennetty sisältämään kiistämättömyys ja pääsynvalvonta. Tietoa tallentava tai käyttävä henkilö pitää olla tunnistettavissa kiistämättömästi, myös oikeudellisessa tilanteessa, jossa henkilö yrittää kiistää käyttäneensä tai muokanneensa tietoa. Pääsynvalvonnan avulla estetään ulkopuolisten henkilöiden pääsy käyttämään heille kuulumattomia tietoja. (2, 4–5.)

Tietoturvauhkat

Tietoturvallisuusuhkat voidaan jakaa ulkoisiin ja sisäisiin uhkiin. Ulkopuolelta tulevat uhkat tulevat internetin välityksellä. Tällaisia ovat esimerkiksi virukset, madot ja troijalaiset sekä luvattomat murtautumisyritykset palvelimille. Sisäpuolelta tulevia uhkia ovat esimerkiksi yrityksen tai organisaation työntekijät, jotka yrittävät kirjautua luvatta yrityksen palvelimelle. Sisäpuolelta tulevassa

hyökkäyksessä murtaudutaan yrityksen sisäverkon kautta tai fyysisesti suoraan palvelinhuoneessa. Murtautuja yrittää päästä käyttämään yrityksen salaisia tietovarastoja, joihin hänellä ei ole normaalisti pääsyä. (8, 7.)

Tietoturvasuunnitelma

Hyvä tietoturvallisuus vaatii jatkuvaa ja järjestelmällistä kehitystä. Organisaatiolla onkin hyvä olla tietoturvasuunnitelma. Suunnitelmassa kerrotaan tavoiteltava tietoturvataso ja siihen edellyttävät ratkaisut ja laitteet. Tietoturvasuunnitelmassa kerrotaan myös esimerkiksi, miten yritys on hoitanut palvelinten suojaamisen ja kuka siitä on vastuussa. Tietoturvasuunnitelmassa määritellään lisäksi riskiluokat ja uhkasuunnitelma. Riskiluokan mukaan määritellään erittäin tärkeää tietoa sisältävä palvelin, joka ei saa joutua hakkeroiduksi. Riskialttiin palvelimen suojaaminen vaatii tavanomaista korkeampaa panostusta tietoturvalaitteisiin ja tiukemmat tietoturva-asetukset. (8, 6–7.)

2.2 Palomuurit

Palomuurien tehtävä on suodattaa kahden erillisen verkon välistä liikennettä. Ulkoverkosta (internet) tulevaa ja sisäverkosta (intranet) lähtevää haitallista verkkoliikennettä. Hyvin toimivan palomuurin on tarkoitus päästää läpi vain toivottu liikenne ja estää kaikki muu liikenne. Jotta palomuuri saadaan toimimaan toivotulla tavalla, pitää siihen määritellä huolellisesti suodatussäännöt. Palomuurin käytön perustana on, että kaikki liikenne kulkee sen kautta, eikä mikään verkkoliikenne pääse ohittamaan palomuuria. (8, 64–72.)

Palomuurit toimivat joko ohjelmallisena tai erillisessä laitteessa. Ohjelmallinen palomuuri voi toimia käyttöjärjestelmään integroituna tai tietokoneeseen asennettuna erillisenä palomuuriohjelmistona. Erillistä palomuurilaitteistoa kutsutaan rautapalomuuriksi. Rautapalomuuri sisältää myös palomuuriohjelmiston. Yrityskäytössä yleisin ratkaisu on erillinen palomuurilaitteisto. Palomuuritoiminto voidaan yhdistää myös osaksi reititintä, joka soveltuu kevyeen käyttöön. (5, 109; 8, 64.)

Palomuuri voidaan toteuttaa kolmella eri toteutusratkaisulla: pakettisuodatuksella, välityspalvelimella tai sovellustason yhdyskäytävällä. Pakettisuodatuspalomuuri (*packet filtering*) on yleisin käytössä oleva palomuurityyppi. Pakettisuodatuspalomuuri tutkii verkkoliikennettä jokainen tietoliikennepaketti kerrallaan ja päättää, estetäänkö vai päästetäänkö paketti läpi. Suodatuspäätös perustuu pakettisuodatuspalomuuriin asetettujen sääntöjen perusteella. Sääntölista (suodatussääntö, *filter rule*) sisältää määritykset, joiden mukaan suodatus tapahtuu. Asetuksiin pystyy määrittämään esimerkiksi lähde- ja kohde-IP-osoitteet porttinumeroineen, protokollat (yleensä UDP, TCP ja ICMP) sekä suodatettavan liikenteen suunnan. Kaikki liikenne, joka tulee listan ulkopuolelta olevasta osoitteesta, estetään. Sääntölista kannattaa pitää mahdollisimman lyhyenä ja tarkkaan määriteltynä, jotta vältytään sääntöristiriidoilta ja turhilta avonaisilta porteilta. (2, 187–188; 8, 65–66.)

Palomuurina voidaan käyttää myös välityspalvelimeksi kutsuttua palomuurityyppiä eli proxy-palvelinta. Sisäverkon ja julkisen verkon liikenne kulkee palvelimen eli proxyn kautta. Esimerkiksi internet-sivut kierrätetään proxy-palvelimen kautta ennen niiden päätymistä käyttäjän internet-selaimelle. Proxy-palvelin vaatii, että siihen määritellään etukäteen kaikki käytettävät sovellusprotokollat. Proxy-palvelimen heikkouksina on liikenteen hidastuminen ja tunkeutumisyritykset, joissa haitallinen liikenne naamioidaan näyttämään harmittomalta. (2, 187; 8, 71–72, 61–62.)

Kaikissa palomuurityypeissä ovat omat heikkoutensa, jonka vuoksi palomuurin toimintaa tulee tarkkailla säännöllisesti. Ruohonen (8, 65–72) kertoo, että valvontaa auttaa palomuurin keräämät lokitiedostot. Lokitiedostoihin palomuuri tallentaa tietoa sen läpi kulkevasta liikenteestä. Lokitiedostot sisältävät yleensä kuvauksen palomuurin läpi kulkevista paketeista ja palomuurin tekemän päätöksen, hylättiinkö paketti vai välitettiinkö se eteenpäin. Lokitiedostoja tutkimalla voidaan varmistaa palomuurin toiminta ja havaita mahdolliset murtoyritykset.

Windows Server 2008 R2 -käyttöjärjestelmän omaa palomuuria on käsitelty tarkemmin luvussa *3.2.3 Windows Server 2008 R2 -palomuuri*.

2.3 IDS/IPS

IDS

Tunkeilijan havaitsemisjärjestelmien eli IDS-järjestelmien (*Intrusion Detection System*) tavoitteena on havaita tietoverkkoon kohdistuva hyökkäys ja hälyttää niistä yhdelle tai useammalle tietokoneelle. Ilmoitus tietomurrosta voidaan asettaa hälyttämään esimerkiksi ylläpitäjän tietokoneen näytölle, sähköpostiin tai kännykkään. (8, 86, 93.) IDS-järjestelmän keräämien tietojen avulla murtoyrityksen tekevä henkilö on myös mahdollista jäljittää. IDS-järjestelmillä ei ole tarkoitus korvata palomuureja, vaan niitä käytetään palomuurien rinnalla. Tunkeilijan havaitsemisjärjestelmien avulla pyritään löytämään myös ne hyökkäykset, jotka saattaisivat päästä palomuurien läpi.

IDS-järjestelmät voidaan jakaa kahteen ryhmään niiden sijoittelun mukaan. Verkkopohjaisiin (*NIDS, Network-based IDS*) tai tietokonepohjaisiin IDS-järjestelmiin (*HIDS, Host-based IDS).* Verkossa on suositeltavaa käyttää molempia järjestelmiä yhtä aikaa. Verkkopohjainen IDS-järjestelmä sijoitetaan verkossa olevaan tietokoneeseen, jonka tehtävänä on tutkia verkkoliikenteen paketteja. Tietokonepohjainen IDS-järjestelmä on tietokoneen toimintaa tarkkaileva järjestelmä. Se analysoi tietokoneen lokitiedostoja ja tarkkailee järjestelmän muutoksia. (8, 86–94.)

Tunkeutumisyritysten havaitsemiseen IDS-järjestelmät käyttävät kahta menetelmää hyväkseen. Nämä ovat väärinkäytösten tunnistaminen (*misuse detection* tai *signature-based detection*) tai poikkeavuuksien tunnistaminen (*anomaly detection*). Väärinkäytösten tunnistamismenettelyssä IDS-järjestelmä pyrkii havaitsemaan tunkeutumisyritykset tiettyjen hyökkäysmallien perusteella. Poikkeavuuksien tunnistamismenettelyssä IDS-järjestelmä tarkkailee järjestelmän toimintaa ja vertaa, onko toiminta tavanomaista vai normaalista poikkeavaa. (8, 91–93.)

IDS-järjestelmien heikkouksina on turhien hälytysviestien lähetys ja IDS-järjestelmiä pystytään huijaamaan muokkaamalla haitallinen liikenne näyttä-

mään sallitulta liikenteeltä. IDS-järjestelmillä voi myös olla vaikeuksia ehtiä tarkistaa kaikki vilkkaasti liikennöidyn verkon paketit. (8, 86–93.)

IPS

Tunkeutumisenestojärjestelmä eli IPS-järjestelmä (*Instrusion Prevention Systems*) pyrkii tunnistamaan ja estämään yrityksen verkkoon kohdistuvat hyökkäykset. IPS-järjestelmä on IDS-järjestelmän jälkeen kehitetty tietoturvallisuutta parantava tekniikka. Näitä verkon suojausjärjestelmiä on tarkoitus käyttää yhdessä. Olennaisin ero IDS- ja IPS-järjestelmien välillä on, että IPS-järjestelmässä kaikki verkkoliikenne kulkee sen läpi. Tämän vuoksi IPS-järjestelmä pystyy myös haitallisen liikenteen torjuntaan ja voi tarvittaessa katkaista tunkeilijan yhteyden. IPS-järjestelmä asennetaan tietoverkon solmupisteeseen, jossa yhteyksiä on rajallinen määrä. Tyypillinen sijoitus on internetin ja yrityksen sisäverkon yhtymäkohta, reitittimen ja palomuurin välissä olevat linkit. Yrityksen verkon reunalla IPS-järjestelmä kykynee tehokkaasti suodattamaan sisään ja ulospäin tulevasta liikenteestä nollapäivähyökkäykset, virukset ja madot. (1, 1–6; 3, 4–10.)

IDS- ja IPS-järjestelmien yhteiskäyttö tehostaa yrityksen verkon valvontaa ja hallintaa. Hyvin määriteltyjen ja oikeaan paikkaan asennettujen IDS- ja IPS-järjestelmien avulla tunkeilijat pidetään tehokkaasti pois yrityksen verkosta ja verkon käyttökatkoksista aiheutuvat kustannukset pienenevät. Uusien ohjelmien ja teknologioiden käyttöönoton yhteydessä on tärkeää, että IPS/IDS-järjestelmät säädetään hyväksymään sallittu liikenne. (3, 10, 9, 4.)

2.4 Virustorjunta

Kaikissa yrityksen tietokoneissa tulee olla ajan tasainen ja mahdollisimman automaattisesti käyttäytyvä virustorjuntaohjelma (8, 226). Virustorjuntaohjelmaa käytetään yhdessä palomuurin kanssa. Palomuurit osaavat suodattaa haitallista verkkoliikennettä, mutta ne eivät pysty havaitsemaan jo koneelle päässyttä haittaohjelmaa. Tähän tarkoitukseen tarvitaan virustorjuntaohjelmaa, joka tutkii esimerkiksi sähköpostien liitetiedostot ja muistitikulla olevat tiedostot virusten varalta.

Erilaisia viruksia on maailmalla valtavia määriä ja joka päivä tehdään lisää. Virustorjuntaohjelmat pystyvät tunnistamaan uuden viruksen vasta, kun se on tutkittu ja viruksesta on kehitetty tunnistetiedot. Tämän vuoksi virustorjuntaohjelman virustietokanta tulee päivittyä säännöllisesti. Päivitystahti voi olla esimerkiksi kerran viikossa tai kerran päivässä. Virustorjuntaohjelman päivitystiheyden määrittämisessä tulee ottaa huomioon virustorjuntaohjelman käyttökohde ja virusten ajankohtainen leviämistilanne. Virustietokantojen päivitysten ei tule häiritä käyttäjien työskentelyä, mutta esimerkiksi sähköpostipalvelin vaatii tiheästi päivittyvän virustorjunnan. (8, 227.) Ajankohtaisia tietoturvauutisia voi seurata esimerkiksi Viestintäviraston ylläpitämästä Cert-fi -sivustolta.

Yritysten virustorjunta voidaan hallita keskitetysti. Keskitetty hallinta helpottaa virustorjuntaohjelmien asennuksia ja ylläpitoa. Keskitetyn hallinnan avulla myös tietoturvapäivitykset voidaan jakaa palvelimelta käsin, mikä vähentää verkon kuormitusta. (7; 8, 227.)

2.5 Haittaohjelmat

Haittaohjelmat (*malware)* ovat epätoivottuja ohjelmia, jotka asentuvat salaa käyttäjän tietokoneelle. Haittaohjelmia kehitetään koko ajan lisää ja niiden määrä on kasvanut räjähdysmäisesti muutaman viime vuoden aikana. Haittaohjelmien tekijät ovat pääsääntöisesti vaihtuneet amatöörikoodareista ammattilaisrikollisiin. Osa haittaohjelmista aiheuttaa vain pientä kiusaa käyttäjälle, mutta esimerkiksi näppäimistökaapparien avulla rikolliset saattavat tyhjentää uhrin pankkitilin tai voivat päästä kirjautumaan luvatta yrityksen palvelimille. Yleisimpiä haittaohjelmien pääsykeinoja tietokoneelle ovat sähköpostien liitetiedostot, käyttöjärjestelmän ja internetselaimen aukot ja muistitikut. (5, 77–89.)

Virukset

Tietokonevirukset ovat useimmiten haittatarkoitukseen tehtyjä pieniä tietokoneohjelmia. Virukset kykenevät monistamaan itsestään uusia kopioita ja ne

on naamioitu toisen, harmittomalta vaikuttavan ohjelman tai tiedoston sisään. Virus ei pysty toimimaan itsenäisesti, vaan vaatii aina toimiakseen toisen tiedoston tai ohjelma johon tarttua. Ohjelmaa tai tiedostoa, johon virus on tarttunut, kutsutaan saastuneeksi. Virukset voivat toimia monella tavalla ja aiheuttaa haittaa eri tavoin. Ne saattavat sekoittaa käyttöjärjestelmän täydellisesti tai poistaa tiedostoja. On myös suhteellisen harmittomia viruksia. Ne tekevät monenlaisia temppuja, kuten esittävät näytöllä tekstiä tai kuvia. Virukset leviävät tavallisesti sähköpostin liitetiedostojen, muistitikkujen ja netistä ladattujen ohjelmien ja tiedostojen välityksellä. (8, 345–347.) Viruksia kehitetään jatkuvasti lisää, joten virustorjuntaohjelmien haasteena on tehdä viruksia vastaan uusia tunnistetietoja.

Madot

Madot ovat virusten kaltaisia haittaohjelmia. Viruksista poiketen madot pystyvät toimimaan itsenäisesti erillisinä ohjelmina ja ne aktivoituvat automaattisesti. Myös madot osaavat kopioida itseään. Madot leviävät useimmiten sähköpostien välityksellä ja ne käyttävät hyväksi käyttöjärjestelmien ja sovellusten tietoturva-aukkoja. (5, 88.) Madot saattavat myös aiheuttaa monenlaista tuhoa ja harmia järjestelmiin, mutta yleensä niiden tarkoituksena on vain levitä mahdollisimman laajasti (8, 353).

Troijan hevoset ja takaportit

Troijan hevonen on haittaohjelma matojen ja virusten tapaan. Troijan hevonen näyttäytyy käyttäjälle normaalina ja vaarattomana ohjelmana. Tällä tavoin se harhauttaa tietokoneen käyttäjää asentamaan troijalaisen ja käyttämään sitä. Troijan hevoset aiheuttavat monenlaista tuhoa ja harmia aktivoituessaan. Ne jättävät esimerkiksi tietokoneelle takaportteja ja poistavat tiedostoja. (8, 354.) Takaportti tarkoittaa järjestelmään jätettyä ovea (takaovi), jonka hakkeri jättää auki murtautuessaan tietokoneelle. Takaportin kautta hakkereilla ja haittaohjelmilla on myöhemmin helppo päästä järjestelmään sisälle. (8, 344.) Troijan hevosten välttämiseksi ohjelmien asentamisessa ja latauksessa kannattaa noudattaa varovaisuutta ja ohjelmat tulee ladata vain luotetuista lähteistä.

Vakoiluohjelmat

Vakoiluohjelma (*spyware)* on tietokoneelle piiloutunut ohjelma, jonka tarkoituksena on yrittää selvittää käyttäjästä tietoa ja levittää niitä eteenpäin. Vakoiluohjelma etsii tietoja käyttäjän tottumuksista ja internet-sivuista, joilla käyttäjä on vieraillut. Kerättyjä tietoja lähetään eri yrityksille ja esimerkiksi mainontaa voidaan kohdistaa tietojen avulla. Käyttäjä saattaa asentaa vakoiluohjelman huomaamatta jonkun toisen ohjelman asennuksen mukana. Vakoiluohjelman asentamisesta on yleensä maininta, mutta niiden ilmoitukset jäävät monesti huomaamatta. (5, 78–80, 99–100.) Vakoiluohjelmat eivät tavallisesti aiheuta järjestelmän toiminnalle merkittävää haittaa, mutta vaarantavat käyttäjien tietosuojan ja ovat varsinkin yrityskoneissa haitallisia.

Näppäimistökaapparit

Näppäimistökaappari (*keyboard logger)* tallentaa muistiin kaikki tietokoneen käyttäjän tekemät näppäimistöpainallukset. Ohjelman avulla rikolliset pyrkivät selvittämään erityisesti verkkopankkien salasanoja ja käyttäjätunnuksia. Tallennetut tiedot näppäimistökaappari lähettää joko sähköpostiviestinä tai IRC-ohjelmalla. Näppäimistökaapparien avulla myös palvelimille murtautuminen on helpompaa selvitettyjen salasanojen vuoksi. (5, 89.)

3 PALVELIMEN TURVALLISUUS

3.1 Palvelin

Palvelimella (*server)* tarkoitetaan tietokonetta, johon on asennettu palvelinkäyttöön suunniteltu käyttöjärjestelmä tai palvelinohjelma. Palvelintietokone palvelee verkon muita tietokoneita (asiakastietokoneet) tarjoamalla niille verkon välityksellä erilaisia palveluja. Yleisimpiä palvelimella ajettavia palveluja ovat muun muassa tulostuspalvelu, tiedostojenjakopalvelu, sähköpostipalvelu ja DNS-nimipalvelu. Tulostuspalvelun avulla palvelimeen kytkettyjen tulostimien käyttö onnistuu verkon muilta tietokoneilta. Tiedostojenjakopalvelulla jaetaan ja hallitaan keskitetysti palvelimella olevia tiedostoja verkon käyttäjien kesken. Sähköpostipalvelu tarjoaa nimensä mukaisesti sähköpostipalveluja yrityksen työntekijöille. Nimipalvelun avulla palvelin selvittää verkossa olevien tietokoneiden nimien ja IP-osoitteiden yhteyden. (8, 106.)

Käyttäjien, käyttäjäryhmien ja tietokonetilien keskitetty hallinnointi onnistuu toimialueen ohjauspalvelimen (*Domain Controller, DC)* avulla. Hallinnointia varten ohjauspalvelimeen asennetaan toimialueen käyttäjätietokanta ja hakemistopalvelu (*Active Directory, AD*). Jokaiselle käyttäjälle luodaan oma käyttäjätili ja käyttäjäprofiili. Käyttäjäprofiilin avulla hallinnoidaan esimerkiksi käyttäjien kirjautumisia tietokoneille ja määritellään yksityiskohtaisia sovellusasetuksia ja käyttäjän kotikansio. (8, 106.) Keskitetty hallinta helpottaa verkon hallinnointia ja parantaa tietoturvallisuutta oleellisesti.

3.2 Windows Server 2008 R2

Windows Server 2008 on julkaistu 27. helmikuuta 2008. Tästä uudistettu versio Windows Server R2 julkistettiin virallisesti 22. lokakuuta 2009. Palvelinkäyttöjärjestelmän pohjana on ollut Windows Vista, joka perustuu Windows NT -ytimeen. Windows Server 2008 R2 -palvelinkäyttöjärjestelmän keskeisimpiä uudistuksia Windows Server 2008 verrattuna ovat tehokkaampi energianhallinta, parannetut virtuaalisointi ominaisuudet, uudet hallintatyökalut ja

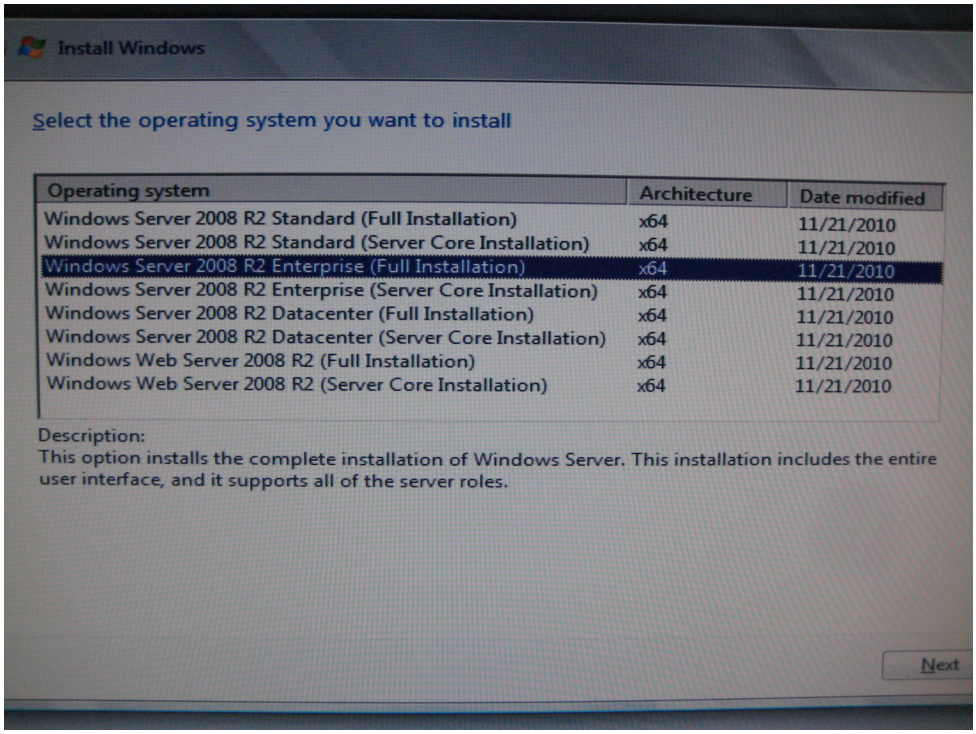
aktiivihakemiston parannukset sekä tehostettu suorituskyky ja täysi tuki 64-bittiselle tietojenkäsittelylle. (6, 36, 44; 10; 11.)

Windows Server 2008 R2 -palvelinkäyttöjärjestelmästä on tehty useita versioita. Datacenter-, Enterpise- ja Standard-versioiden tärkeimmät erot ovat käyttöjärjestelmän tuki prosessorien määrälle ja fyysisen muistin tuki. Muita Windows Server 2008 R2 -käyttöjärjestelmäversioita ovat erityiskäyttöön tarkoitetut versiot. WWW-palvelimeksi suunniteltu Windows Web Server ja supertietokoneiden käyttöjärjestelmä Windows HPC Server 2008 R2, Windows Server 2008 R2 for Itanium-based systems on Itanium prosessoreille suunnattu versio. (10; 12)

3.2.1 Windows Server 2008 R2 asennus ja perusasetukset

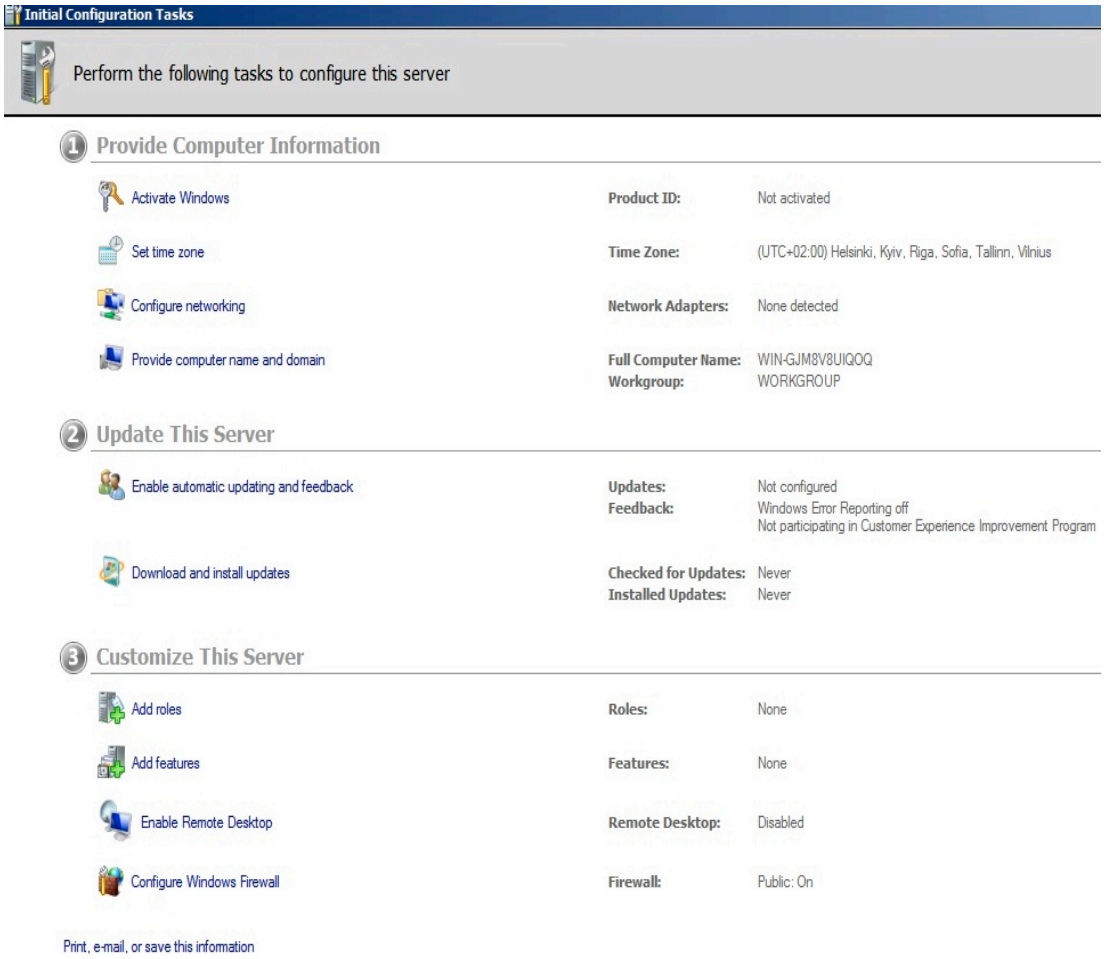
Valitsin opinnäytetyöhöni Windows Server 2008 R2 Enterprise -version (kuvio 1). Päädyin Enterprise -versioon, koska se on yleisesti käytössä yrityksissä ja sisältää kaikki keskeisimmät toiminnallisuudet. Projekti alkaa lataamalla käyttöjärjestelmän levykuva-tiedoston Microsoft MSDN-palvelusta. Sieltä Rovaniemen ammattikorkeakoulun tietotekniikan opiskelijat voivat ladata useita Microsoftin kehittämiä ohjelmistoja ilmaiseksi käyttöönsä. Tässä luvussa käyn pääpiirteittäin läpi palvelimen asennuksen ja siihen tehtävät perusasetukset.

Käyttöjärjestelmän asennus on yksinkertaista ja asennus etenee ohjatusti, kuten työpöytäkäyttöön suunnitellussa Windows-käyttöjärjestelmässä. Asennusohjelma kysyy asennusvalikossa käyttöjärjestelmän perustietoja, kuten asennuskielen, aikaformaatin, näppäimistöasetukset ja mihin palvelinkäyttöjärjestelmä asennetaan.



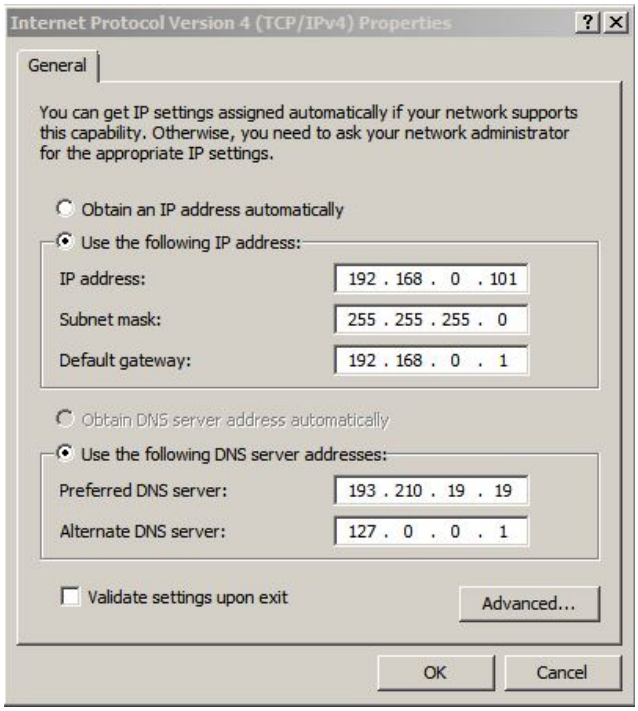
Kuvio 1. Palvelinkäyttöjärjestelmän version valinta

Ensimmäisellä käynnistyskerralla käyttöjärjestelmän työpöydälle avautuu konfigurointitehtävät hallintaruutu (*Initial Configuration Tasks*) (kuvio 2). Initial Configuration Tasks -hallintatyökalu kokoaa keskeisimmät asetukset yhteen ikkunaan. Hallintatyökalun kautta pääsee asettamaan muun muassa verkkoasetukset, palvelintietokoneen nimen ja toimialueen, roolit ja päivitykset. (6, 80.)



Kuvio 2. Initial Configuration Tasks -hallintatyökalu

Configure networking -kohdassa määritellään palvelimen TCP/IP-asetukset. Palvelimelle on hyvä määrittää kiinteät IP-osoitteet, jotta IP-osoite pysyy palvelimessa samana. Tietoturvasyistä TCP/Ipv6-protokollan valinta kannattaa poistaa, jos IPv6-versiota ei ole otettu käyttöön. Testipalvelimeen asetin kiinteäksi IP-osoitteeksi 192.168.0.101, aliverkon peitteeksi 255.255.255.0 ja oletusyhdyskäytäväksi reitittimen IP-osoitteen 192.168.0.1. DNS-palvelimen osoitteeksi asetin internet-yhteyden palveluntarjoajan DNS-palvelimen IP-osoitteen 193.210.19.19 (kuvio 3).



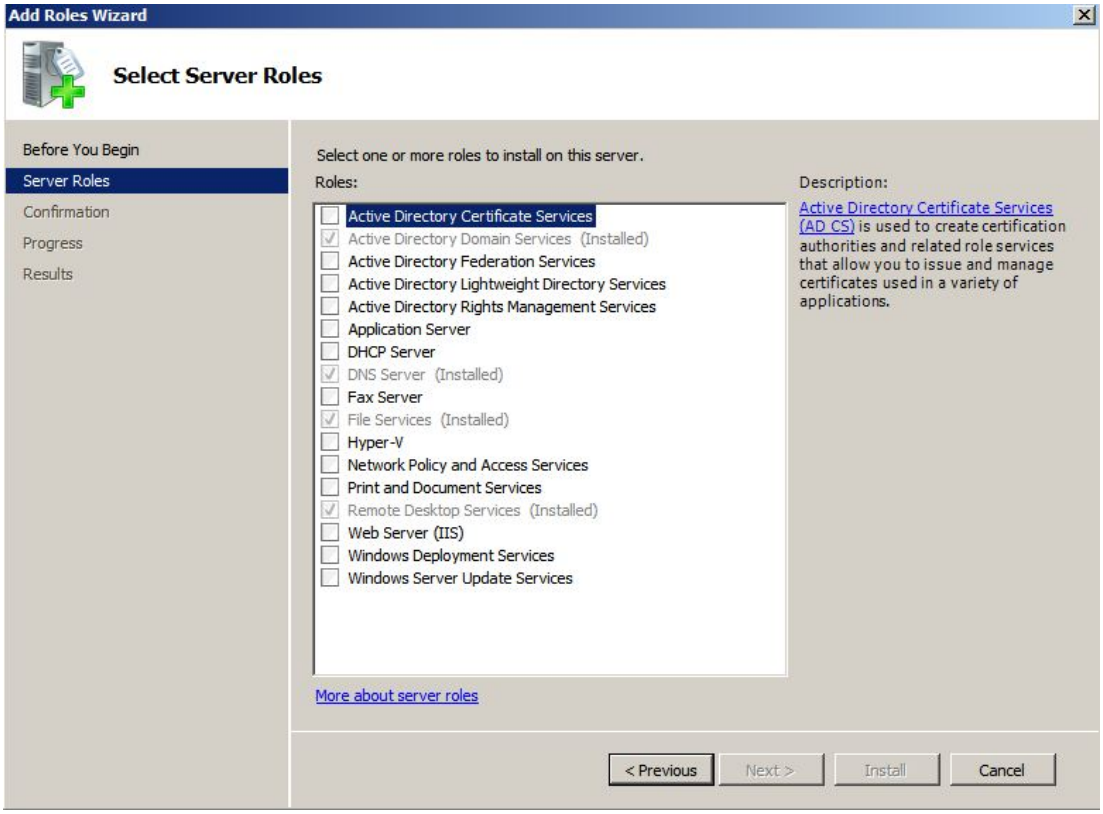
Kuvio 3. Palvelimen verkkoasetukset

Verkkoasetusten määrittelemisen jälkeen muutin testipalvelimen nimen Provide computer name and domain -kohdasta Roiserveriksi. Tässä projektissa palvelin ei liity olemassa olevaan toimialueeseen, joten oletustyöryhmä annetaan olla tässä vaiheessa ja toimialue vaihdetaan palvelimen roolien asettamisen jälkeen.

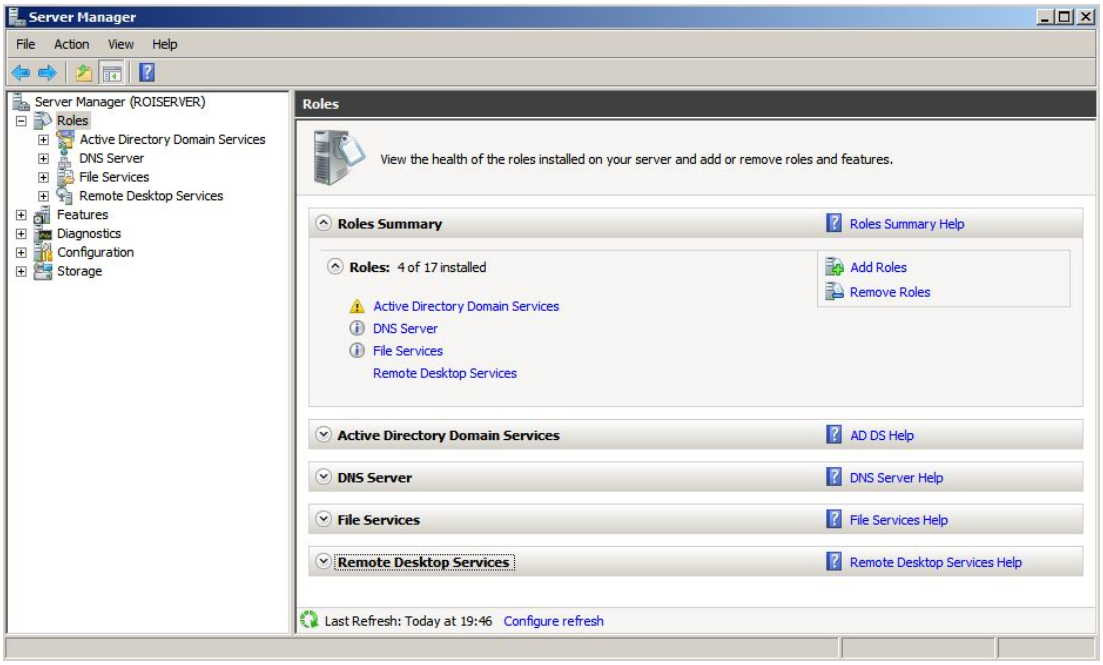
Palvelinkäyttöjärjestelmän päivitysten asennukset ja hallinta määritellään Update This Server -osion alta kohdasta Download and install updates. Päivitystenhallinnassa määritellään päivitysasetukset ja tarkistetaan ja asennetaan saatavilla olevat päivitykset. Päivitysten hallinta tarjoaa automaattiasetuksia tai manuaaliasetuksia. Automaattiasetukset kannattaa ottaa käyttöön tietoturvallisuuden lisäämiseksi. Ennen palvelimen käyttöönottamista on syytä asentaa tärkeät päivitykset. Jatkossa päivityksiä asennettaessa pitää tarkistaa, että päivitykset eivät aiheuta ongelmia käytössä oleviin ohjelmistoihin.

3.2.2 Palvelimen roolit

Palvelimen roolit lisätään Add roles -kohdasta. Palvelinrooleilla palvelimeen saadaan useita toiminnallisuuksia ja palveluita. Rooleiksi valitsin yleisimpiä yrityksissä käytössä olevia palvelinrooleja. Näitä olivat: DNS-palvelin *(DNS Server*), aktiivihakemiston toimialuepalvelu (*Active Directory Domain Services*), tiedostopalvelu (*File Services*) ja terminaalipalvelu (*Terminal Services*) (kuvio 4). Muita saatavilla olevia palvelinrooleja ovat esimerkiksi DHCP-palvelin (*DHCP Server*), Web-palvelin (*Web Server*) ja faksipalvelin (*Fax Server*). Tietoturvallisuuden näkökulmasta palvelimeen kannattaa asentaa vain ne roolit, jotka ovat tarpeellisia. Roolien poisto tapahtuu Server Manager -hallintakonsolin avulla (kuvio 5), (6, 100).



Kuvio 4. Roolien lisäys

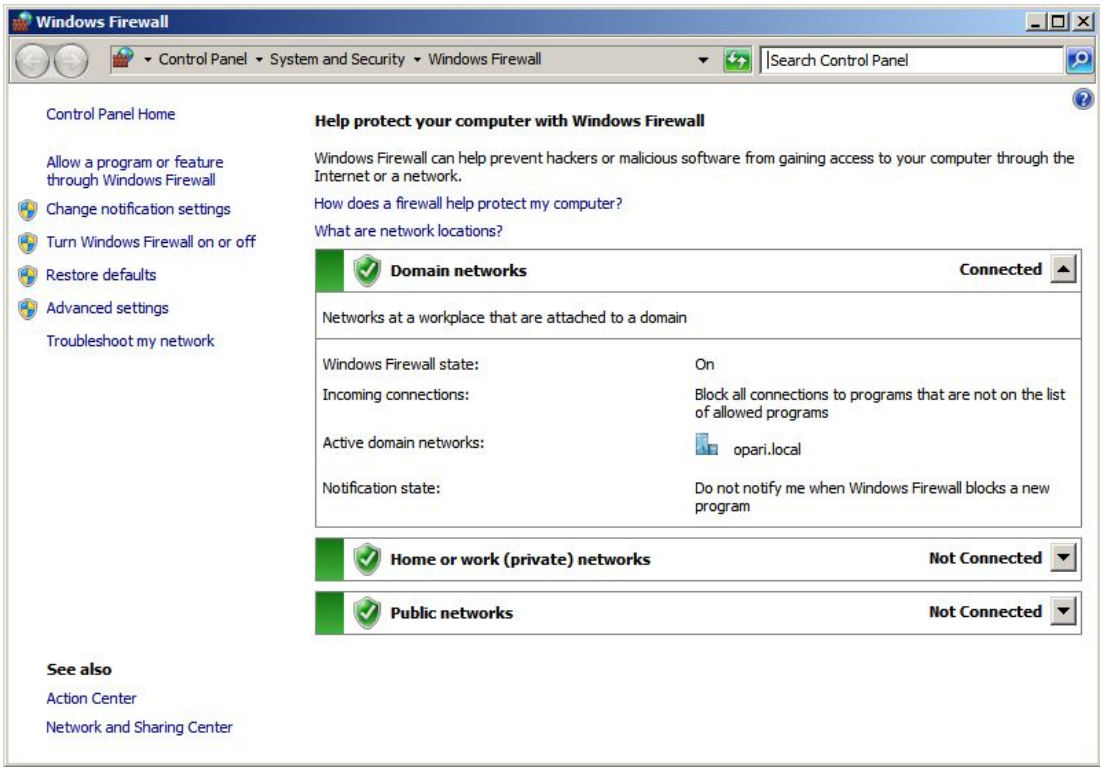


Kuvio 5. Roolien poisto

Palvelimen roolien lisäyksen jälkeen asensin Add features -kohdasta WINS-palvelin ominaisuuden. WINS-palvelin mahdollistaa WINS-nimipalvelun käytön, jonka tehtävänä on hoitaa NetBIOS-nimiselvitystä (6, 443).

3.2.3 Windows Server 2008 R2 -palomuuri

Windows Server 2008 R2 sisältää käyttöjärjestelmään integroidun palomuurin. Palomuuri tarjoaa tietokoneesta sisään ja ulospäin tapahtuvan verkkoliikenteen suodatuksen. Palomuuri on oletuksena päällä heti käyttöjärjestelmän asennuksesta lähtien. (6, 466.) Se kannattaa myös pitää aina päällä, jos tietokoneessa ei ole jotain toista palomuuria. Palomuuria pääsee hallitsemaan useasta paikasta, esimerkiksi Initial Configuration Tasks -hallintatyökaluikkunan kautta. Palomuuriasetuksien muokkauksessa pitää olla erityisen varovainen ja olla tietoinen siitä mitä tekee. Varomaton palomuurisääntöjen muokkaus saattaa heikentää tietoturvaa oleellisesti (6, 466).



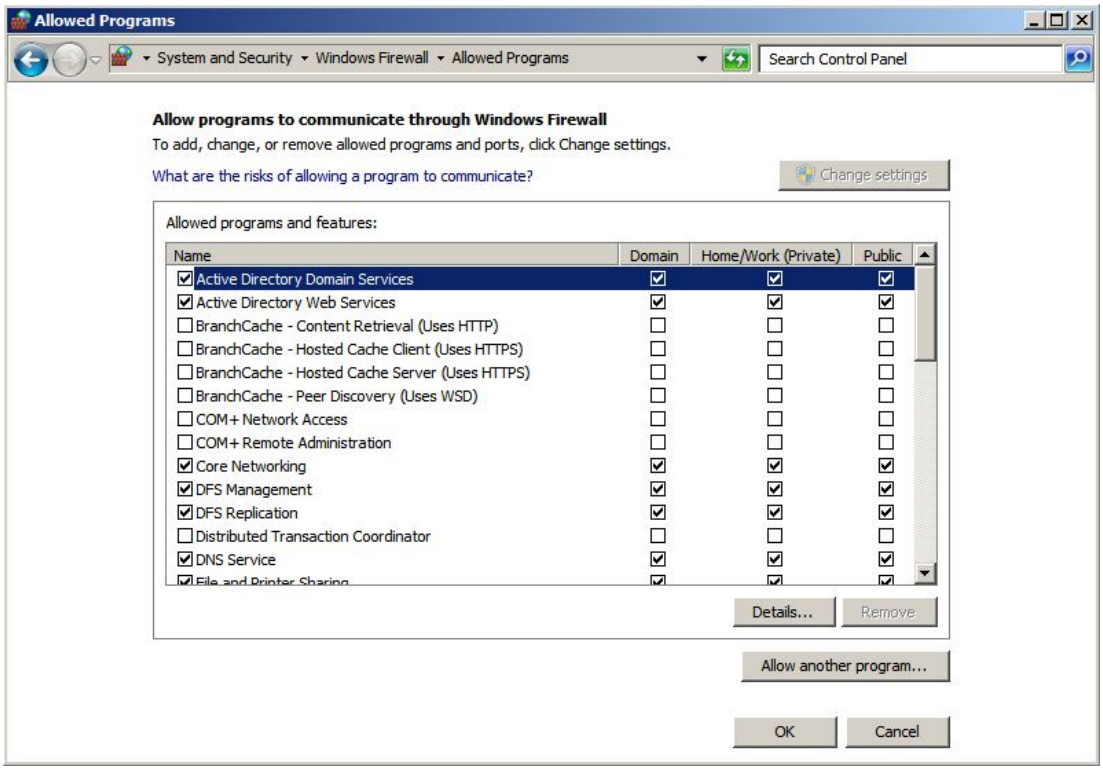
Kuvio 6. Windows-palomuuri

Palomuuri-ikkunan etusivulta (kuvio 6) pääsee palomuurin muokkausasetuksiin ja näkee tietoja palomuurin tilasta. Kuviosta 6 ilmenee, että palomuuri on käytössä (*Windows Firewall state: On*), sisään tulevat yhteydet, jotka eivät ole sallittujen listalla estetään (*Incoming connections: Block all connections to programs that are not on the list of allowed programs*) ja verkkosijainti on toimialueverkko (*Active domain networks:opari.local*). Toimialueverkko mahdollistaa keskitetyt palomuuriasetukset ryhmäkäytäntöjen avulla (6, 466).

Käyttöjärjestelmä avaa automaattisesti palomuurista poikkeussäännön palvelimen omille palveluille, kuten DNS-palvelulle ja aktiivihakemiston palveluille (6, 467). Manuaalisia määrityksiä tarvitaan esimerkiksi kolmannen osapuolten ohjelmille. Määrityksiä pääsee muokkaamaan Allow a program or feature through Windows Firewall -kohdasta. Ohjelmalle voidaan määritellä säännöt verkkosijaintikohtaisesti. Näitä ovat toimialue (*domain*), kotiverkko/työverkko (*home/work*) ja julkinen verkko (*public*) (kuvio 7). Palomuuri avaa sallitulle ohjelmalle sisään ja ulospäin tapahtuvan liikenteen. Tilanteesta riippuen palomuurin voidaan avata joko uusi portti tai ohjelma. Näiden erona on, että avoin portti on jatkuvasti auki, mutta ohjelma on auki vain silloin, kun sitä tar-

vitaan. Uusien sääntöjen luomisessa kannattaa suosia jälkimmäistä vaihtoehtoa, jos se vain on mahdollista. (6, 467–469.)

Palomuurista kannattaa tarkistaa säännöllisesti, onko siinä tarpeettomia auki olevia portteja ja sääntöjä. Kaikki palomuuripoikkeukset lisäävät tietoturvariskiä (6, 467).



Kuvio 7. Sallittujen ohjelmien lista

Windows Server 2008 R2 tarjoaa järjestelmään integroidusta palomuurista myös laajennetun version (*Windows Firewall with Advanced Security*). Laajennettu palomuuri mahdollistaa laajemmat säätömahdollisuudet, palomuurin etähallinnan ja IPsec-suojauksen. Laajennettu palomuuri toimii tilallisena. Se suodattaa lähtevän ja saapuvan liikenteen palomuuriin tehtyjen konfiguraatioiden perusteella. Tietokoneiden välisissä yhteyksissä käytetään todennusta ja tietoliikenteen suojausominaisuuksia. (6, 470.)

3.3 Windows Server 2008 R2 koventaminen

Palvelimen koventaminen (*server hardening*) tarkoittaa prosessia, jonka tarkoituksena on lisätä turvallisuutta palvelinkäyttöjärjestelmässä ja pienentää hakkerien käyttämää hyökkäysaluetta. Kovennuksessa palvelimesta tehdään sietokykyisempi ja vahvempi tietoturvahyökkäyksiä vastaan. (9.) Koventaminen kannattaa tehdä, ennen kuin palvelin kytketään toimintaverkkoon ja sitä aletaan varsinaisesti käyttämään. Palvelin tulee kuitenkin olla mahdollisimman käyttövalmis järjestelmä, kun kovennusta aletaan tekemään.

Kovennusprosessissa käydään läpi useita palvelimen asetuksia ja ohjelmistoja. Tarkistuskohteet vaihtelevat palvelimen käyttötarkoituksen ja siihen asennettujen ohjelmistojen mukaan. Suoraan käytettävää yleispätevää kovennusohjetta on vaikea laatia ja käyttää. Internetistä löytyy kuitenkin useita kovennuksen tarkistuslistoja (*hardening checklist*) ja ohjeita, joita kannattaa käyttää apuna.

Tässä luvussa käyn läpi testipalvelimen kovennusprosessin vaiheita. Apuna käytin internetistä löytämiäni kovennusohjeita, pääosin National Institute of Standards and Technology -organisaation laatimaa ohjetta. Kovennusprosessin jälkeen testaan palvelimen tietoturvatason kahden analysointiohjelman avulla. Analysointiohjelmista ja niiden antamista tuloksista kerrotaan tarkemmin neljännessä luvussa.

3.3.1 Päivitysten asentaminen ja tarkistaminen

Palvelimeen asennettujen tarvittavien palvelujen ja ohjelmistojen jälkeen ensimmäisenä tehtävänä on tärkeää tarkistaa Windows Update -palvelusta saatavilla olevat päivitykset ja järjestelmän korjaukset. Testipalvelin löysi ensimmäisellä päivityskerralla 62 tärkeää päivitystä. Asennettaessa päivityksiä tuotantokäytössä oleviin palvelimiin palvelinten ylläpitäjän täytyy varmistaa, etteivät uudet päivitykset aiheuta ongelmia käytössä oleviin ohjelmistoihin.

Kun palvelinta päivitetään ensimmäistä kertaa, se on syytä suojata huolellisesti päivitysprosessin aikana. Uusi käyttöjärjestelmä on erityisen altis hyök-

käyksille, koska palvelimesta löytyy suuri määrä paikkaamattomia käyttöjärjestelmän tietoturva-aukkoja, joita hyökkääjät voivat käyttää hyväkseen. Päivityksen aikana palvelin kannattaa kytkeä suojattuun verkkoon tai käyttää ulkoista tallennuslähdettä, josta päivitykset asennetaan. Palvelinta päivitettäessä sille kannattaa luoda erillinen VLAN-verkko (*Virtual Local Area Network)*, jossa se on eristetty verkon muista lähiverkon tietokoneista. (4, 25–26.)

3.3.2 Tarpeettomien ohjelmien ja palveluiden poisto

Palvelimen kovennuksessa käyttöjärjestelmästä poistetaan kaikki tarpeettomat ohjelmat, palvelut ja verkkoprotokollat (esimerkiksi IPv6). Palvelinkäyttöjärjestelmän minimikokoonpano pienentää hyökkäyspinta-alaa, koska poistettujen palvelujen ja ohjelmien tietoturva-aukkoja ei voida enää käyttää hyödyksi, sillä ne ovat kokonaan poistettu. Pienempi määrä palveluita ja ohjelmia vähentää myös lokitiedostoihin kerättyä tietoa, joten todennäköisten uhkien havaitsemisesta tulee helpompaa. (4, 26–27.)

Ohjelmista jää usein tiedostoja käyttöjärjestelmään ohjelmistojen poiston jälkeenkin, joten paras tapa on asentaa käyttöjärjestelmä minimikokoonpanolla ja lisätä myöhemmässä vaiheessa siihen uusia palveluita ja ohjelmia. Joitakin palveluita ei pysty kokonaan poistamaan, vaan niiden toiminta täytyy estää. Tyypillisiä mahdollisesti tarpeettomia ohjelmia ja palveluita ovat esimerkiksi langattoman verkon palvelut, järjestelmän kehitystyökalut, sähköpostipalvelut, web-palvelin, tarpeettomat etäkäyttöpalvelut ja tiedostojen ja tulostimien jakopalvelut. (4, 26–27.) Opinnäytetyössä käyttämäni testipalvelimen käyttöönotossa ja asennuksessa otin minimikokoonpano periaatteen huomioon jo projektin suunnitteluvaiheessa.

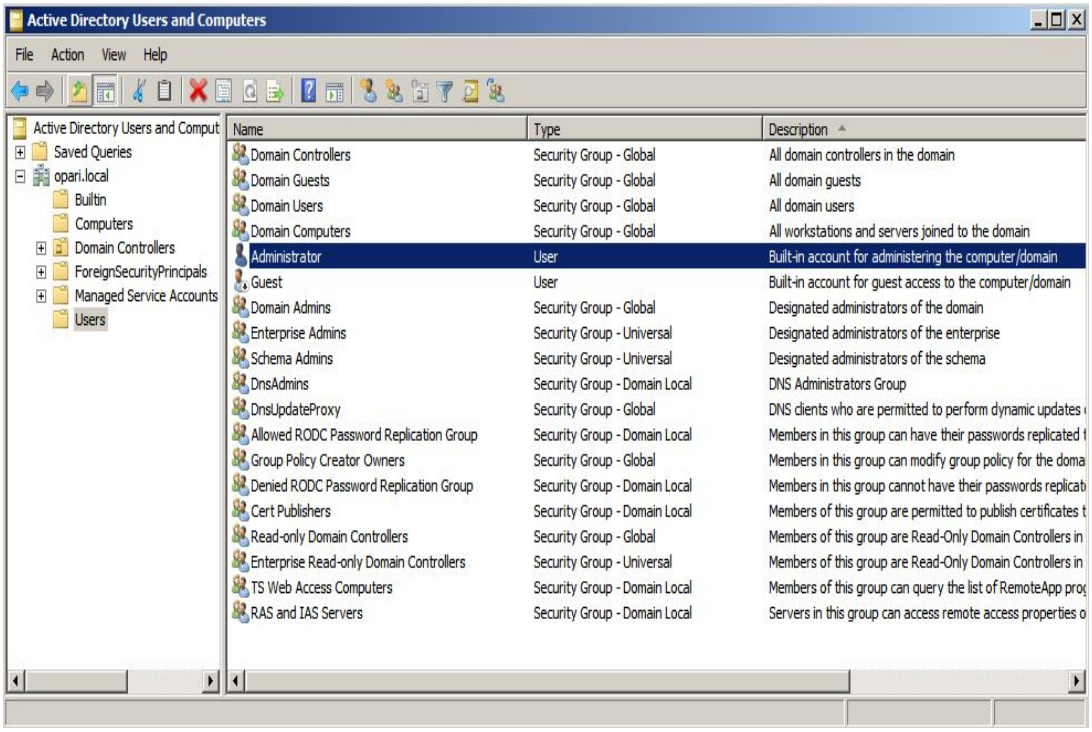
3.3.3 Käyttäjätunnukset ja -ryhmät

Palvelimen käyttäjätunnusten hallinnointi tulisi tehdä siten, että käyttöjärjestelmään pystyy kirjautumaan vain rajattu määrä käyttäjätunnuksia ja palvelimen asetuksia voi muokata ainoastaan käyttöjärjestelmän ylläpitäjät. Palvelimen tarjoamat palvelut tulee olla niitä tarvitsevien työntekijöiden saatavilla,

mutta vain tietyille käyttäjille annetaan oikeudet kirjautua itse käyttöjärjestelmään.

Oletuksena käyttöjärjestelmään sisältyy useita sisäänrakennettuja (*built-in*) käyttäjätunnuksia ja ryhmiä. Oletusarvoisesti luotuja käyttäjätunnuksia ovat esimerkiksi vieras (*Guest*) ja järjestelmänvalvoja (*Administrator*). Tarpeettomat käyttäjätunnukset ja ryhmät tulee poistaa, nimetä uudelleen tai muuttaa salasanat yrityksen salasanakäytäntöjen mukaisiksi. (4, 28; 8, 144–145.)

Käyttöjärjestelmän paikallisten käyttäjien ja ryhmien hallintaan päästään Server Manager Configuration -kohdasta, josta löytyy Local Users and Groups -valikko. Jos palvelin toimii toimialueen ohjauspalvelimena – kuten opinnäytetyön testipalvelin – käytössä on paikallisen käyttäjätietokannan sijaan Active Directory -toimialueen käyttäjätietokanta. Active Directory käyttäjätietokantaa hallitaan Administrative Tools -valikosta löytyvällä Active Directory Users and Computers -hallintakonsolilla (kuvio 8). (6, 368–369.)



Kuvio 8. Active Directory Users and Computers -hallintakonsoli

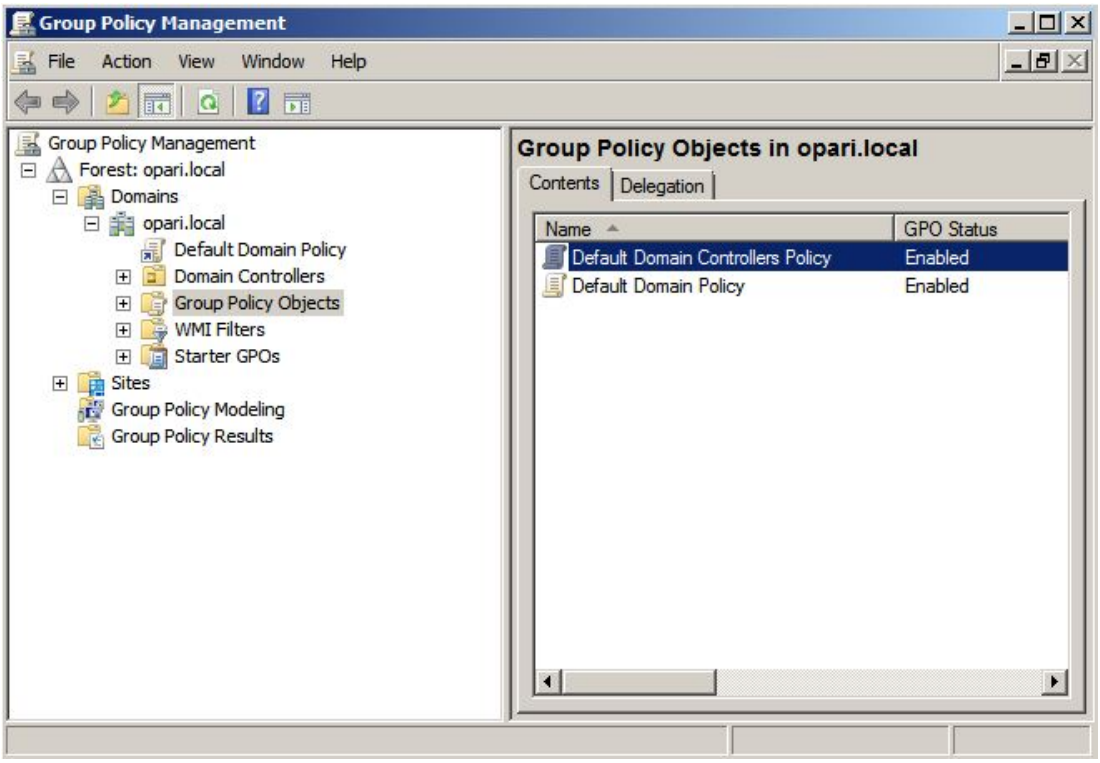
Käyttäjäryhmien luonnissa kannattaa suosia yrityksen rakenteeseen, osastoihin, toimipisteisiin, projekteihin ja käyttäjien toimenkuvaan perustuvia ryhmiä. Tämä helpottaa käyttäjäryhmien hahmotusta ja pitää käyttäjärakenteen

loogisena. Käyttäjätunnukset lisätään ryhmiin ja oikeudet ja ominaisuudet annetaan käyttäjäryhmälle, jolloin oikeudet periytyvät kaikille ryhmään kuuluville käyttäjille. (2, 155–156.)

3.3.4 Salasanakäytäntö ja käyttäjätilien lukitusmääritykset

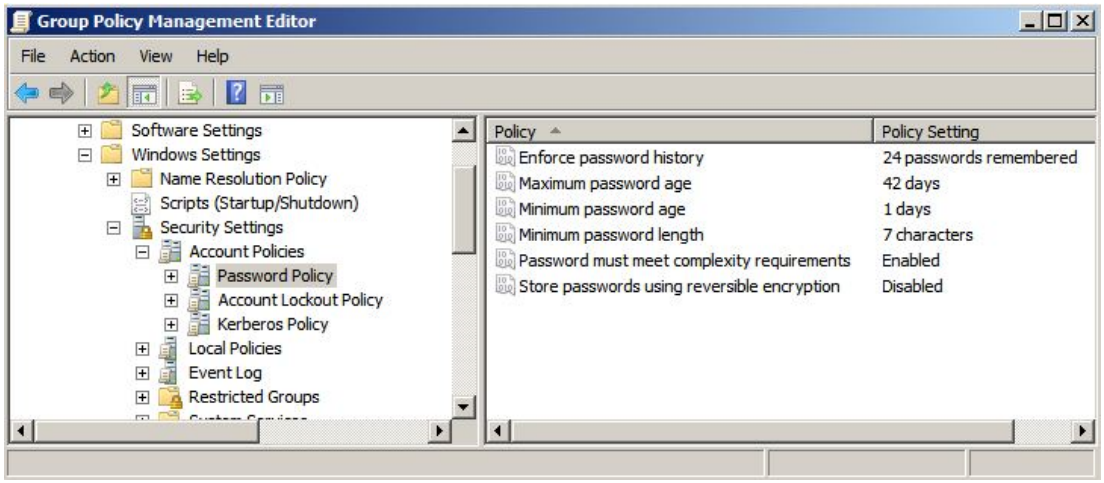
Käyttäjätilien suojaaminen vahvalla salasanalla on tärkeä keino varmistaa, että järjestelmään ei pysty kirjautumaan kuka tahansa henkilö. Jotta salasanasuojaus toimisi, pitää sen olla riittävän vahva ja vaikeasti arvattava. Helpot salasanat murtuvat nopeasti hyökkääjien käyttämien salasanankaappaus ohjelmien avulla. Yrityksen käyttäjätileille tulee asettaa riittävän tiukat, vahvaan salasanaan määräävät käytännöt. (8, 151–152.)

Toimialuetasolla salasanakäytäntöjä hallitaan ryhmäkäytäntöjen (*Group Policy*) avulla. Ryhmäkäytäntöjen avulla käyttäjille, käyttäjäryhmille ja työasemille pystytään keskitetysti linkittämään asetuksia ja oikeuksia. Ryhmäkäytäntöjen hallintaan päästään Administrative Tools -valikosta löytyvästä Group Policy Management -hallintakonsolista (kuvio 9). Ryhmäkäytäntöobjektit löytyvät Group Policy Objects -kansiosta. Toimialuelaajuista Default Domain Policy -objektia pääsee muokkaamaan Action-valikosta valitsemalla Edit.



Kuvio 9. Group Policy Management -hallintakonsoli

Salasanakäytäntöihin päästään kohdasta Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy (kuvio 10). Kuviossa näkyy oletusasetuksilla olevat salasanakäytännöt. Salasanahistoria on voimassa ja 24 viimeksi käytettyä salasanaa muistetaan (*Enforce password history: 24 passwords remembered).* Tämä tarkoittaa että 24:ää edellistä salasanaa ei voida käyttää uudestaan. Salasanan enimmäisikä on 42 päivää (*Maximum password age: 42 days*) ja minimi-ikä 1 päivä (*Minimum password age: 1 days*). Salasanan täytyy olla monimutkainen (*Password must meet complexity requirments*) eli salasana pitää sisältää merkkejä isoista ja pienistä kirjaimista ja siinä on oltava numeroita ja erikoismerkkejä. Lisäksi salasanassa ei voi olla enempää kuin kolme merkkiä käyttäjätilin nimestä. Oletusasetuksen mukaan salasanoja ei säilytetä avattavassa muodossa *(store passwords using revesible encryption).* (6, 668–669.) Oletusasetuksillakin ryhmäkäytäntöjen salasanakriteerit ovat riittävän tiukat useimpiin käyttöympäristöihin.

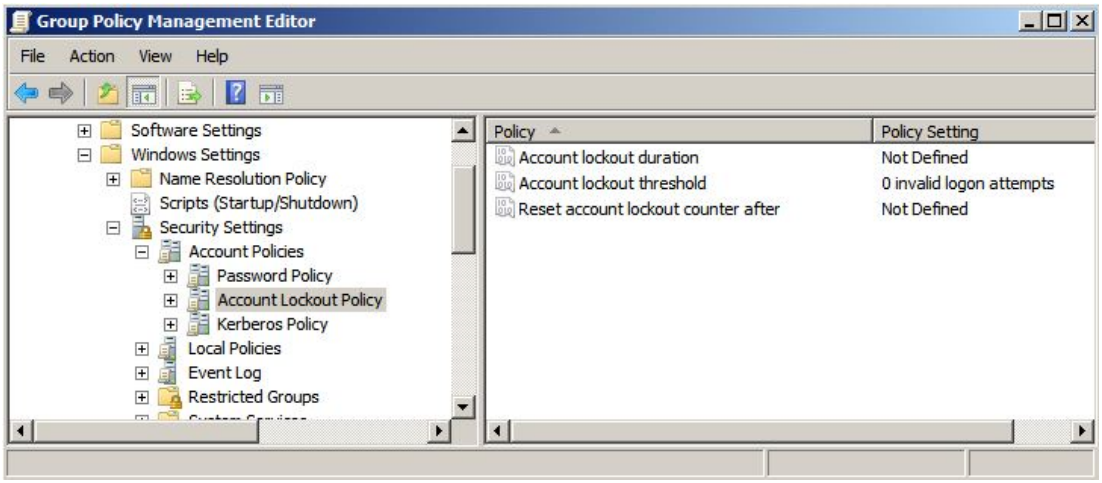


Kuvio 10. Salasanakäytännöt

Ryhmäkäytäntösääntöjen lisäksi hyvän salasanan kriteereinä ovat seuraavat ehdot:

- Salasanan muistilappua ei saa säilyttää helposti löydettävässä paikassa, esimerkiksi näppäimistön alla.
- Salasana ei saa löytyä sanakirjoista.
- Salasanassa ei saa käyttää esimerkiksi nimiä, syntymäpäiviä tai harrastuksia. (8, 151–152.)

Account Lockout Policy -kohdasta hallitaan käyttäjätilien lukituskäytäntömäärityksiä (kuvio 11). Määritysten avulla voidaan määritellä käyttäjätilin lukituksen kesto (*Account lockout duration*), käyttäjätilin kirjautumisyritysten enimmäismäärä (*Account lockout threshold*) ja käyttäjätilin lukituksenaikalaskurin nollaantumisaika. Oletuksena näitä asetuksia ei ole määritelty. Lukituskäytäntömääritykset on kuitenkin hyvä ottaa käyttöön. Niiden avulla voidaan estää esimerkiksi hyökkääjien käyttämien salasanojen arvausohjelmien käyttö (4, 29).



Kuvio 11. Käyttäjätilien lukituskäytännöt

3.3.5 Varmuuskopiointikäytännöt

Varmuuskopioinnista (*backup)* huolehtiminen on yksi tietoturvallisuuden tärkeimmistä osa-alueista. Varmuuskopioinnin tarkoituksena on, että tiedot ja palvelut ovat aina tallessa ja nopeasti saatavilla, myös häiriötilanteissa. Yrityksellä pitää olla ajantasainen varmuuskopiointikäytäntö, jossa palvelimet ja työasemat on varmennettu. Varmennuksessa tulee huolehtia niin tiedostojen, ohjelmistojen kuin käyttöjärjestelmien varmuuskopioinnista. Varmuuskopioiden toimivuus pitää myös testata säännöllisesti. Palvelinten varmuuskopiointi on erityisen tärkeää, koska monen yrityksen työntekijän toiminta on riippuvainen palvelimella olevista tiedoista. Palvelimen toimintahäiriön saattavat aiheuttaa useat tekijät. Näitä ovat esimerkiksi ohjelmistovirhe, palvelimen hakkerointi tai laitteistovika. Myös inhimillisen virheen seurauksena saatetaan menettää tärkeitä tietoja tai aiheuttaa haittaa palvelimen toimintakyvylle. (4, 41–42; 8, 209.)

Yrityksen varmuuskopiointistrategia sisältää useimmiten suunnitelmat ainakin varmuuskopioinnin säilytyksestä, ajoittamisesta, palautuksesta, varmuuskopiointitiheydestä ja tiedot siitä mitä varmistetaan. Varmuuskopioiden säilytyksessä tulee ottaa huomioon onnettomuustilanteet ja luonnonkatastrofit. Varmennukset on hyvä säilyttää tulipalolta ja varkauksilta suojaavassa kaapissa, joka sijaitsee eri rakennuksessa kuin alkuperäiset tiedot. Varmuuskopioiden ajoitukset pitää suunnitella siten, että niistä aiheutuu mahdollisimman vähän haittaa työnteolle ja työpäivän aikana muuttuneet tiedostot tulee varmenne-

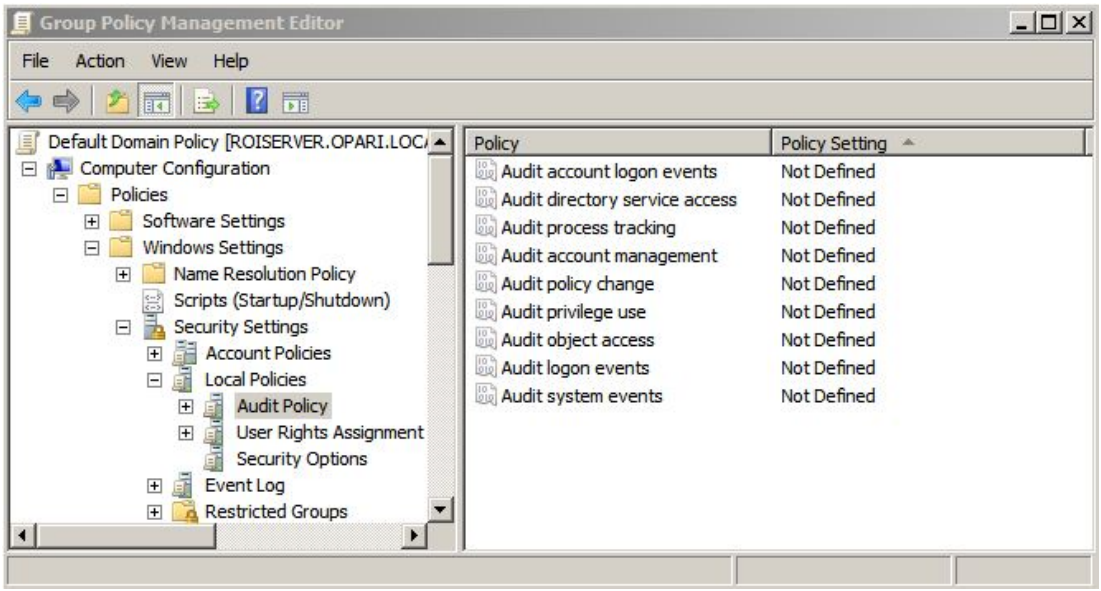
tuksi. Sopivin ajankohta varmistuksille on useimmiten yö. Varmuuskopiointityypeillä voidaan vaikuttaa varmistuksiin kuluvaan aikaan. Normaalit varmuuskopiot kannattaa tehdä esimerkiksi kerran viikossa ja suorittaa varmuuskopioiden lisäyksen tai erotuksen kopioivia varmuuskopioita päivittäin. Varmuuskopiointijärjestelmien suunnittelussa tulee ottaa huomioon myös varmennusten tallennustilantarve ja sopiva varmennuksien kierto. (8, 210–214, 217–218.)

Windows Server 2008 R2 -käyttöjärjestelmän mukana tulee Windows Server Backup -varmuuskopiointiohjelma. Ohjelma asennetaan Server Manager -hallintakonsolista löytyvästä Add Features -kohdasta. Mukana tuleva varmuuskopiointiohjelmisto on ominaisuuksiltaan rajoitettu, mutta mahdollistaa perustason varmuuskopioinnin ja järjestelmän varmentamisen. Windows Server Backup -ohjelmistolla pystytään varmistamaan koko palvelin ja käyttöjärjestelmä voidaan palauttaa esimerkiksi kiintolevyn rikkoutumisen jälkeen. Käyttöjärjestelmän omassa varmistusohjelmistossa on kuitenkin puutteita, joiden vuoksi yrityksen kannattaa harkita kolmansien osapuolten valmistamien varmuuskopiointiohjelmien käyttöä. Windows Server Backup ei tue esimerkiksi nauhavarmistusta ja varmuuskopiointimenetelmissä on rajoitteita. (6, 1151–1153.)

3.3.6 Auditointi

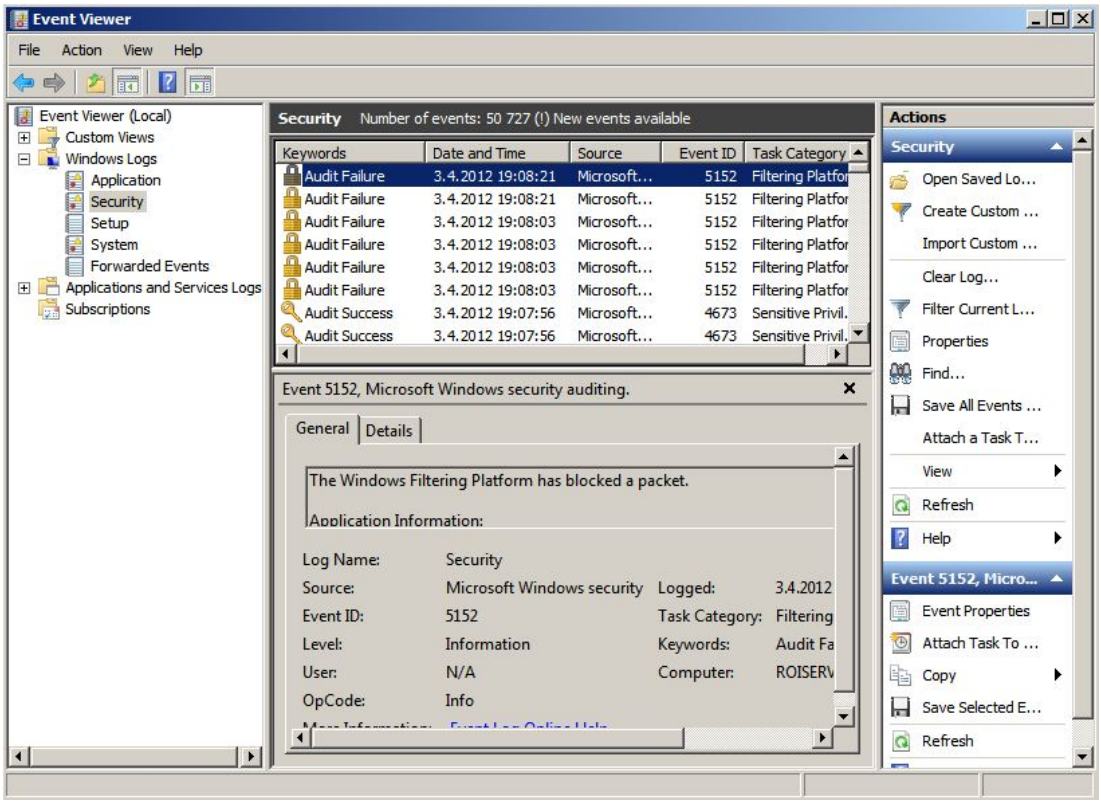
Auditointi tarkoittaa käyttöjärjestelmän valvontaa. Windows-käyttöjärjestelmässä voidaan valvoa esimerkiksi käyttöjärjestelmän toimintaa ja käyttäjien kirjautumistapahtumia. Valvontatiedot kirjataan lokitiedostoihin, joista tapahtumia pystytään seuraamaan. Lokitiedostoja seuraamalla voidaan havaita murtautumisyritykset tai jokin muu käyttöjärjestelmän epäilyttävä käyttäytyminen. Oletuksena valvontakohteita ei ole määritelty. Valvonta kannattaa ottaa käyttöön ainakin seuraaville kohteille: käyttäjien kirjautumistapahtumat (*Audit account logon events*), käyttäjätunnusten hallinta (*Audit account management*), objektien käyttö (*Audit object access*). Palvelimen valvontamääritykset tulee tehdä niin, että valvottavaksi valitaan vain ne kohteet, jotka ovat tarpeellisia. Ylimääräinen valvonta kasvattaa lokitiedostojen kokoa ja lokitapahtumien seuranta vaikeutuu. (2, 156–160; 8, 174–176.)

Palvelimen paikallisiin auditointi määrityksiin päästään kohdasta Administrative Tools -> Local Security policy -> Security Setting -> Local policies -> Audit policies. Auditointimääritykset voidaan asettaa myös Group Policy Management -hallintatyökalulla (kuvio 12).



Kuvio 12. Audit Policy -hallintatyökalu

Auditointiasetuksissa on valittavana onnistunut ja epäonnistunut tapahtuma. Esimerkiksi epäonnistunut kirjautumisyritys kirjataan failure-tyypiksi ja onnistunut kirjautuminen success-tyypiksi. Auditoinnin tallentamaa lokitiedostoa voi seurata Event Viewer -työkalun avulla (kuvio 13). Lokiin tallentuu tapahtuman tyyppi, päivämäärä, kellonaika, tietoa mahdollisesta käyttäjästä ja tarkempi kuvaus tapahtumasta.



Kuvio 13. Tapahtumien seuranta -työkalu

3.3.7 Virustorjuntaohjelman asennus

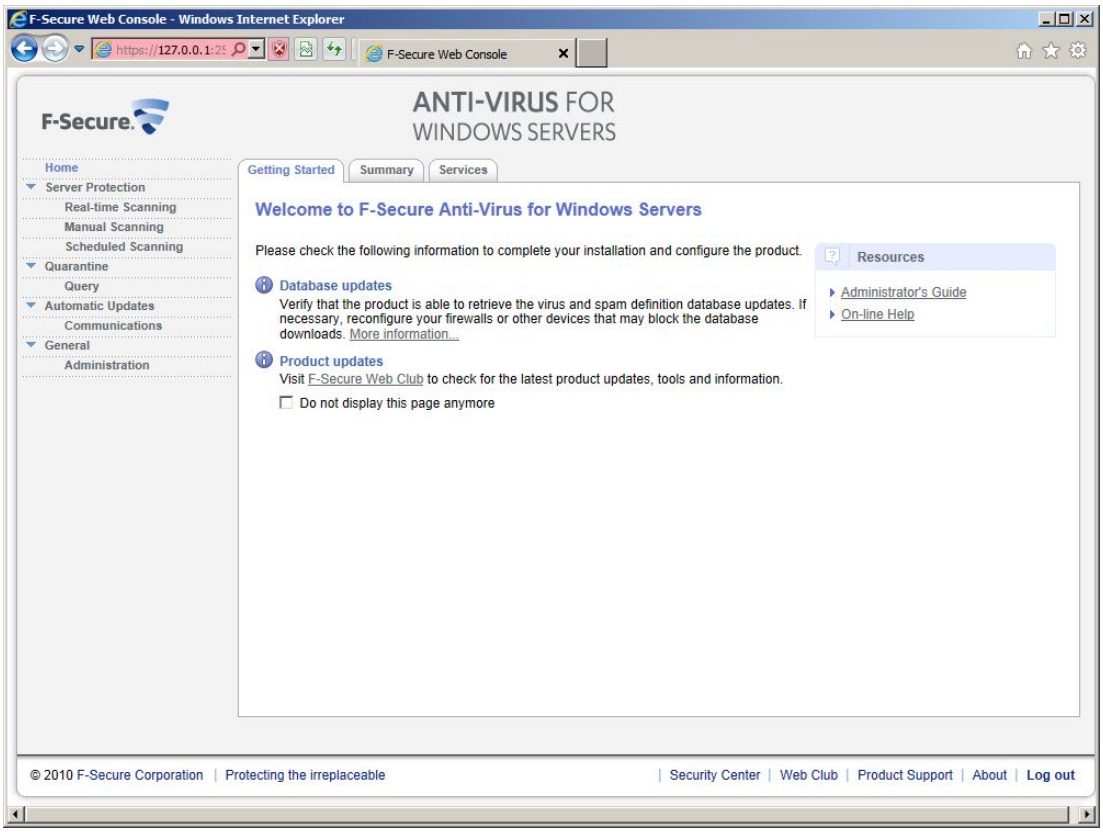
Virustorjuntaohjelmiston asennus ja käyttöönotto on tärkeä osa palvelimen koventamisprosessia. Virustorjuntaohjelmiston asennus tulee tehdä, ennen kuin palvelin kytketään verkkoon. Virustorjuntaohjelma kannattaakin asentaa erilliseltä tallennusvälineeltä, eikä palvelimella suoraan internetistä lataamalla. Palvelimelle suunniteltuja virustorjuntaohjelmia on tarjolla laaja valikoima useilta valmistajilta. Tunnetuimpia virustorjuntaohjelmien tekijöitä ovat F-Secure, Panda, Symantec Norton, Trend Micro ja McAfee. Virustorjuntaohjelmiston valinnassa kannattaa kiinnittää huomiota ainakin virustorjuntaohjelmiston käytettävyyteen ja asennuksien helppouteen. Virustorjuntaohjelmistoissa on eroja muun muassa siinä, kuinka helposti ja ohjatusti virustorjuntaohjelmistot asennetaan useille työasemille ja minkälaisen kokonaiskuvan virustorjuntaohjelma antaa yrityksen tietoturvasta (7).

Opinnäytetyössä asensin testipalvelimelle F-Securen valmistaman virustorjuntaohjelman Anti-Virus for Windows Servers 9.00. Päädyin F-Securen tuot-

teeseen, koska se on tunnetun valmistajan kehittämä, laajasti yrityksissä käytetty ohjelma ja siitä oli mahdollista saada 60 päivän ilmainen kokeilujakso. Ohjelman pystyi lataamaan F-Securen sivuilta rekisteröintilomakkeen täytön jälkeen. Anti-Virus For Windows Servers -ohjelman asentaminen oli yksinkertainen ja helppo prosessi. Asennusvalikossa ohjelma kysyy, hallittaanko tietokoneen virustorjuntaa keskitetysti F-Secure Policy Manager -työkalun avulla vai tehdäänkö paikallisesti hallittu itsenäinen asennus (kuvio 14). Valitsin jälkimmäisen vaihtoehdon.

Kuvio 14 F-Secure Policy Manager -työkalun valinta

Anti-Virus For Windows Servers -virustorjuntaohjelmaa hallitaan internetselainpohjaisella käyttöliittymällä (kuvio 15). Ohjelman aloitusikkuna on hyvin pelkistetyn ja yksinkertaisen näköinen. Aloitusikkunassa ovat linkit muun muassa tarkistusvalintoihin, päivityksiin, ohjelman hallinnointiin ja viruskaranteeniin.



Kuvio 15. F-Secure Web -konsoli

4 PALVELIMEN TIETOTURVAN ANALYSOINTIOHJELMAT

Palvelimen tietoturva on hyvä testata säännöllisesti ja tarkistaa, että kaikki tietoturva-asetukset ovat kunnossa ja ajan tasalla. Tarkistukset voi tehdä esimerkiksi kerran viikossa tai kuukaudessa. (4, 31–32.) Tietoturvan testaamisessa auttavat erilaiset ilmaiset tai maksulliset analysointiohjelmat. Analysointiohjelmat testaavat useita palvelinturvallisuuteen vaikuttavia asioita. Ne tutkivat esimerkiksi, ovatko ohjelmat ajan tasalla, puuttuuko käyttöjärjestelmän päivityksiä tai vastaavatko palvelimen tietoturvamääritykset yrityksen tietoturvakäytäntöjä (4, 45–46). Analysointiohjelmat tekevät tarkistukset niiden tietoturvatietokannan pohjalta. Tämän vuoksi analysointiohjelmat löytävät uusimmat tietoturvauhkat vasta, kun niiden tietoturvatietokanta on päivitetty. (4, 46–47). Tarkistustulosten analysoinnissa pitää olla asiantuntevaa tietämystä ja tulkita tuloksia kriittisesti. Kaikki löydökset eivät välttämättä heikennä tietoturvallisuutta oleellisesti ja vääriä hälytyksiä tapahtuu paljon. Tarkistustulokset on kuitenkin syytä dokumentoida ja tarvittaessa korjata puutteet pikaisesti. Käytetyistä ohjelmista GFI LanGuard tarjosi hyvät työkalut tarkistusraporttien laatimiseen. Tarkistusten hidastava vaikutus verkon ja palvelimen kuormitukseen on myös syytä huomioida tarkistuksia ajettaessa.

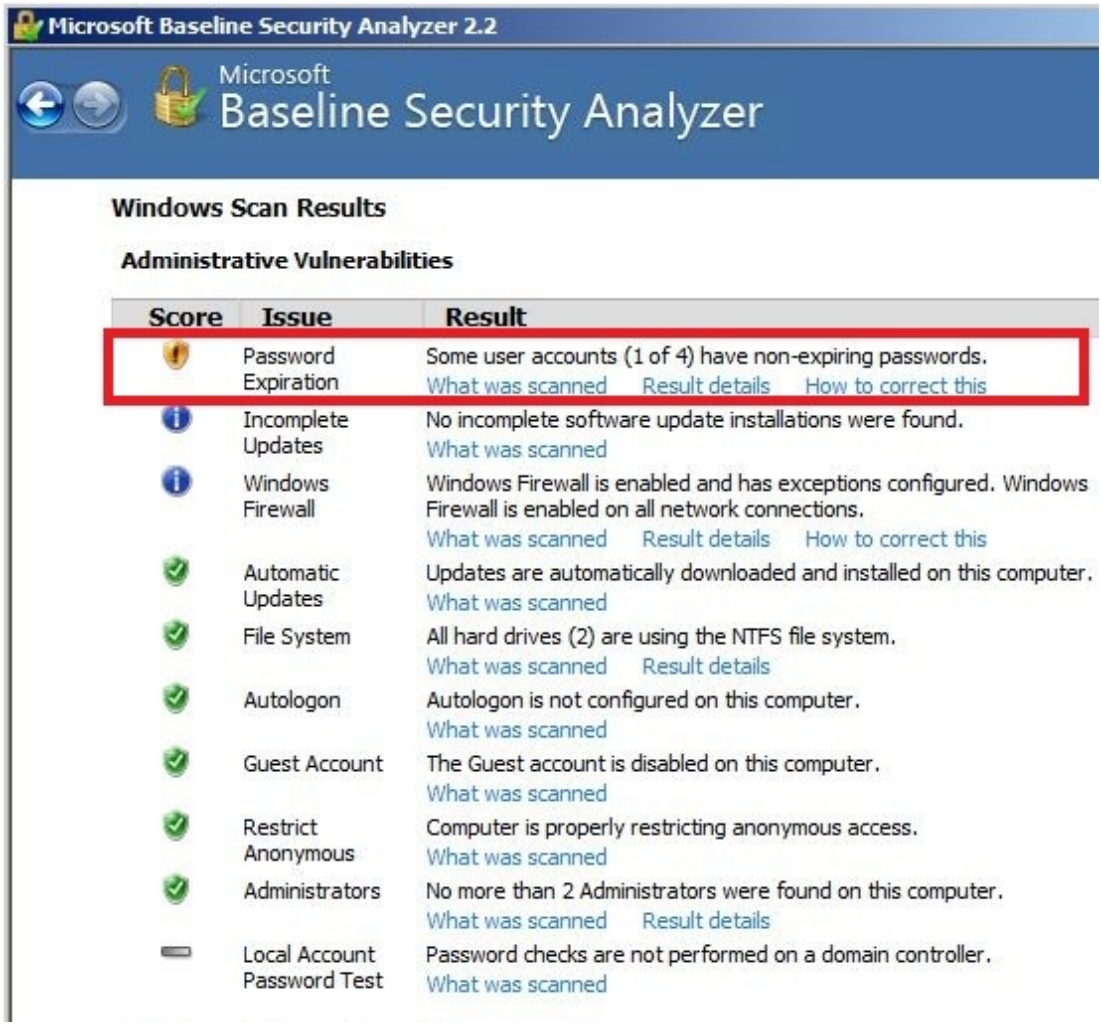
Palvelimen tietoturvatasosta luotettavan kuvan saamiseksi pitäisi käyttää useampaa kuin yhtä analysointiohjelmaa. Tarkistusohjelmissa on paljon eroja ja toisella ohjelmalla saattaa tulla erilaisia tuloksia kuin toisella. (4, 47.) Opinnäytetyössä käytin kahta eri palvelimen tietoturvatasoa mittaavaa ohjelmaa. Ensimmäiseksi tein tietoturvaselvityksen Microsoft Baseline Security Analyzer 2.2 -skannausohjelmalla ja tämän jälkeen tarkistin testipalvelimen GFI LanGuard -ohjelmalla. Analysointiohjelmiin tutustumisen aloitin perehtymällä asennusoppaisiin ja ohjelmien käyttöä esitteleviin videoihin. Microsoft Baseline Security Analyzer -ohjelman asensin ensin Windows 7 Professional -käyttöjärjestelmälle, jossa tutustuin ohjelman käyttöön ennen sen asentamista testipalvelimeen.

4.1 Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) on Microsoftin valmistama sovellus, mikä tarkistaa Windows-käyttöjärjestelmän ja Microsoftin ohjelmiin liittyviä tietoturvariskejä. Tietoturvaselvitys voidaan tehdä joko paikallisesti tai verkon yli. Verkon kautta pystyy tarkistamaan useita tietokoneita käyttämällä toimialueen nimeä tai määrittämällä tarkistettavien tietokoneiden IP-osoitealue. MBSA tarkistaa päivitysten tilan ja useita muita tietoturvaan liittyviä asetuksia. Päivityksiin liittyen ohjelma tutkii onko päivityksiä jäänyt kesken tai asentamatta. MBSA osaa varoittaa myös esimerkiksi käyttäjätunnusten heikoista salasanoista ja palomuuriasetuksista. (5, 29–31.)

Tarkistustulokset

MBSA laatii tuloksista selkeän raportin. Raportissa eritellään mitä kohteita on tarkistettu ja mikä asia vaatii korjausta. Testipalvelimen tarkistuksessa Microsoft Baseline Security Analyzer varoitti vierailija-käyttäjätunnuksen salasanan vanhentumattomuusasetuksen päällä olosta (kuvio 16). Tuloksia pystyy katsomaan tarkemmin Result details -kohdasta. Ohjelma osaa antaa myös vinkkejä, kuinka löydetty tietoturvariski korjataan. Salasana-asetuksen lisäksi muita tietoturvariskejä ohjelma ei löytänyt.



Kuvio 16. MBSA -ohjelman tarkistuksen tulokset

Microsoft Baseline Security Analyzer on liian suppea tietoturvaohjelmisto kokonaisvaltaisen palvelimen tietoturvaselvityksen tekemiseen. Ohjelma havaitsee vain Microsoftin tuotteisiin liittyviä tietoturvaongelmia, mutta ei ota huomioon kolmansien osapuolten kehittämiä sovelluksia. Tämän vuoksi on suositeltavaa käyttää myös jotakin muuta tietoturvallisuuden tarkistusohjelmaa.

4.2 GFI LanGuard

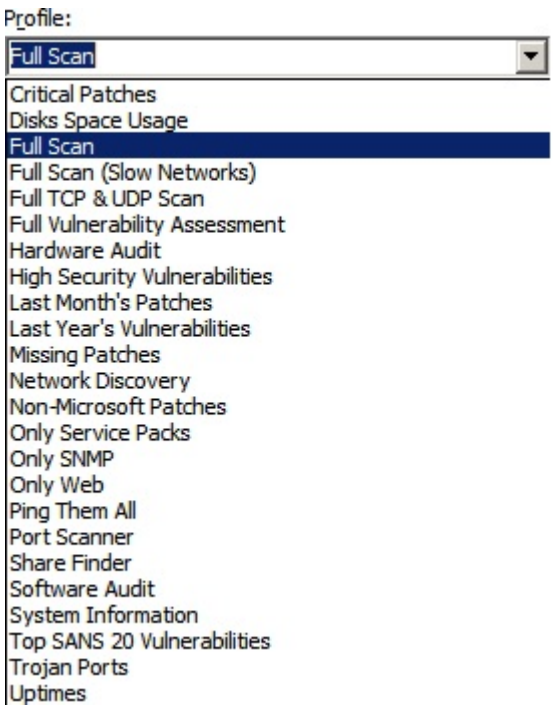
GFI Software Ltd:n kehittämä GFI LanGuard on tietoverkon turvallisuusuhkien ja haavoittuvuuksien etsintään suunniteltu ohjelma. Ohjelma tarkistaa verkon, käyttöjärjestelmien ja sovelluksien tietoturva-aukot ja auttaa niiden paikkaamisessa. GFI LanGuard tarkistaa esimerkiksi auki olevat portit ja avoimet

verkkojaot, käyttäjätunnuksien ja ryhmien määritykset, asennetut ohjelmat, puuttuvat huolto- ja korjauspäivitykset. GFI LanGuard tukee Microsoftin 32- tai 64-bittisiä käyttöjärjestelmiä Windows 2000 -versiosta lähtien. GFI LanGuard on maksullinen ohjelma, mutta siitä saa 30 päivän kokeiluversion. Kokeiluversio edellyttää rekisteröintiä GFI-internetsivuille. Rekisteröintilomakkeeseen pitää syöttää muun muassa etu- ja sukunimi, sähköpostiosoite ja postinumero. 30 päivän kokeilukäyttöön oikeuttava lisenssikoodi lähetetään sähköpostiin. Kokeiluversio on rajoitettu viiden IP-osoitteen auditointiin.

Opinnäytetyössäni käytin uusinta mahdollisinta versiota ohjelmasta, joka oli GFI LanGuard 2011 (build: 20111128). Ohjelman asentaminen on hyvin yksinkertaista. Asennuksen aikana ohjelma kysyy asennuksen kohdesijainnin, käyttöjärjestelmän järjestelmänvalvojan tunnukset ja salasanan sekä aktivointikoodin. GFI LanGuard -asennuksen jälkeen aukeaa ohjelman aloitusikkuna (kuvio 17). Aloitusikkunassa on paikallisen tietokoneen haavoittuvuuksien tasosta kertova mittari, ohjelman tarjoamat uusimmat tietoturvauutiset sekä valinta haavoittuvuustarkistuksen aloittamiseen. Remediate Security Issues -valinta tarjoaa työkalut tietoturvaongelmien korjaukseen.

Kuvio 17. GFI LanGuard -pääikkuna

Tarkistuksen aloittamiseksi valitaan tarkistuskohde, määritellään tarkistusoikeudet (käyttäjätunnus, tyhjä istunto, yksityinen avain) ja lisäksi valitaan tarkistusprofiili. Tässä projektissa tarkistuskohteeksi valitsin paikallisen testipalvelimen, tarkistusoikeudeksi järjestelmänvalvojan käyttäjätunnuksen ja tarkistusprofiiliksi ensimmäisellä tarkistuskerralla täydellisen tarkistuksen. Tarkistusprofiilien avulla etsintää voidaan kohdistaa ja rajata halutun tarkoituksen mukaisesti. Valittavana on useita valmiita profiileja, kuten täydellinen etsintä, laite- ja ohjelmistoauditointi (kuvio 18).



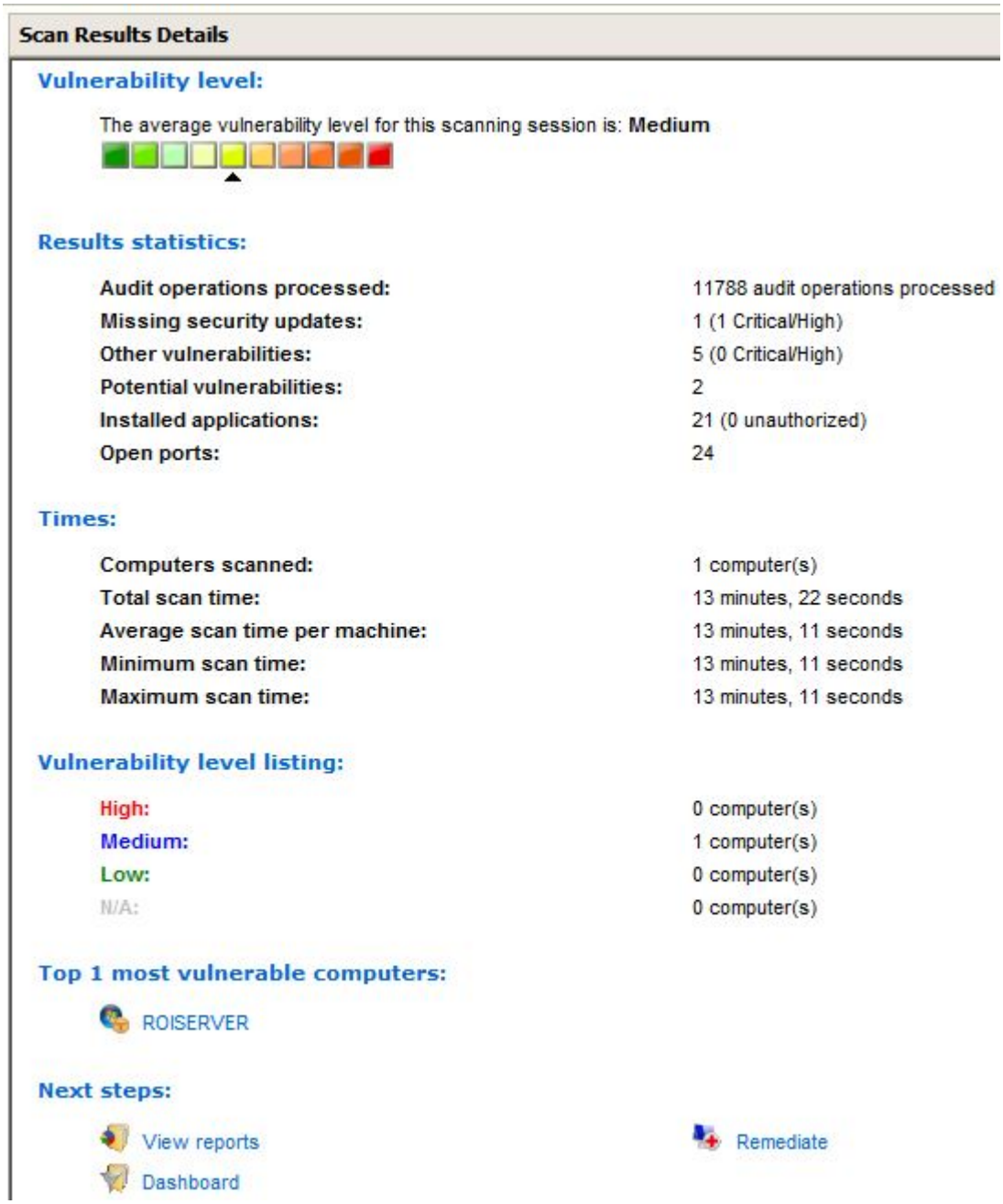
Kuvio 18. Tarkistusprofiilit

Profiileja pystyy myös muokkaamaan laajasti. Tarkistusprofiilien muokkaus tapahtuu Configuration-välilehdestä. Opinnäytetyötä varten en katsonut tarpeelliseksi muokata profiileja, vaan tein tarkistukset oletusasetuksilla.

Tarkistustulosten yhteenveto

Täydellisen tarkistuksen (*full scan)* jälkeen ohjelma luo tarkistustuloksista kuvion 19 mukaisen yhteenvedon. Yhteenveto kokoaa tiedot tarkistustuloksista, tarkistukseen käytetystä ajasta ja tietokoneiden haavoittuvuustasosta. Tarkistustuloksien alalaidassa on kolme linkkiä:

- View reports (raporttien katselu)
- Remediate (tietoturvauhkien korjaus)
- Dashboard (yleisnäkymä tietokoneen tilasta, tarkistuskohteista ja tietoturvauhkien korjauksesta).



Kuvio 19. Tarkistustulokset

Tarkistusraportti

Tietoturvaraporttien laadintaan GFI LanGuard tarjoaa monipuoliset työkalut. Raportteihin voidaan sisältää laajat ja yksityiskohtaiset tiedot tietoturvariskeistä, jotka ohjelma on löytänyt. Raportteja pystyy myös muokkaamaan haluamikseen ja niistä voi suodattaa tarpeettomat tiedot pois.

Kuviossa 20 on ote testipalvelimen tietoturvatasosta tehdystä raportista. Tietokoneen yleistä tietoturvallisuustasoa havainnollistaa neljään osaan jaettu mittari: ei mitattu, matala, keskitaso ja korkea. Testipalvelimen haavoittuvuustasoksi ohjelma ilmoittaa keskitason. Löydetyt tietoturvariskit ohjelma luette-

lee riskiluokan mukaisessa järjestyksessä. Testipalvelimesta analysointiohjelma löysi viisi tietoturvariskiä. Näitä olivat esimerkiksi puuttuva käyttöjärjestelmäpäivitys ja järjestelmänvalvojan automaattisesti jaossa olevat kansiot (*AutoShareWKS*). Microsoft oli julkaissut uusia käyttöjärjestelmäpäivityksiä Microsoft Baseline Security Analyzer -ohjelmalla tehdyn tarkistuksen jälkeen, minkä vuoksi MBSA ei niistä varoittanut.

Kuvio 20. Tarkistusraportti

Haavoittuvuuksien korjaus

Tarvittaessa ohjelma osaa kertoa tietoturvariskeistä lisätietoja ja opastaa niiden korjauksessa. Joitakin tietoturvauhkia pystyy korjaamaan ohjelmalla suoraan. Löydetyistä tietoturvariskeistä puuttuva käyttöjärjestelmäpäivitys oli kuitenkin ainoa, jonka pystyi korjaamaan ohjelman avulla. Muut tietoturvariskit täytyi korjata manuaalisesti analysointiohjelman antamien ohjeiden perusteella.

Analysointiohjelmien yhteenveto

Ohjelmat poikkeavat toisistaan paljon, eikä niitä ole mielekästä suoraan verrata. Microsoft Baseline Security Analyzer on ilmainen Microsoftin tuotteisiin keskittyvä ohjelma ja GFI LanGuard puolestaan maksullinen, monipuoliseen tietoverkon ja järjestelmien testaukseen tarkoitettu ohjelma.

GFI LanGuard tarjoaa selkeästi monipuolisempaa tietoturvan analysointia kuin Microsoft Baseline Security Analyzer. GFI LanGuard osaa varoittaa monista sellaisistakin tietoturvauhkista, jotka MBSA-ohjelmalla jäisi huomioimatta. Monipuolisuudestaan huolimatta ohjelman käyttö oli suhteellisen helppoa selkeän käyttöliittymän ja loogisten toimintojen ansiosta.

Kokenut palvelinylläpitäjä pystyy tarkistamaan suurimman osan analysointiohjelmilla tarkistettavista kohteista ilman erillisen ohjelman käyttöä. Hyvin pitkälle automatisoidut ohjelmat helpottavat kuitenkin urakkaa suuresti ja mikä tärkeintä, tarkistukset tulee todennäköisesti tehtyä säännöllisemmin tarkistusohjelman avulla.

5 YHTEENVETO

Saavutin mielestäni opinnäytetyölle asetetut tavoitteet hyvin ja työ valmistui ajallaan. Tavoitteena oli Windows-palvelinkäyttöjärjestelmän asentaminen alusta asti ja määritellä siihen perusasetukset ja roolit. Tämän jälkeen palvelimesta oli tarkoitus tehdä mahdollisimman turvallinen ja vastustuskykyinen tietoturvahyökkäyksiä vastaan. Tietoturvan taso oli lisäksi tarkoitus testata analysointiohjelmien avulla.

Palvelimista oli kertynyt kesätyöpaikkojen kautta hieman kokemusta, mutta syvällisempi kokemus puuttui. Opinnäytetyön ansiosta tietämys palvelimista ja palvelinturvallisuudesta kasvoi huomattavasti ja näiden tietojen pohjalta on hyvä jatkokehittää tietämystäni niistä.

Opinnäytetyön suurimpana haasteena oli saada palvelinturvallisuus-aihe rajattua mielekkääksi ja järkeväksi kokonaisuudeksi. Windows-palvelinkäyttöjärjestelmä sisältää erittäin paljon toimintoja ja erilaisia asetuksia. Oleellisimpia asioita ei saisi jäädä pois, mutta pieniä yksityiskohtia ja asetuksia oli välttämätön karsia. Aiheen rajausta auttoi tietoturvallisuudesta kertova kirjallisuus sekä internetistä löydetyt palvelimen suojaamisohjeet. Käyttökelpoisia ja luotettavia palvelimen koventamisohjeita oli kuitenkin yllättävän vaikea löytää.

Työn tekemisessä haasteena oli myös löytää sopivia tietoturvan analysointiohjelmia, joilla palvelimen tietoturvatason pystyi tarkistamaan. Kriteereinä oli löytää täysin ilmainen ohjelma sekä maksullinen ohjelma, joka sisältää ilmaisen kokeilujakson. Työhön soveltuvia ilmaisia ohjelmia ei tuntunut löytyvän muita kuin opinnäytetyössä käytetty Microsoft Baseline Security Analyzer. Maksullisia ohjelmia olisi ollut tarjolla useilta valmistajilta. Jatkokehitysideana tietoturvan analysointiohjelmien toimintaan voisi keskittyä syvällisemmin ja selvittää tarkemmin, mitä kohteita ohjelmat tarkistavat ja laatia niiden pohjalta tarkistuslista.

Opinnäytetyöstä voisi tehdä vastaavantyyppisen suojausohjeen myös Linux-palvelimille.

LÄHTEET

1 Drum, R. 2006. IDS and IPS placement for network protection. Osoitteessa http://www.infosecwriters.com/text_resources/pdf/IDS_Placement_RDrum.pdf. 12.4.2012.

2 Hakala, M. – Vainio, M. – Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: Docendo.

3 Holland, T. 2004. Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth. SANS Institute. Osoitteessa http://www.sans.org/reading_room/whitepapers/detection/1381.php. 12.4.2012.

4 Jansen, W. – Scarfone, K. – Tracy, M. 2008. Guide to General Server Security. National Institute of Standards and Technology. Osoitteessa http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf. 30.4.2012.

5 Järvinen, P. 2006. Paranna tietoturvaasi. Porvoo: Docendo.

6 Kivimäki, J. 2009. Windows Server 2008 R2 Tehokas hallinta. Hämeenlinna: Kariston Kirjapaino Oy.

7 Kotilainen, S. 2005. Keskitetty virustorjunta. Tietokone. Osoitteessa http://www.tietokone.fi/lehti/tietokone_4_2005/keskitetty_virustorjunta_2473. 25.4.2012.

8 Ruohonen, M. 2002. Tietoturva. Porvoo: Docendo.

9 Server Hardening. Osoitteessa http://www.serverhardening.com. 15.3.2012.

10 Windows Server 2008 Edition Comparison. Osoitteessa http://www.directionsonmicrosoft.com/sample/DOMIS/update/2008/02feb/0208ws2plp_ch.htm. 28.2.2012.

11 Windows Server 2008 R2 Features. Osoitteessa http://www.microsoft.com/en-us/server-cloud/windows-server/2008-r2-features.aspx. 28.2.2012.

12 Windows Server 2008 R2 Editions. Osoitteessa http://www.microsoft.com/en-us/server-cloud/windows-server/2008-r2-editions.aspx. 28.2.2012.