VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Vesa-Pekka Turunen & Kenan Kelmendi

SHAREPOINT-VIRUSTORJUNTA VALTAKUNNALLISEEN KONESALIIN

Valtion tieto- ja viestintätekniikkakeskus Valtori

Liiketalous ja matkailu, Tietojenkäsittely
2015

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Kenan Kelmendi ja Vesa-Pekka Turunen
Opinnäytetyön nimi	SharePoint-virustorjunta valtakunnalliseen konesaliin
Vuosi	2015
Kieli	Suomi
Sivumäärä	62
Ohjaaja	Mäkitalo Antti ja Kipronen Samuli (Valtori)

Tässä työssä tarkoituksena oli parantaa Valtorin (Valtion tieto- ja viestintätekniikkakeskus) tietoturvaa arkaluontoisten dokumenttien käsittelyssä. Pääpaino oli tutkimuksessa, testauksessa ja asennuksessa. Tässä työssä vastaamme kysymykseen miksi SharePoint-virustorjunta tarvitaan ja mikä on oikea ja toimeksiantajan tarpeisiin sopiva virustorjuntaohjelma.

Tärkeää työssä on myös dokumentointi ja tutkimus. SharePoint-virustorjunta on suhteellisen uusi asia ja tietoa on vaikea löytää.

Löydettyämme parhaan vaihtoehdon, teemme siitä karkean kustannusarvion ja hankintaehdotuksen.

Avainsanat Virustorjunta, tietoturva, palvelin

UNIVERSITY OF APPLIED SCIENCES
Bachelor of business administration, information technology

ABSTRACT

Author	Kenan Kelmendi & Vesa-Pekka Turunen
Title	SharePoint Antivirus Protection for a National Data Center
Year	2015
Language	Finnish
Pages	62
Name of Supervisors	Mäkitalo Antti & Kipronen Samuli (Valtori)

This work aimed to improve the handling of documents with sensitive information at Valtori (Government ICT Centre). The main focus centers on researching, testing and installing. This work aimed to answers such questions as: Why is SharePoint anti-virus needed? What is the best product for our needs?

Also, documenting is an important area of the thesis work. Antivirus for SharePoint is a relatively new topic and therefore information is hard to find. After finding the best option, a purchase suggestion and an evaluation of costs was made.

Keywords Antivirus, server, security

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

1 JOHDANTO 8

1.1 Työympäristö 9

1.2 Toimeksiantaja 9

1.3 Projektin suunnitelma 10

2 LÄHTÖTILANNE 12

3 SHAREPOINT 13

3.1 Työtilat 13

3.1.1 Työtilojen tärkeimmät oletusominaisuudet 14

3.1.2 Valinnaiset ominaisuudet 14

3.2 SQL 15

4 MIKSI ERILLINEN SHAREPOINT-VIRUSTORJUNTA TARVITAAN? 17

5 SHAREPOINT VIRUSTORJUNNAN TOIMINTA 18

6 HAITTAOHJELMAT/UHAT 20

6.1 Virukset 20

6.2 Madot 20

6.3 Troijalaiset 21

6.4 Lataaja 21

6.5 Takaovi 22

6.6 Näppäimistön tallentaja 22

6.7 Rootkit 23

6.8 Kiristysohjelmat 23

7 TESTIVIRUS EICAR 24

8 MUU TIETOTURVA JA INHIMILLISET VIRHEET 25

9 TUOTTEIDEN VERTAILU 27

10 SHAREPOINT-VIRUSTORJUNTATESTAUS 30

10.1 Testaussuunnitelma 30

10.2 Testiympäristö 31

10.3 Symantec Protection for SharePoint Servers 32

10.3.1 Asennus ja testaus 32

10.3.2 Testaus ja konfigurointi 32
10.4 ESET Security for Microsoft SharePoint Server 36
10.4.1 Asennus ja testaus 36
10.4.2 Testaus ja konfigurointi 38
10.5 Yhteenveto 39
10.5.1 Valinta 40
10.6 Symantec jatkotestaus 41
10.6.1 Tuotantoa vastaava testiympäristö 41
10.6.2 Päivitykset 42
11 HANKINNAT 43
12 LISENSSI 45
13 KUSTANNUSARVIO 46
14 YHTEENVETO 47
LÄHTEET 48
LIITTEET

KUVIO- JA TAULUKKOLUETTELO

Kuvio 1 Asiakkaat (Valtori 2015, www) 10
Kuvio 2 Työtila 15
Kuvio 3 Virustorjunta toimintakaavio 19
Kuvio 4 Kiristysohjelmat 23
Kuvio 5 Palvelimen varmistus 30
Kuvio 6 Symantec_conf 1 33
Kuvio 7 Symantec_conf 2 33
Kuvio 8 Symantec_conf 3 33
Kuvio 9 Prosessorin käyttö 34
Kuvio 10 EICAR testi 1 34
Kuvio 11 EICAR lisäys 34
Kuvio 12 EICAR testi 2 34
Kuvio 13 EICAR testi 3 35
Kuvio 14 Symantec_conf 4 35
Kuvio 15 Sähköposti-ilmoitus 36
Kuvio 16 ESET 37
Kuvio 17 ESET Conf 1 37
Kuvio 18 ESET scan 38
Kuvio 19 ESET Conf 2 38
Kuvio 20 ESET Virus havainto 39
Kuvio 21 ESET CPU käyttö 39
Kuvio 22 Symantec asennussuunnitelma 41
Kuvio 23 Hankintakaavio 44

Taulukko 1 Pisteet 28

LIITELUETTELO

LIITE 1. Eset security for Microsoft SharePoint server asennus

LIITE 2. Symantec protection for SharePoint asennus

1 JOHDANTO

Tietoturva on tärkeä asia nykypäivänä varsinkin yrityksissä. Tämän takia jokaisen työntekijän täyttyy yrittää pitää yllä tietoturvatasoa.

Omalla toiminnalla voi parantaa tietoturvaa huomattavasti ja perusteet ovat hyvät, jos yksilötasolla oikeat toimintatavat ovat hallussa. Tietoturvakoulutukset, tietoturvatasojen tietäminen, tiedottaminen ajankohtaisista uhkista, avoimuus ja tiedon jakaminen parantavat turvallisuutta.

Valitettavasti tämä ei aina riitä. Nykyaikaiset haittaohjelmat ovat hyvin kehittyneitä ja järjestäytynyt kyberrikollisuus on yleistä. Valtionhallinnossa jälkimmäinen voi olla myös valtiollisten konfliktien, tiedustelun ja häirinnän aiheuttamista.

Tässä opinnäytetyössä parannamme valtakunnallisen konesalin tietoturvaa SharePointin osalta. SharePointissa käsitellään arkaluontoisia dokumentteja, jotka voivat olla haluttua tietoa epäilyttäville tahoille. Myös haittaohjelmilla on tätä kautta epäsuora pääsy palvelimille käyttäjien jatkuvasti ladaten ja lähettäen Office-dokumentteja työasemalta. Jo ennen tiedostojen saavuttamista määränpäätänsä ne tulisi olla tarkistettuja.

Tässä työssä asennetaan tarpeisiin sopiva virustorjunta SharePoint-palvelimelle ja tutkitaan, miksi erillistä SharePoint-virustorjuntaa tarvitaan

1.1 Työympäristö

Valtorin Länsi-Suomessa sijaitsevassa valtakunnallisessa konesalissa on tällä hetkellä kaikkiaan 111 palvelinta, joista 67 on virtuaalisia ja 45 ovat fyysisiä. Palvelimista 92 prosenttia on käyttöjärjestelmältään Windows, joista SharePoint-palvelimia on kahdeksan. Näistä neljä on testauskäyttöä varten ja neljä tuotantoa varten.

Yllä mainittujen palvelimien lisäksi opinnäytetyötä varten on asennettu vielä yksi erillinen SharePoint-palvelin, joka ei ole tekemisissä tuotannon tai muiden testipalvelimien kanssa. Tässä palvelimessa voi tehdä erilaisia riskialttiimpia testauksia.

Kaikki SharePoint-palvelimet ovat virtuaalisia ja käyttöjärjestelmältään Windows server 2008 R2. Käyttäjä määrä on vaihteleva, mutta suurimmillaan tuhansia. SharePointilla pyörii osa mm. Elinkeino-, liikenne- ja ympäristökeskusten ja Aluehallintovirastojen palveluista, kuten SharePoint-työtilat.

Osassa näistä palvelimista on Microsoft Forefront-virustorjuntaohjelmisto. Suljetusta verkosta huolimatta tietoturvaohjelma on oltava kaikissa alustapalvelimissa. Valtorin käytössä on jo Microsoft ForeFront-virustorjunta ja tarkoituksena on asentaa kyseinen virustorjuntaohjelma kaikkiin alustapalvelimiin. Forefrontiin on saatavilla myös SharePoint-virustorjunta, mutta Microsoft lopettaa tuen koko Forefrontille vuoden 2015 lopussa.

Tämän takia SharePoint-virustorjunnaksi tulee kartoittaa jonkin toisen valmistajan ohjelmisto.

1.2 Toimeksiantaja

Valtion tieto- ja viestintätekniikkakeskus Valtori perustettiin vuoden 2014 alussa olemassa olevien valtion ict-palvelukeskusten ja virastojen tietohallintoyksiköiden yhdistymisten tuloksena.

Valtori on valtiovarainministeriön alainen virasto, joka tuottaa perustietotekniikka- ja tietojärjestelmäpalveluja sekä sähköisen asioinnin ja hallinnon tukipalveluja.

Seuraavana on lukuja Valtorin tilastoista.

- Tällä hetkellä henkilöstöä n. 550 henkilöä. Tulevien toimintosiirtojen myötä vuoden 2015 lopussa henkilöstöä tulee olemaan n. 1100.
- Toimintaa 34 paikkakunnalla.
- Sopimuskanta n. 142 M€.
- Työasemia hoidossa n. 47 500 kpl.
- Palvelimia vastuulla n. 3700 kpl.

Toiminta on valtakunnallisesti hajautettua mutta pääpaikkakuntana on Jyväskylä, Helsinki on myös merkittävässä asemassa. Kuviossa 1 on Valtorin asiakkaita ja palveluiden hajaantuminen niiden kesken.

Kuvio 1 Asiakkaat (Valtori 2015, www)

1.3 Projektin suunnitelma

Tämä työ tullaan tekemään projektina, jossa koitetaan noudattaa opinnoissa ja työpaikalla olevia ohjeistuksia projektien hallinnasta. Projektin suunnitellaan ja tarkastuspisteet määritellään, jotta jaetut työt pysyvät aiheessa. Projektinhallinnalla saadaan pidettyä tutkitut sekä tuotetut materiaalit kasassa ja yhdistettyä lopulliseksi työksi.

Kerran kahdessa viikossa käydään ohjaajan kanssa läpi työn eteneminen, asetetut tavoitteet sekä muutokset ja haasteet. Tällöin sovimme uusista tehtävistä ja etenemisen jatkosta, mikä mahdollistaa myös työn jakaantumisen projektiryhmän kesken. Projektissa on kaksi henkilöä.

Budjetissa pysymistä ei tässä tapauksessa tarvitse seurata, mutta resursointia täytyy pohtia tasaisin väliajoin. Lopuksi teemme kustannusarvion ohjelmiston hankinnasta. Töiden tekeminen on ensimmäinen prioriteetti ja kiireet ensisijaisessa työssä menevät tarvittaessa tämän työn edelle. Kiireisissä työtilanteissa voi toinen henkilö tarvittaessa hoitaa toisen tehtäviä.

Vaikka tämä projekti ei ole ohjelmistokehitystä, niin projektinhallinta noudattaa jossakin määrin Scrum tyylistä etenemistä. Esimerkiksi kahden viikon välein olevat tarkastuspisteet, eli ”sprintit”.

Yksi osa projektia ovat testaukset, jotka on jaettu eri tehtäviksi. Tämä suunniteltiin niin, että yksi henkilö suorittaa yhden sovelluksen asennuksen, dokumentoinnin ja testauksen, ja toinen toisen. Tähän sisältyy testiympäristön valmistelua kuten esim. palvelimen varmistaminen nauhalle. Sen jälkeen dokumentit kasataan yhteen, käydään läpi ja kootaan yhdeksi raportiksi.

2 LÄHTÖTILANNE

Kuten aikaisemmin todettu, Valtorilla on tällä hetkellä työasemilla ja joillakin palvelimilla Microsoft Forefront-virustorjuntaohjelmisto. Tällä hetkellä Valtori on kilpailuttanut uuden virustorjunnan hankinnan. Hankinnassa on ilmoitettu vaaditut ominaisuudet ja palvelinten kohdalla ei ole mainintaa SharePoint-torjuntaominaisuudesta.

3 SHAREPOINT

Microsoft SharePoint on ohjelmisto, joka asennetaan Microsoft Windows-Palvelimelle. Taustalla on Sql-palvelin ja tietokanta. Ohjelmiston tarkoitus on tarjota selainpohjainen järjestelmä tiedostojen ja tiedon jakamiseen, sekä säilöntään ilman syvällisempää tietotekniikan ymmärrystä. Ohjelmoijat voivat toki laajentaa SharePointin toiminnollisuutta, mutta pelkät valmiit perusominaisuudet tarjoavat runsaasti työkaluja luoda kehittyneitä web-sivuja.

SharePointia käytetään organisaatioissa intranet- ja extranet-palveluina, joita voi hyödyntää suuri joukko käyttäjiä. Tämä mahdollistaa myös suurten tai pienten projektien hallinnan ja yhteistyön. Projekteja varten voidaan luoda ns. työtiloja.

Työtiloihin voidaan lähettää ja ladata tietoa, työstää dokumentteja monen henkilön toimesta ja sallia organisaation ulkopuolisten henkilöiden osallistuminen. Ulkopuolisille käyttäjille luodaan omat tunnukset, joilla pääsee vain haluttuun työtilaan. Halutussa työtilassa voidaan rajata käyttöoikeuksia tarpeen mukaan.

SharePointin hyvin suunniteltu dokumenttikirjasto mahdollistaa mm. töiden hyväksymistä, versiointia ja sisällönhallintaa yleisesti. Työtilat helpottavat täten erilaisten työprosessien automatisointia. (Premier point solutions 2015; www. Microsoft 2015, www)

3.1 Työtilat

Yrityskäytössä työtilat ovat oleellisia toimintoja SharePointissa. Tässä työssä katsomme asiaa tarkemmin Valtorin näkökulmasta.

Työtilat ovat nopeasti käyttöönotettavia ryhmätyötiloja, joita voi muokata vastaamaan erilaisten työryhmien toimintaa. Työtila voi koostua esimerkiksi kalenterista, asiakirjakirjastoista, tehtävälistoista ja keskustelufoorumista.

Työtiloja tarjottaessa palveluna asiakas voi halutessaan itse rakentaa käyttöoikeushierarkian.

Asiakas voi muokata työtilaa, muuttaa sen näkymiä sekä lisätä ja poistaa vakiokomponentteja. Muokkaus tapahtuu selaimella. Asiakkaan itse toteuttamia komponentteja ei voi liittää työtiloihin. Palveluun ei sisälly muokkauksen opastusta eikä muuta SharePoint-opastusta.

3.1.1 Työtilojen tärkeimmät oletusominaisuudet

Dokumenttikirjasto

Dokumenttikirjasto on työryhmäläisten omien ja yhteisten asiakirjojen säilytyspaikka. Kirjasto tarjoaa helpon tavan asiakirjan yhteiselle muokkaamiselle, yhteisille asiakirjojen metatietokentille ja versionhallinnalle.

Ilmoitukset-lista

Ilmoitukset -lista mahdollistaa tärkeän tiedon levittämisen työryhmän etusivun kautta jokaiselle työryhmäläiselle.

Tehtävälista

Tehtävälistalla voidaan luoda ja määrittää tehtäviä työryhmän jäsenille sekä seurata niiden edistymistä

Keskustelualue

Keskustelualue on työryhmän jäsenille tietojen jakamista ja keskustelua varten.

3.1.2 Valinnaiset ominaisuudet

Projektitehtävät

Projektitehtävä on komponentti, jolla voidaan hallita projektia aikatauluttamalla ja määrittelemällä erilaisia projektitehtäviä. Näitä voidaan nostaa tarpeen vaatiessa esille laajemmin, kuten etusivulle.

Linkkilista

Linkkilista sisältää työryhmään tai projektiin liittyviä linkkejä.

Oma Wiki-sivusto

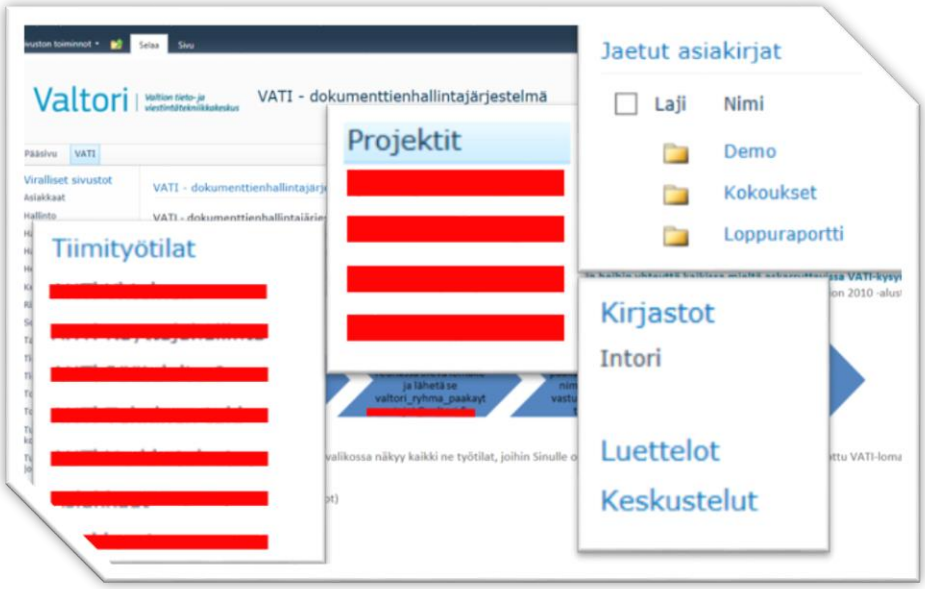
Wikipedia-tyylinen sivu projektiin liittyvää tietoa, apua ja vihjeitä varten.

Blog

Blogi on epävirallisempi osio, jota voidaan käyttää etenemisen tiedottamiseen sisäisesti ja ulkoisesti.

Yhteystiedot

Yhteystiedot ovat ryhmän ja tärkeiden kontaktien yhteystietojen lisäämistä sekä ylläpitämistä varten.



Kuvio 2 Työtila

3.2 SQL

Sql on oleellinen osa SharePointin toimintaa. SharePointin konfiguraatiot, sisältötietokannat ja sovelluspalvelut ovat sql:ssä. Yksinkertainen SharePoint-farmi voi vaatia jopa 32 eri tietokantaa. SharePoint-sivustoilla voi olla useita tietokantoja.

Vähimmäisvaatimukset SharePointissa ovat SQL Server 2008 R2, jossa on oltava vähintään Service Pack 1, SQL Server 2012 tai SQL Server 2014.

SharePoint sovellus on rakennettu SQL Server-tietokannan päälle. Useimmat sisältö-, asetus- ja konfiguraatiotietokannat on tallennettu sql-palvelinten relaatiotietokantoihin.

Konfiguraatiotietokannat sisältävät mm:

- tietoa farmin asetuksista ja määrityksistä sekä mitä tietokantoja käytetään.
- IIS web-sovelluksista ja palveluista
- sivusto pohjat ja estetyt tiedostomuodot
- farmilla voi olla vain yksi konfiguraatiotietokanta.

Sisältötietokannoissa on esim.:

- sivuston dokumentit, kuten kirjastot sisältöineen (käyttäjien dokumentit)
- SharePoint-sovellusten vaatimat tiedot
- käyttäjänimet ja käyttöoikeudet.

Jokaisella web-sovelluksella voi olla oma sisältötietokanta. Jokaiseen “sivustokokoelmaan” voi liittää vain yhden sisältötietokannan, mutta yksi sisältötietokanta voi olla monessa sivustokokoelmassa.

Näiden lisäksi palvelusovelluksilla on omat tietokannat.

SharePoint-palvelimen tuetut tietokannat luodaan yleensä automaattisesti asennuksen aikana tai myöhemmin ohjatun asennustoiminnon aikana. Tietokantojen ylläpitäjät voivat tehdä niitä manuaalisesti.

4 MIKSI ERILLINEN SHAREPOINT-VIRUSTORJUNTA TARVITAAN?

Virustorjunta SharePoint-ympäristössä jakaantuu kahteen kategoriaan: palvelinten suojaaminen ja SharePointiin tallennettujen tiedostojen suojaaminen.

SharePointin tallentaessa tiedon sql-sisältötietokantoihin ei palvelimella itsellään ole varsinaisesti vaaraa saada tartuntaa SharePointiin ladatusta tiedostosta. Mutta ilman SharePoint-virustorjuntaa SharePointista voi muodostua eräänlainen varasto haittaohjelmille. Varsinkin suorittavat tiedostomuodot voisivat aiheuttaa harmia ja ne ovatkin yleensä estettyjen tiedostomuotojen joukossa.

Työasemat ovat jo oletuksena suojattuja. jos työasemat ovat puhtaita, ei SharePointiinkaan asti pääse haittaohjelmia. Voidaanko omiin työasemiin luottaa? Työasemilla tapahtuvat haittaohjelmahavainnot eivät ole harvinaisia.

Ulkopuoliset käyttäjät luovat uhan ja niiden puhtauteen ei tulisi luottaa. Vaikka työtilaan olisi hyväksytty ulkopuolinen käyttäjä luotettavasta organisaatiosta, ei organisaatio eikä ympäristö silti ole oma ja tunnettu. Tarkoituksellinen urkinta, takaovien luonti ja tiedustelu on myös varsinkin valtion hallinnossa vakavasti otettava uhkatekijä. SharePointiin kohdistettu epäilyttävä toiminta on todennäköisesti hyvin vähäistä, mutta siihenkin panostamalla saadaan lisää tietoturvaa. On otettava huomioon, että kokonaistietoturva koostuu useista tekijöistä.

“I find it curious that more antivirus vendors don’t offer such protection. Without an additional layer of protection users can mistakenly upload compromised files to the SharePoint Server and infect the entire database,” Richard Foley, ESET Ireland, Toimitusjohtaja.

Yllä oleva lainaus on varsin paikkaansa pitävä. On erikoista että nyt vasta SharePoint-virustorjunnat ovat alkaneet yleistymään. Silti kaikki tuotteet eivät tue viimeisimpiä SharePointin versioita. (SPTechCon 2015, www)

5 SHAREPOINT VIRUSTORJUNNAN TOIMINTA

SharePointissa itsessään on virustorjunta ohjelmointirajapinta (Application Programming Interface, API). Tämä ohjelmointirajapinta perustuu Microsoft Exchange Palvelimen VS API 2.0 rajapintaan.

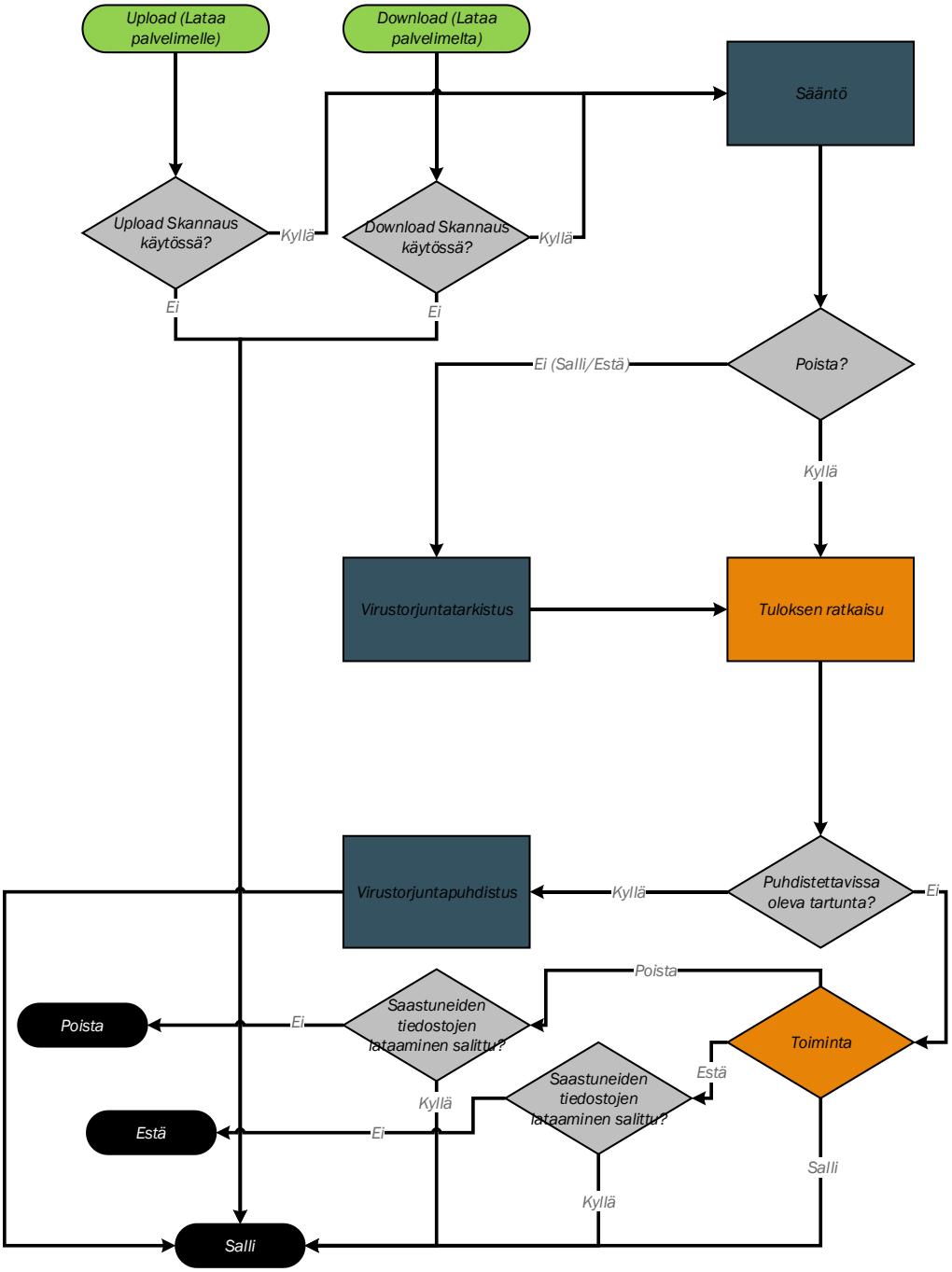
SharePoint VS API 1.4 sisältää paljon alkuperäisiä Exchange palvelimen ominaisuuksia, mutta on optimoitu nopeuteen Microsoft SQL palvelin-ympäristössä. Tämä saavutetaan luomalla alemman tason API, joka integroituu suoraan tiedoston tallennus ja avaustoimintoon SharePointissa.

SharePointin rajapinta mahdollistaa kolmannen osapuolen virustorjunnan asentamisen SharePointiin ja sen hallinnan integroimisen SharePointin hallintakäyttöliittymään.

SharePoint-virustorjunta perustuu oleellisesti siihen, että tiedostot skannataan silloin kun ne avataan tai tallennetaan.

Koska tiedostoja tallennetaan suoraan SharePoint-sisältötietokantaan, tavallisten palvelinperusteisten tiedostoskannereiden ei ole mahdollista tarkastaa tiedostoja ”lennosta”. Ne eivät myöskään ymmärrä ja havaitse jo tietokannoissa mahdollisesti olevia haittaohjelmia. (Taylor 2015, www. Microsoft 2015b, www. Microsoft 2015c, www)

Kuvio 3 Virustorjunta toimintakaavio



Kuviossa 3 on kaavio, jossa on kuvattu esimerkki siitä millaiset säännöt tiedostojen tarkistamiselle voi asettaa, kuten sallitaanko saastuneen tiedoston lataus, vai poistetaanko se.

6 HAITTAOHJELMAT/UHAT

Tunkeutumiset suoritetaan yleensä haittaohjelmia hyväksikäyttäen. Seuraavaksi käydään läpi yleisimpiä haittaohjelmia.

6.1 Virukset

Tietokonevirus korruptoi jo olemassa olevia tiedostoja tietokoneella. Virukset on nimetty biologisten virusten mukaan, koska ne käyttävät samanlaisia tekniikoita levitäkseen tietokoneesta toiseen.

Virukset hyökkäävät pääsääntöisesti suorittavia- ja dokumentti-tiedostoja kohti. Lisääntyäkseen virus kiinnittää itsensä tiedoston loppuosaan.

Lyhyesti, tietokonevirus toimii seuraavasti: Kun tartunnan saanut tiedosto suoritetaan, virus aktivoi itsensä ennen alkuperäistä sovellusta. Tämän jälkeen se suorittaa ennalta määritetyn tehtävän. Vasta sen jälkeen alkuperäinen sovellus suoritetaan. Usein virus ei voi tartuttaa konetta, ellei käyttäjä itse vahingossa tai tahallaan avaa haittaohjelmaa.

Tietokoneviruksia on monenlaisia riippuen niiden tarkoituksesta. Osa niistä on erittäin vaarallisia, koska ne voivat poistaa tarkoituksella tiedostoja pysyvästi. Toisaalta, jotkin virukset eivät aiheuta varsinaisesti vahinkoa, mutta niiden tarkoitus on vain häiritä käyttäjää ja näyttää niiden kehittäjän teknisiä kykyjä.

On tärkeää huomata, että virukset ovat harvinaisempia, koska ne eivät ole kaupallisesti houkuttelevia haittaohjelmien luojille verrattaessa troijalaisiin ja vakoiluohjelmiin. Termiä ”virus” käytetään usein väärin kuvaamaan kaikkia tunkeutumistapoja ja haittaohjelmia. Nykyisin käytetäänkin termiä haittaohjelma, malware.

6.2 Madot

Tietokonemato on ohjelma, joka sisältää haitallista koodia ja leviää verkkojen välityksellä. Oleellinen ero viruksen ja madon kohdalla on, että madoilla on kykyä li-

sääntyä ja kulkea itsenäisesti – ne eivät ole riippuvaisia isäntätiedostoista tai käynnistysosioista. Madot leviävät sähköpostiosoitteiden kautta yhteystietolistoilta tai hyödyntävät tietoturva-aukkoja verkkosovelluksissa.

Täten madot ovatkin kannattavampia ja elinkykyisempiä. Internetin laajuudesta johtuen ne voivat levitä maailman laajuisesti tunneissa tai jopa minuuteissa niiden julkaisusta. Kyky monistua itsenäisesti ja nopeasti tekee madoista vaarallisempia kuin muuntyyppisistä haittaohjelmista.

Järjestelmässä aktivoitunut mato voi aiheuttaa monenlaisia haittoja poistamalla tiedostoja, alentamalla järjestelmän suorituskykyä tai jopa poistamalla ohjelmia. Tietokonematojen luonne ja toiminnot myös mahdollistavat liikenteen muunlaiselle tunkeutumiselle järjestelmään.

6.3 Troijalaiset

”Troijan hevoset” nimitys juontaa juurensa historiaan ja niiden toimintatapa on samanlainen. Ne esittävät olevansa hyödyllisiä ohjelmia ja näin huijaavat käyttäjän suorittamaan niitä. Niiden yksinomainen tarkoitus on tunkeutua järjestelmään niin helposti kuin mahdollista ja suorittaa haitalliset tehtävät. Ilmaisemalla että koneella on troijalainen, tarkoitetaan tunkeutumista, jota ei voida luokitella mihinkään tarkkaan tai haittaohjelmatyyppiin.

Troijalaiset ovat hyvin laaja käsite ja niinpä ne usein jaetaan moniin alatyyppeihin.

6.4 Lataaja

Lataaja on haitallinen ohjelma, joka tunkeuduttuaan lataa lisää haitallisia ohjelmia järjestelmään.

Tämä on myös yksi ns. troijalaisista ja kykenee yhdistämään internetiin HTTP-yhteyden avulla. Asennuttuaan koneelle tämä haittaohjelma voi myös tallentaa näppäimistön painalluksia ja lähettää yksityisiä tietoja rikollisille. Lataajatyyppinen troijalainen on hyvin vaarallinen ja avaa suuren aukon kohteen tietoturvaan.

6.5 Takaovi

Takaovi on sovellus, joka mahdollistaa kommunikoinnin etäkohteeseen. Toisin sanoen se voi avata ei haluttuja etäyhteyksiä järjestelmään ja mahdollistaa järjestelmän luvattoman käyttämisen.

Yleensä takaovet sijaitsevat ohjelmien koodissa ja ovat ohjelmoijan sinne laatimia. Takaovia voidaan laittaa ohjelmiin tarkoituksella jo niitä valmistettaessa. Tämä mahdollistaa sen, että ohjelmaa voidaan myöhemmin käyttää tiedon hankkimiseen. Suurimmalle osalle käyttäjistä ohjelma siis voi olla täysin vaaraton. Esimerkiksi valtiollisten toimijoiden halutessa voidaan takaovia käyttää hyväksi tiedustelussa ja vastaavassa toiminnassa.

6.6 Näppäimistön tallentaja

Näppäimistön tallentaja tallentaa näppäimistön painallukset ja lähettää ne eteenpäin. Päästyään koneelle voi tallentaa jokaisen näppäimistön painalluksen, säilöä ne erilliseen tiedostoon ja lähettää ne eteenpäin hyökkääjälle. Näppäimistön tallentaja voi vuotaa käytännössä kokonaisia keskusteluja, käyttäjätunnuksista ja salasanoista puhumattakaan.

Esimerkkinä tallennetuista näppäimistön painalluksista voidaan lukea järjestyksessä seuraavaa. Käyttäjä on kirjoittanut Facebookin osoitteen, jonka jälkeen voidaan olettaa lähes varmasti seuraavien painallusten olevan kyseisen palvelun käyttäjätunnus ja salasana.

Näppäimistön tallentaja voi olla myös fyysinen laite näppäimistön ja koneen välissä, joka tallentaa painallukset. Laite haetaan myöhemmin ja sisältö puretaan haluttuun sijaintiin.

6.7 Rootkit

Rootkit on luvaton ohjelma joka mahdollistaa laajempien käyttöoikeuksien saamisen koneelle. Sana ”Root” viittaa Linux-maailman järjestelmänvalvojaoikeuksiin. Rootkiteille on ominaista jatkuva ja aktiivinen piilossa pysyminen. Rootkitien toiminnalle on tyypillistä erittäin vaikea havaittavuus.

Rootkittejä käytetään myös bottiverkkojen, eli orjakoneverkkojen rakentamiseen.

6.8 Kiristysohjelmat

Viime aikoina on myös yleistynyt eräänlainen lunnaiden vaatiminen haittaohjelmien avulla. Koneen tiedot voidaan salata luvattomasti ja niitä ei avata ennen kuin salaaja on saanut haluamansa lunnaat. Lunnaiden maksaminen ei takaa tietojen palauttamista. (Wiki-Security 2015, www)

Kuvio 4 Kiristysohjelmat

7 TESTIVIRUS EICAR

EICAR testitiedoston tarkoitus on tarjota standardivirustorjunta ohjelmien testaamiseen.

Testitiedoston on kehittänyt European Institute for Computer Antivirus Research (EICAR) ja Computer Antivirus Research Organization (CARO).

Sitä tukevat virustorjunta ohjelmat havaitsevat sen samalla tavalla kuten oikean haittaohjelman. Tämä mahdollista asennuksen onnistumisen varmistamisen, erilaisten konfiguraatioiden kokeilemisen, erilaisten virheiden ja havaintojen ilmoitusten säätämisen.

Tiedostosta on joitakin eri versioita, mutta yleisin lienee tietyn merkkijonon sisältävä txt-tiedosto esim. X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*.

Yllä olevan merkkijonon voi tallentaa tekstitiedostoksi (.txt-tiedosto), ja on sen jälkeen torjuntaohjelmistojen havaittavissa.

(Virus bulletin 2015, www)

8 MUU TIETOTURVA JA INHIMILLISET VIRHEET

SharePointin tietoturva on paljon muutakin kuin vain virustorjunta. Suuri osa tietoturva-aukoista on inhimillisiä, käyttäjiin ja oikeuksiin liittyviä. Esimerkkinä voidaan pitää Yhdysvaltojen armeijan wikileaks-tietovuotoa. Erään todistajanlausunnon mukaan suuri osa vuotaneista tiedoista saatiin SharePoint-palvelimilta.

Tämä on oiva esimerkki siitä, kuinka valvonnalla ja oikeuksilla SharePointissa on oleellinen rooli tietoturvan kannalta. Valvonta ei tarkoita reaaliaikaista työskentelyn seurantaa vaan sitä, että tiedetään kuka ja miksi tarvitsee pääsyn tietoihin. On toki mahdotonta ennustaa kenenkään tulevia mahdollisia haitallisia toimia, kuten wikileaks-vuodossa, mutta rajaamalla jo alusta pitäen oikeudet vain sitä tarvitseville voidaan pienentää riskejä huomattavasti.

Tietoturvakoulutukset ovat erittäin tärkeä osa tietoturvaa, kuten aiemminkin jo tässä työssä on todettu. Moni tutkimus osoittaa, että suuri osa käyttäjistä ei välitä tai he eivät tiedä tietoturvan tärkeydestä SharePointissa. Niin sanottu ”kunhan työ tulee tehtyä” asenne murtaa yllättävän monta turvakäytäntöä, eikä tämä koske vain SharePointtia.

Tietojen vaihto SharePoint työtilaan oikeudet omaavan käyttäjän ja sinne ilman oikeutta olevan välillä on myös vaikea tilanne. Työtilaan pääsyn omaava voi tallentaa tietoa usb-muistitikulle ja luovuttaa tämän kollegalle, jotta työt saadaan tehtyä. Tällainen tilanne on ongelmallinen kahdesta syystä; Joko oikeudet ovat määritelty väärin tai sinne pääsyä tarvitsevalta käyttäjältä ne ovat jääneet saamatta. Tästä johtuen tietoa siirretään helposti hukkaan joutuvalta usb-tikulta koneille, joiden perässä ei enää pysytä, tai käyttäjällä ei ole tarkoituksella oikeutta kyseisiin tietoihin. Joka tapauksessa käyttäjien tulisi anoa oikeuksia, jos tällainen ongelma ilmenee. Tähän tosin harvoin halutaan ryhtyä, koska joissakin organisaatioissa käyttöoikeuksien saaminen voi olla yllättävänkin jäykkää ja suuren byrokratian takana.

Yllä olevat asiat voivat jäädä seisomaan myös koska ei tiedetä mistä oikeuksia haetaan ja missä niitä hallinnoidaan. Ei riitä että SharePoint ympäristö laitetaan pystyyn vaan sitä täytyy myös ylläpitää. Ilman ylläpitäjää ei voida pitää myöskään ohjelmistoja ajan tasalla, kuten tietoturvapäivityksiä.

Ylläpito ja oikeuksien määrittely on myös erittäin laaja teema, joka voisi olla lähes oma aiheensa. Yleensä kuitenkin käyttöoikeuksia jaetaan ryhmittäin, joten hyvin luotu Active Directory on tärkeää. Sen avulla yleensä erilaiset käyttäjätunnuksiin liittyvät määritykset linkitetään ja sieltä tehdyt määritykset periytetään muuallekin.

SharePointissa on mahdollista määritellä hakutoimintoja eri tavoin. Virheellisesti määritellyt hakuasetukset voivat arkaluontoista tietoa sisältävillä SharePoint-palvelimilla johtaa hakutuloksiin, jotka paljastavat väärät dokumentit väärille henkilöille. Pelkkä hakutulos ja parin esikatselurivin näkeminen word-dokumentista voi riittää, vaikka oikeutta ei olisi avata koko dokumenttia. Tämä tieto väärissä käsissä voi johtaa siihen, että haluttu tieto löydetään, mutta sitä ei saada auki.

Eräs mielestämme kyseenalainen toiminto on Valtorilla tullut vastaan muutamissa tilanteissa: SharePoint tietojen synkronointi työasemille tarkoittaen kokonaisen työtilan pitämistä offline-tilassa työasemalla näkyen käyttäjälle paikallisena kansiona, johon tallennetut tiedot latautuvat verkossa ollessa automaattisesti myös SharePoint palvelimelle. Jos työasema joutuu uhatuksi, on tältä työasemalta myös periaatteessa suora pääsy työtilaan ja jopa SharePoint-palvelimeen.

9 TUOTTEIDEN VERTAILU

Aluksi käymme läpi yleisten arvosteluiden ja julkaisujen pohjalta parhaat vaihtoehdot. Sen jälkeen tarkoitus on tutustua ja testata kahden tuotteen yksinkertainen käyttöönotto ja pieni koekäyttö. Testauksessa tarkoituksena on käydä läpi konfiguroinnit ja käyttöliittymät. Tavoitteena on yksinkertaisuus, mutta kuitenkin riittävät mahdollisuudet erilaisia konfigurointeja varten. Myös resurssien käyttöön kiinnitetään huomiota. SharePoint virustorjunnan on vaadittava mahdollisimman vähän ylläpitoa ja olla huomaamaton taustalla. Liikenne ja dokumenttien määrät, jotka SharePoint-työtiloissa ovat voivat olla huomattavia. Jos dokumenttien hallinta ei ole sujuvaa, se tulee heijastumaan pahimmillaan kokonaisten organisaatioiden toimintaan projekteissa ja tavallisessa työskentelyssä.

Alustava tuotteiden kartoitus

SharePoint-virustorjuntavaihtoehtoja oli viisi, joista kaksi valittiin testattavaksi. Kartoituksessa mukana olivat BitDefender, Forefront, Symantec, SopHos ja ESET. Koekäyttöön valitut SharePoint-virustorjunnat ovat ESET Security for Microsoft SharePoint ja Symatec Protection for SharePoint.

Ennen vertailua mietimme erilaisia ominaisuuksia ja vaatimuksia, joita tuotteelta haluamme. Sen jälkeen pisteytimme eri ohjelmistoja perustuen siihen miten hyvin haluamamme määritelmät löytyivät niistä.

Laitteisto- ja ohjelmistovaatimuksena virustorjunnan täytyy tukea Windows Server 2008:aa ja uudempia versioita sekä sisältää tuki SharePoint 2013:lle. Käyttöliittymän olisi hyvä olla integroitu SharePointin omaan käyttöliittymään hallinnoinnin helpottamiseksi. Virustorjunta on SharePoint-palvelimen ylläpitäjän tehtävä.

Matalat laitteistovaatimukset ovat myös etu. Toki olemassa olevat laitteistot käyttöjärjestelmineen täyttävät laitteistovaatimukset mutta resursseja on aina rajallinen määrä. Myös vähäinen kuormitus tarkoittaa vakaampaa toimintaa. Hyvä olisi myös olla mahdollisuus jonkinlaisten rajojen määrittämiseen sille, kuinka paljon virustorjuntaohjelmisto saa resursseja.

Tiedostojen tarkistamisessa olisi hyvä olla mahdollisuus tehdä se toisella palvelimella. Eli ns. Scan engine tulisi olla mahdollista asentaa omalle palvelimelle, jolloin tiedostot tarkistetaan siellä, eikä se täten kuormita jo suurta dokumenttiliikennettä pyörittävää SharePoint-palvelinta.

Reaaliaikainen seuranta on pakollinen vaatimus.

Toimiva ja nopea sähköpostihälytys olisi hyvä löytyä, sekä jonkinlaisten raporttien luominen.

Ohjelmiston kieli sekä siihen tarjottavan tuen kieli tulisi olla suomi tai englanti. Englanti riittää, mutta suomi olisi lähinnä etu.

Vahvimpina ovat ESET ja Symantec.

Taulukko 1 Pisteet

	ESET	BitDefender	Forefront	Symantec	SopHos
Laitteistovaatimukset	5 p	5 p	5 p	5 p	5 p
Yhteensopiva käyttöjärjestelmä	5 p	2 p	5 p	5 p	3 p
Keskeiset ominaisuudet	5 p	5 p	5 p	5 p	5 p
Tuki	5 p	5 p	0 p	5 p	5 p
Hallintaliittymä	5 p			5 p	
Raportointi	5 p			5 p	
Kuormituksen jakaminen	5 p			5 p	
Koekäyttömahdollisuus	5 p			5 p	
Käyttöliittymän integroituminen	0 p			5 p	
Yhteensä	40 p	17 p	15 p	45 p	18 p

Käytössämme olevat laitteet täyttävät kaikki laitteistovaatimukset, joten jokainen virustorjunta sai 5 pistettä. BitDefender ei ollut yhteensopiva SharePoint 2013:n kanssa, joten pisteiden saaminen jäi vähemmälle. Myös SopHosin yhteensopivuus oli epävarmaa, joten vähemmän pisteitä siitä. Kaikissa oli hyviä perusominaisuuksia, joita ennen taulukkoa määrittelimme ja jokainen sai täydet pisteet. Tuki oli yksi iso ongelma Forefrontille. Microsoft on ilmoittanut, että tuki Forefrontille loppuu vuoden 2015 lopussa. Tuki jatkuu vain siinä tapauksessa, jos tuotteen jo omistaa, joten kyseistä tuotetta ei voi edes enää hankkia.

Hallinta ja raportointi selviävät testiasennuksen jälkeen.

Tuotteiden kartoituksessa käytettiin avuksi valmistajilta saatavia teknisiä dokumentaatioita. Näistä dokumenteista selviää tarkempia tietoja ohjelmistoista ja ne ovat suunnattu muutenkin yrityskäyttöön.

Myös erilaisia arvostettuja alan organisaatioita, jotka testaavat, tarjoavat ohjelmistojen vertailuja, sertifikaatteja ja arviointeja käytettiin hyväksi. (AV comparatives 2015, www)

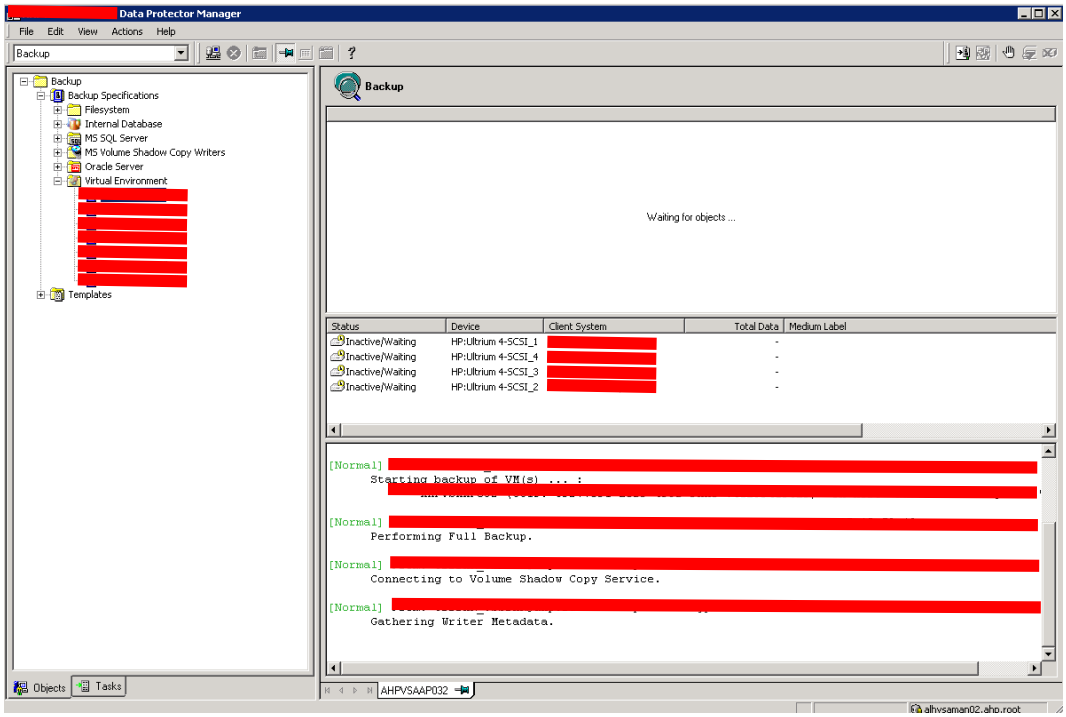
10 SHAREPOINT-VIRUSTORJUNTATESTAUS

10.1 Testaussuunnitelma

Ensiksi teemme varmistuksen työtä varten asennetusta testipalvelimesta. Tällöin voidaan aina palauttaa kaikki haluttuun pisteeseen, jos jotakin menee vikaan.

Sen jälkeen asennamme kummankin virustorjuntasovelluksen vuorollaan samalle palvelimelle ja perehdymme käyttöliittymään sekä peruskonfigurointiin ja ominaisuuksiin. Valituksi tuleva sovellus koekäytetään vielä tuotantoa mallintavassa testiympäristössä. Tällä tavalla saadaan suuri dokumenttimäärä sovelluksen tarkistettavaksi. Kyseiset dokumentit ovat kopio tuotannosta, joten periaatteessa saastuneita tiedostoja voi löytyä jo nyt, jos niin on päässyt käymään.

Tietoturvasta johtuen emme voi dokumentoida palvelimien hallintaa yksityiskohtaisesti.



Kuvio 5 Palvelimen varmistus

Varmistusten hallintaan käytetään HP Data Protection Manager sovellusta.

10.2 Testiympäristö

SharePoint-palvelimia on yhteensä 8 kpl. 4 niistä on testipalvelimia ja 4 on tuotantopalvelimia.

Ympäristöt ovat pyritty toteuttamaan pääosin virtuaalisesti.

Virtualisoinnilla saadaan yksi taso lisää laitteiston ja käyttöjärjestelmän väliin. Skaalautuvuus ja päivitettävyys paranee huomattavasti ilman että virtuaalipalvelmien käyttöjärjestelmät vaatisivat muutoksia tai päivityksiä. Virtuaalisten palvelimien etu on myös se, että niiden fyysisiä resursseja voidaan jakaa helposti käytön mukaan, eikä niille tarvita erillisiä omia laitteistoja.

Virtualisointi parantaa ylläpitoa monella tavalla:

- Virtuaalipalvelimia voidaan siirrellä alustapalvelimille
- Uusia virtuaalipalvelimia on helppo pystyttää
- Yksinkertaisemmat varmuuskopiot
- Kapasiteetin kasvattaminen.

SharePoint on mahdollista asentaa seuraaville virtualisointialustoille ja näistä uudemmille:

- Windows palvelin 2008 ja Hyper-V
- Microsoft Hyper-V palvelin 2008
- Server Virtualization Validation Program (SVVP) sertifioima virtuaalialusta, kuten VMWare.

Yksi hyvä huomio on virtuaalipalvelinten suurempi tehon tarve verrattuna fyysiseen palvelimeen, jotta suorituskyky olisi sama. Tehoa tarvitaan noin 20 prosenttia enemmän.

Testiympäristö on täysin samanlainen kuin tuotanto. Ainoa ero testi- ja tuotantoympäristölle on, että testiympäristössä ei ole käyttäjiä. Virtuaalisilla testipalvelimilla mahdolliset vahingot ovat paljon helpommin korjattavissa ja palautettavissa toimintakuntoon.

Testiympäristössä tulee aina testata kaikki muutokset, jotta pystytään varmistamaan että SharePoint käyttäjille ei tule vahingossakaan mitään käyttökatkoksia. (Microsoft 2015d, www)

10.3 Symantec Protection for SharePoint Servers

10.3.1 Asennus ja testaus

Symatec virustorjunta asennettiin yhdelle testipalvelimelle, jossa pyöri pieni kokoinen SharePoint. Asennusohjeet Symatec-virustorjunnasta löytyy erilliseltä liitteeltä. Asennusvaiheita oli kaksi, konsolin asennus ja ”pesukoneen” eli Scan Enginen asennus. Pesukoneen asennuksen yhteydessä tarvittiin lisenssiä, joka saatiin ottamalla yhteyttä virustorjunnan toimittajaan. Lisenssin saamisen jälkeen skannauspesukone saatiin aktivoitua ja yhdistettyä hallintakonsoliin.

Periaatteessa pelkästään käyttöliittymään on siis mahdollista tutustua ilman lisenssin tuomia skannausmahdollisuuksia.

10.3.2 Testaus ja konfigurointi

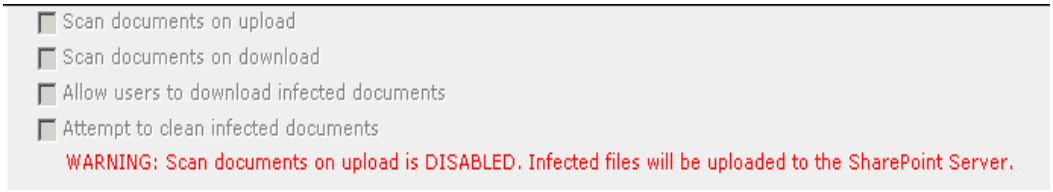
Tiedostot tarkistetaan sitä mukaa, kun niitä avataan tai tallennetaan. Tarkistus voidaan asettaa myös vain tallennettaessa tai avattaessa.

Tiedostotyypistä riippumatta kaikki tiedostot tarkistetaan, ellei näitä määritellä itse tarkemmin.

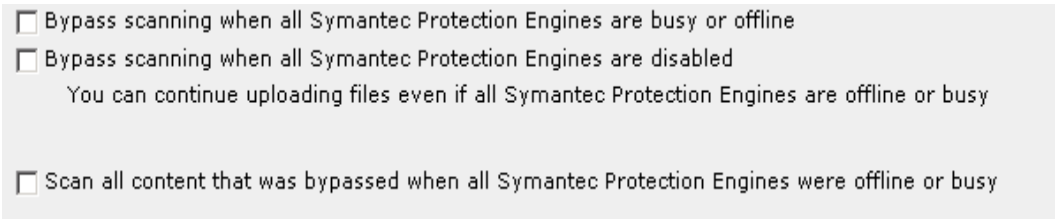
Jos skannaus epäonnistuu jostakin syystä reaaliaikaisen tarkistuksen aikana, tarkistus ja tiedoston lataus peruutetaan. Skannaus pyyntö lähtee uudestaan sitten kun käyttäjä yrittää ladata tai tallentaa tietoa uudestaan.

Kuviossa 4 seuraavat vaihtoehdot ovat määriteltävissä:

- Skannaa lähettäessä SharePointiin
- Skannaa ladattaessa/avatessa SharePointista
- Salli käyttäjien ladata saastuneita tiedostoja
- Yritä puhdistaa tartunnan saaneet tiedostot

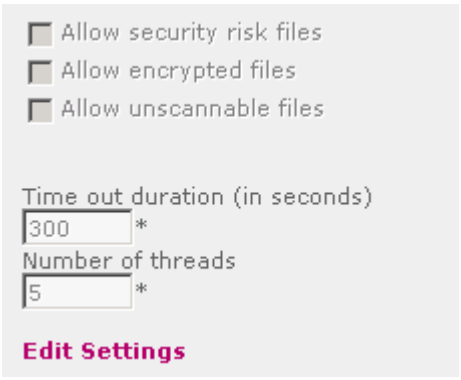


Kuvio 6 Symantec_conf 1



Kuvio 7 Symantec_conf 2

Kuviossa 6 skannaukset voidaan myös määritellä ohitettavaksi, jos pesukoneeseen tulee jokin häiriö. Tietoturvan kannalta tämä ei ole hyvä ratkaisu. Tällaista tilannetta varten olisi hyvä määritellä torjuntaohjelma niin, että kaikki skannaamatta jätetyt tiedot tarkistetaan sen jälkeen, kun pesukone on taas ylhäällä.



Kuvio 8 Symantec_conf 3

Kuviossa 7 voidaan määritellä resurssien käyttöä ja kuormitusta. Time out, eli aikakatkaisu on aika, jonka reaaliaikainen virustarkistus on päällä ennen prosessin lopettamista. Oletus on 5. minuuttia.

Laskentatehon kuormitusta voidaan säätää eräänlaisten virtuaalisten prosessorin ytimien (thread) määrällä.

Tuotantokäytössä käyttäjiä voi olla jopa satoja samassa SharePointissa. Tämän takia on tärkeää testata, kuinka paljon resursseja torjuntaohjelmisto vie. Testaamme lähinnä prosessorin ja muistin kulutuksen.

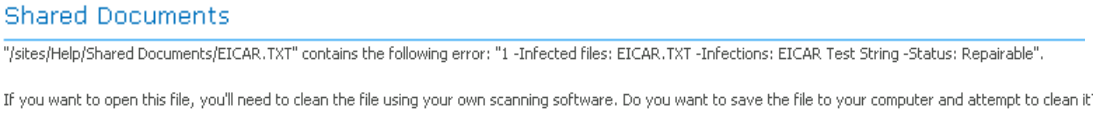
Symantec-virustorjuntapalveluita oli yhteensä kaksi ja konsolin pyöriminen ei vienyt paljon palvelimen tehoja. Testasimme manuaalisen SharePoint-virustarkistuksen, jonka yhteydessä prosessorin käyttö nousi hetkellisesti huomattavasti, jopa yli 50 %.

Kuvio 9 Prosessorin käyttö

Virustarkistuksen jälkeen virusta ei löytynyt, jonka jälkeen latasimme Microsoftin sivuilta EICAR-viruksen ja lisäsimme sen SharePointin. Kokeilimme sen jälkeen uudestaan ja 1 virus löytyi.

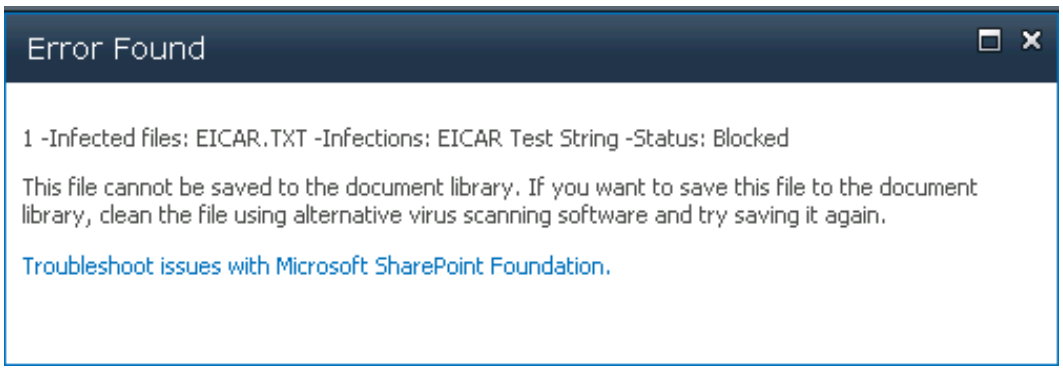
Kuvio 10 EICAR testi 1

Manuaalisen testauksen jälkeen siiryimme muuttamaan reaaliaikaisen tarkistuksen asetuksia. Reaaliaikaisista asetuksista otimme ensimmäisenä käyttöön tiedostojen tarkistuksen avataessa ja ladatessa palvelimeen, jonka seurauksena oli, että SharePointiin pystyi lisämään testivirustiedoston.



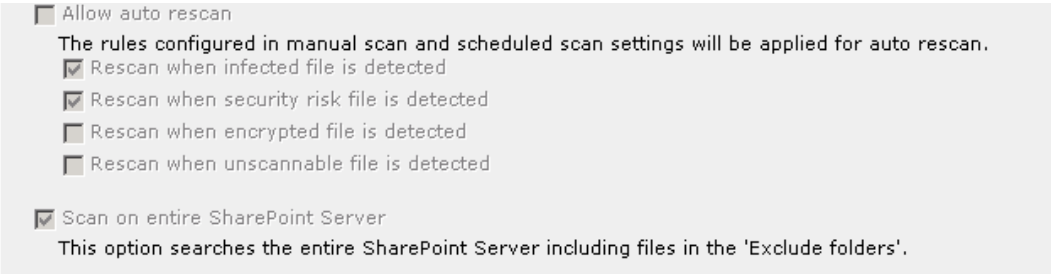
Kuvio 12 EICAR testi 2

Yrittäessä avata tiedostoa, tuli virheilmoitus että tiedosto on saastunut ja kyseistä tiedostoa ei saanut auki.



Kuvio 13 EICAR testi 3

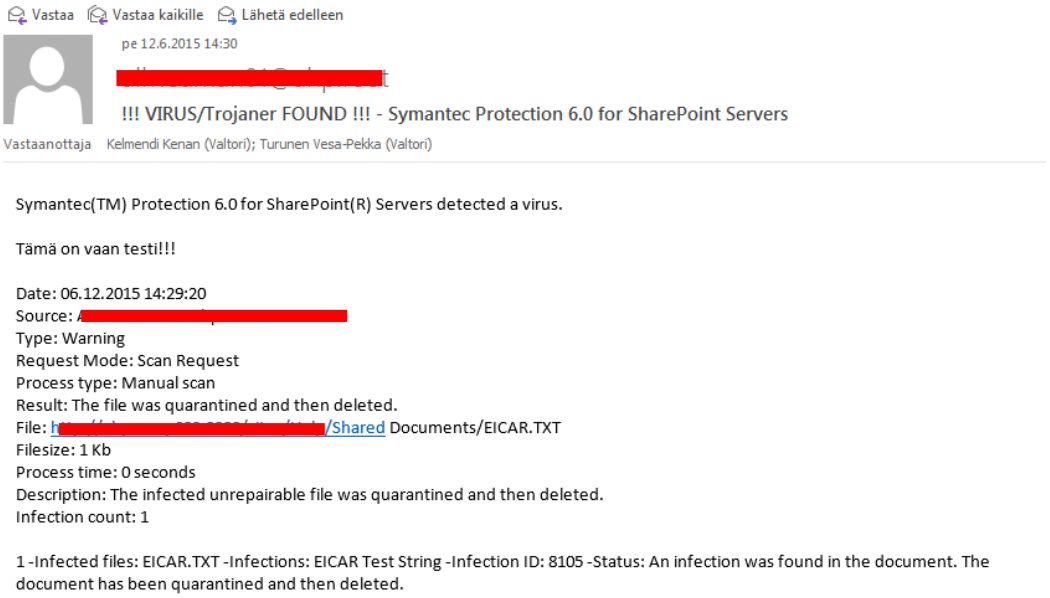
Otimme käyttöön reaaliaikaisen tarkistuksen asetuksista vielä tarkistuksen ladattaessa palvelimelle ja puhdista saastuneet tiedostot. Näillä asetuksilla SharePointin ei enää pystynyt lataamaan virustiedostoa.



Kuvio 14 Symantec_conf 4

Koko SharePoint palvelin voidaan määritellä tarkistettavaksi aina, jos tartunta havaitaan. Tällöin myös tarkistamisen ulkopuolelle jätetyt tiedostomuodot tarkistetaan. Tätä asetusta täytyy miettiä resurssien kannalta. Onko varaa laskea suorituskykyä ja tuotannon tehokkuutta tekemällä täydellinen tarkistus jokaisen tartunnan kohdalla, jos tartunta saadaan puhdistettua saman tien?

Tämä on myös mahdollista määritellä siten, että vain saman-nimiset tiedostot tarkistetaan koko palvelimelta.



Kuvio 15 Sähköposti-ilmoitus

Kun kaikki virustarkistusasiat olivat kunnossa, siirryimme testaamaan sähköpostihälytyksiä. Kyseinen toiminto saatiin yhdistettyä konesalin valvontajärjestelmään, joka valvoo koko konesalin toimintaa.

10.4 ESET Security for Microsoft SharePoint Server

10.4.1 Asennus ja testaus

Eset SharePoint-virustorjunta ohjelmistoon kuuluu koko palvelimen ja kaikkien tiedostojen suojaus. Täten SharePoint-torjuntaa testatessa ovat muut ominaisuudet pois päältä, eikä niihin nyt kiinnitetä huomiota.

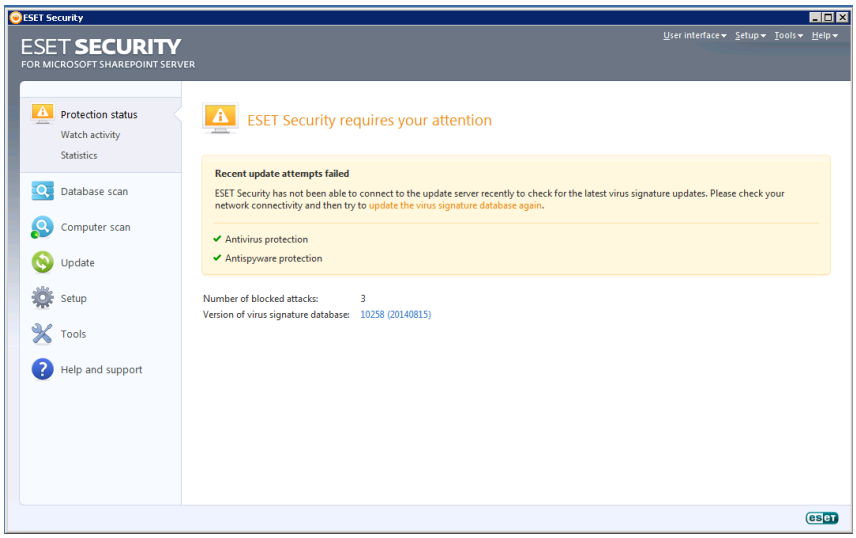
Tuote on rakennettu ESET File Security for Microsoft Windows Server-tuotteen pohjalle, mutta siihen on lisätty oma SharePointille omistettu komponentti.

Esetiin sisältyvät myös nämä toiminnot:

- ESET SysInspector analysoi koko järjestelmän riskien varalta.
- ESET SysRescue järjestelmän palautus, käyttöjärjestelmän palauttamista varten.

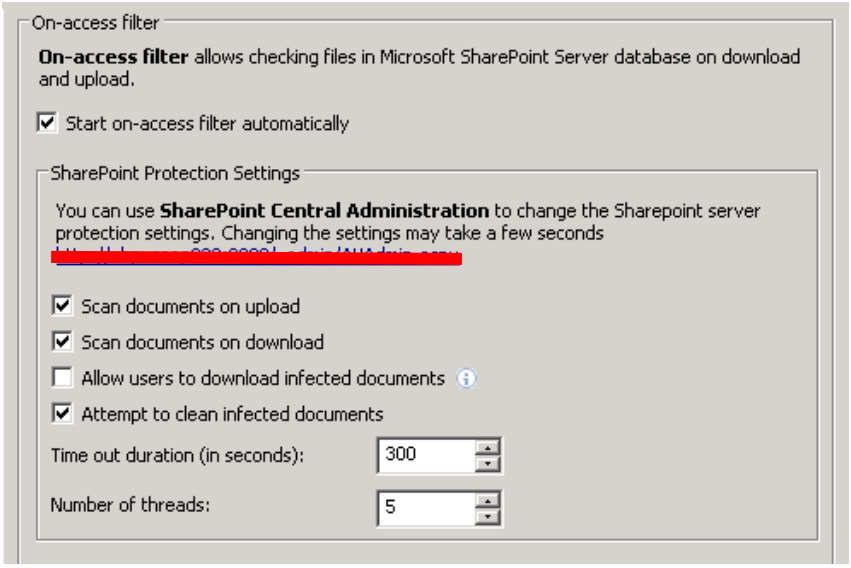
Kuten jo Symantecin kohdalla, myös Eset asennetaan samalle testipalvelimelle. Asennus oli yhtä yksinkertainen ja samankaltainen. Asennus on dokumentoitu liitteeksi.

Asennuksen jälkeen huomio kiinnittyi melko nopeasti siihen, että hallinnalle ei ole SharePointiin integroitua käyttöliittymää.



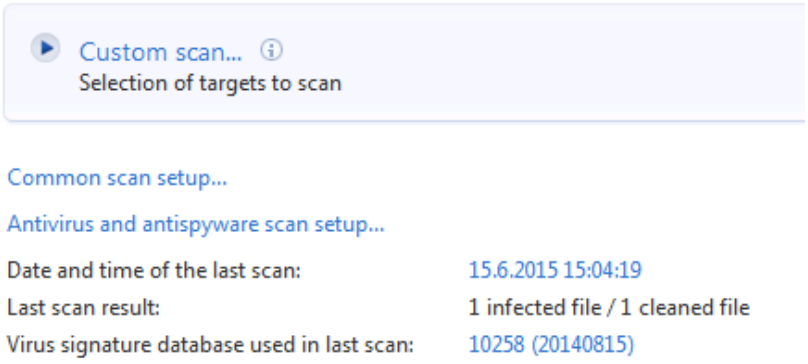
Kuvio 16 ESET

Kuviossa 15 on Esetin perusnäkymä omassa ikkunassaan ja kuviossa 16 skannausasetuksia. Alla olevan kuvan mukaiset asetukset voidaan määrittää myös SharePointin omasta hallintapaneelista, muuten Esetiä ei voi sieltä hallinnoida.



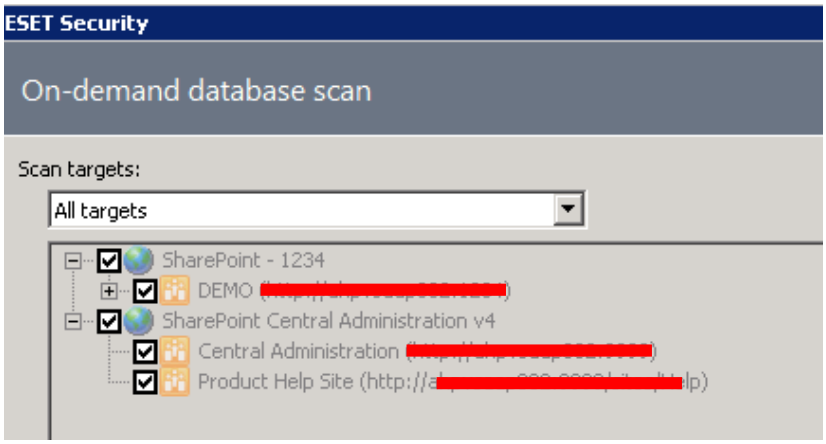
Kuvio 17 ESET Conf 1

10.4.2 Testaus ja konfigurointi



Kuvio 18 ESET scan

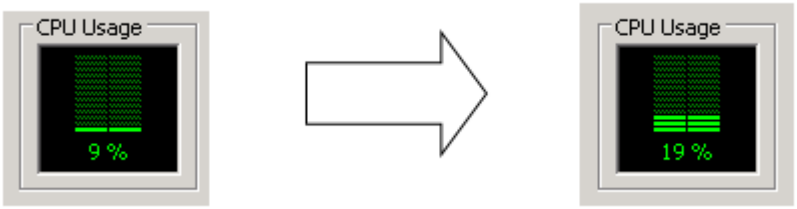
Ensimmäisenä ladattiin EICAR SharePoint DEMO-sivustolle ja ajettiin manuaalinen tarkistus. Tässä vaiheessa palvelimelle lataamisen tarkistaminen ei ollut päällä.



Kuvio 19 ESET Conf 2

Kuvio 20 ESET Virus havainto

Kokeilimme tälläkin tuotteella manuaalista tarkistusta, joka näytti toimivan, kuten odotettiinkin. Tarkistuskohteiksi valittiin kaikki SharePoint-sivustot. Tuotantokäytössä tätä ei ehkä kannata tehdä virastotyöaikana. Eicar-tiedostoa käyttämällä saatiin myös virushavainto testattua ja sovellus onnistui tämän puhdistamaan.



Kuvio 21 ESET CPU käyttö

Manuaalinen tarkistus ei nostanut juurikaan prosessorin käyttöä. Se nousi vain n. 20-prosentin tuntumaan, tämäkin vain hetkellisenä piikkinä.

10.5 Yhteenveto

Kumpikin virustorjunta toimii yhtä luotettavasti. Merkittävimpänä erona on käyttöliittymä, hallinta ja tuotteiden sisältämät ominaisuudet. Symantec on täysin integroitunut SharePointin hallintakäyttöliittymään ja tarjoaa vain SharePoint-virustorjunnan. Esetin hallinta tapahtuu erillisestä käyttöliittymästä ja ei ole aivan niin

helposti lähestyttävä kuin Symantec. Eset vaikuttaa aavistuksen kevyemmältä, kuten jo ennakkoon eri arvioinneista oli luettavissa. Toisaalta symantecilla voi kuormitusta jakaa asentamalla pesukoneet omille palvelimilleen.

Eset ei tarjoa vain SharePoint-virustorjuntaa vaan tuote on tavallinen virustorjunta lisättynä SharePoint torjuntamoduulilla. Tämä voi nousta kynnyskysymykseksi kun normaalia virustorjuntaa aletaan kilpailuttaa. On hyvin mahdollista että SharePoint virustorjunnan rinnalla on toisen valmistajan tavallinen virustorjunta. Muutenkin työn lähtökohtana on etsiä ohjelmisto vain SharePointille.

10.5.1 Valinta

Eri torjuntaohjelmistoja läpi käydessä tällä hetkellä parhaiten soveltuvaksi vaihtoehdoksi päätyi Symantec Protection for SharePoint. Symantec tarjoaa muun ohella tuotteen vain SharePointille.

Tuotteen kohdalla täytyy miettiä myös sitä, kuka tätä virustorjuntaa tulee hallinnoimaan ja ylläpitämään. Tästä johtuen Symantecin käyttöliittymästä SharePointin keskitetyssä hallintapaneelissa on selkeästi hyötyä. SharePointin ylläpitäjälle valikko ja virustorjunnan ylläpito ovat tutussa paikassa, ja keskitetysti muiden SharePoint toimintojen kanssa.

Muiden ohjelmistojen kohdalla tuotteeseen kuuluvat muutkin, kuin vain SharePoint virustorjunnat. Tämä on pakko ottaa huomioon, koska Valtorin tekemän kilpailutuksen tuloksena palvelimet ja työasemat tulevat saamaan jonkin virustorjunta ohjelmiston joka tapauksessa, joten turhasta ei luonnollisesti kannata maksaa.

Kilpailutuksessa vaatimuksena ei ole annettu SharePoint-torjuntaa, joten tuotteelle, joka suojaa vain sitä on selkeä tarve. On hyvin mahdollista että Valtion kilpailutuksen voittanut torjuntaohjelmisto ei sisälläkään suojaa SharePointille.

10.6 Symantec jatkotestaus

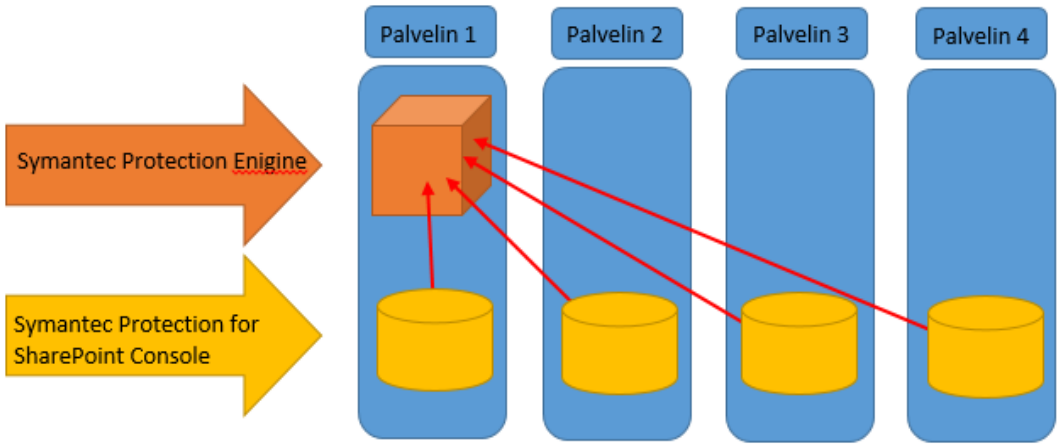
10.6.1 Tuotantoa vastaava testiympäristö

Tässä varsinaisessa ympäristössä on simuloitu tuotantoa ja myös materiaalimäärä on huomattavasti suurempi.

Symantec Protection 6.0 for SharePoint Servers virustorjunta-asennuspaketista voidaan asentaa kerralla tai erikseen Symantec Protection Engine ja hallintakonsoli.

Symantec Protection for SharePoint voidaan asentaa erillisesti eli standalone-asennus. Tällöin Console (=hallintakäyttöliittymä), pesukone ja SharePoint ovat samalla palvelimella. Pienissä ympäristöissä tämä voi olla järkevin ja yleinen ratkaisu.

Tässä tapauksessa on kuitenkin kyseessä usean SharePoint-palvelimen farmi. Käyttäjämäärä on myös suuri. Palvelinfarmille on mahdollista asentaa Scan engine aivan omalle palvelimelle, jossa ei ole mitään muuta. Tämä on hyödyllistä, koska tarkistettavat tiedostot lähetetään sinne ja myös tarkistuksesta johtuva kuormitus tapahtuu siellä.



Kuvio 22 Symantec asennussuunnitelma

Aiemman testauksen lisäksi kokeilemme varsinaisessa testiympäristössä Symatec Protection Enginen hallintaliittymän asentamista jokaiselle palvelimelle ja asennamme pesukoneen yhdelle palvelimelle.

Tämä saatiin toimimaan, mutta ilman pilottikäyttäjäryhmää emme saa selvillä vaikuttaako tämä nopeuteen ja käytettävyyteen merkittävästi. Tuotannosta kopioiduissa tiedostoissa ei ollut yhtäkään saastunutta tiedostoa, toisaalta koeversio on päivittämätön ja virustiedot eivät ole ajan tasalla.

Symantecin suosituksien mukaan Central Admin palvelimen web.config tiedosto kannattaa ottaa talteen ennen asennusta. (PC World 2015, www)

10.6.2 Päivitykset

Tutkimme myös kuinka päivitykset saadaan asennettua. Tähän ei koeversiossa ollut mahdollisuuksia kokeilla käytännössä. Myöskin tietoturvan kannalta palvelin tuskin tulee olemaan suoraan yhteydessä internetiin. Alla olevat määritykset kuitenkin tarvitaan teoriassa.

Seuraavat asetukset tulee olla määriteltynä päivitysten toimintaa varten. Symantec Live Update käyttää tiettyjä portteja ja protokollia.

LiveUpdate.exe täytyy päästää internetiin oikeista porteista ja tietyille toimialueille täytyy sallia pääsy palomuurista. LiveUpdate käyttää TCP porttia 80 (HTTP), 21 (FTP) ja 443 (HTTPS).

Tiedosto joka yhdistää internetiin on LuComServer_*_*.exe LiveUpdate 2.5:ssä ja uudemmissa versioissa. Oletussijainti on C:\Program Files\Symantec\LiveUpdate.

LiveUpdate käyttää http:tä yhdistääkseen osoitteisiin liveupdate.symanteclive-update.com, liveupdate.symantec.com, ja akamai.net. Jos LiveUpdate ei saa HTTP yhteyttä, LiveUpdate yhdistää FTP:llä update.symantec.com/opt/content/onramp sijaintiin. Symantecin LiveUpdate palvelimilla ei ole kiinteitä ip-osoitteita, joten staattisia ip-määrityksiä ei kannata tehdä, koska se voi aiheuttaa päivitysten epäonnistumisen.

11 HANKINNAT

Tämän työn lopputuloksena on tarkoitus esittää, että Valtori hankkisi erillisen SharePoint-virustorjunta ohjelmiston. Tämä ei kuitenkaan ole täysin suoraviivaista vaan hankinnoilla on omat säädökset ja lait. Hankinnat ovat yleensä julkisia ja kilpailutettavia.

Valtori käyttää hankinnoissaan valtion omistaman Hansel Oy:n palveluja puitejärjestelynä. Tämä tarkoittaa sitä, että Hansel Oy tuottaa Valtorille palvelun jossa se hoitaa kilpailutuksen, sopimukset ja yms. Tämä säästää paljon resursseja ja kuluja, kun Valtorin asiakkaana ei tarvitse kuin tietää mitä hankintoja tarvitaan tehdä.

” Yhtiön tehtävänä on hankkia muille hankintayksiköille tavaroita ja palveluja sekä tehdä tavaroita ja palveluja koskevia hankintasopimuksia ja puitejärjestelyjä. Yhtiö ylläpitää yhteishankintoina kilpailutettuja sopimuksia. Lisäksi yhtiön tehtävänä on tuottaa asiakkailleen hankintatoimeen liittyviä asiantuntija- ja kehittämispalveluja.” (Finlex 2015, www)

Suorahankintoja voidaan tehdä, jos niille on hyvät ja painavat perusteet. Tällöin hankinnan arvo täytyy myös olla alhainen. Arvo määritellään virastokohtaisesti.

Valtorille suorahankintaperusteita pienhankinnoille on määritelty seuraavasti.

Pienhankinta (tuote tai palvelu) voidaan toteuttaa suorahankintana ilman tarjouskilpailua seuraavissa tilanteissa:

- Arvo on alle 10 000 € (ns. vähäinen hankinta-arvo)
- kilpailuttamisesta johtuvat kulut ylittävät hyödyt
- yllättävä kiire, joka on Valtorista riippumaton
- hintataso on entuudestaan selvillä ja samanlaisia hankintoja on tehty aiemmin
- vain yksi potentiaalinen toimittaja tiedossa

Käytännössä myös nämä hankinnat voi toteuttaa hyödyntämällä Hansel Oy:n tai vastaavan puitejärjestelyn kautta.

Kuvio 23 Hankintakaavio

Kuviossa 20 on esimerkki kuinka suorahankinta voidaan toteuttaa. Tarjoajien valinnan sijasta myös haluttu tarjoaja voi olla ennalta päätetty.

Hankinnat aloitetaan ja toteutetaan Valtorin sisäisen Hankinnat-tulosyksikön kautta.

Mielestämme SharePoint-virustorjunta voidaan toteuttaa suorahankintana, koska toimittajia on lopulta varsin vähän sekä useiden toimittajien yhteensopivuus uusien SharePoint-tuotteiden kanssa vaikutti olevan vielä kyseenalainen.

Varsinainen virustorjunta on myös kilpailutettu jo, mutta vaatimuksena ei ole ollut SharePoint-virustorjuntaominaisuus. Jos kilpailutuksen tuloksena hankittu ohjelmisto ei sisällä tätä ominaisuutta, ei ole kannattavaa hankkia toista kokonaista virustorjuntaohjelmistoa tätä varten. Sen sijaan on järkevämpää hankkia toimittaja joka tarjoaa vain tähän tarkoitukseen soveltuvan tuotteen ja joka integroituu täysin SharePoint-ympäristöön. Suorahankintana pelkkä SharePoint-torjunta on varsin pieni hankinta.

Hankinnat itsessään olisivat helposti jo oman työn vaativa aihe, joten Hankintaprosessi käydään läpi vain pintapuolisesti. (Valtiovarainministeriö 2015, www)

12 LISENSSI

Symantec SharePoint-virustorjunnan lisenssien hankinnassa on otettava huomioon joitakin asioita.

1. Käyttäjäkohtainen lisenssi sisäiseen käyttöön, eli Valtori

   Sisäiseen käyttöön hankittuna yritysten on hankittava lisenssi jokaista käyttäjää varten, jolla on pääsy SharePointiin.

2. Palvelinkohtainen lisenssi ulkopuoliseen käyttöön, eli asiakkaat ja muut ulkopuoliset käyttäjät.

   SharePoint-ympäristön ulkoisessa käytössä täytyy hankkia palvelinkohtainen lisenssi. Käyttäjämäärällä ei ole väliä.

Käytön ollessa kummankin ylläkuvatun kaltaista, täytyy kumpaakin käyttöä varten hankkia omanlaisensa lisenssit.

Lisenssi sisältää yleensä peruskäyttötuen, johon sisältyy puhelinneuvontaa 1 vuodenajan. Vasteaika 1 tunti ja saatavuus 10 tuntia päivässä klo 08.00 - 18.00 maanantaista perjantaihin

Ohjelmiston päivitykset ovat saatavilla yhden vuoden ajan, saatavuus 24 tuntia päivässä maanantaista sunnuntaihin. (Symantec 2015, www)

13 KUSTANNUSARVIO

Kustannukset riippuvat toimittajasta ja joistakin optioista mitä lisenssin hankinnan aikana voidaan sopia. Esimerkiksi valtioille on oma ”Band S” taso jolla hinnoittelu on hieman eri.

Käyttäjäkohtaisen lisenssin hinta on noin viiden ja kymmenen euron välillä vuodessa ja palvelinkohtaisen lisenssin hinta on noin 1700-3000 euroa vuodessa.

Eräs säästömahdollisuus on että luotetaan omiin työasemiin eikä hankita virustorjuntaa Valtorin sisäiseen käyttöön, mutta vain asiakkaille ja ulkopuolisille.

14 YHTEENVETO

Työn aloittamisen ja rajaamisen jälkeen onnistumisena voi pitää jo sitä, että löysimme tämän tietoturva-aukon, jonka tuomiin kysymyksiin tämä työ vastaa.

Ison organisaation tietoturva on erittäin suuri kokonaisuus, joka muodostuu monesta osasta. Tästä tuli paljon tietoa ja opittua uusia asioita. SharePoint virustorjunnan puuttuminen ei välttämättä heti kaada maailmaa, mutta on kuitenkin yksi osa jolla kokonaisturvallisuus rakennetaan.

Työ oli aluksi erittäin laaja ja käsitti myös sql-palvelimen virustorjuntaa ja työasemien virustorjuntaa ja hallinnointia. Melko pian aloittamisen jälkeen ja ensimmäisten palaverien jälkeen oli parempi rajata työtä huomattavasti ja keskittyä olennaiseen.

Alkuperäinen suunnitelma oli kartoittaa tavallisiakin virustorjuntoja mutta näistä tehtiin kilpailutus ja aihe olisi muutenkin mennyt liian laajaksi. Tämä kilpailutus myös herätti kysymyksiä siitä, onko SharePoint virustorjuntaa otettu siinä huomioon ollenkaan ja voiko se vaikuttaa tähän työhön millään tavalla.

SharePointin ylläpito ja SharePoint-ympäristö oli myös varsin tuntematonta aluetta ja jouduimmekin perehtymään näihin asioihin paljon, jotta voisimme ottaa huomioon mitä kaikkea SharePoint ympäristön ylläpitoon kuuluu jo ennestään ja tuoko virustorjunnan hankinta kuinka paljon lisätyötä.

Myös materiaalin puute oli yksi haaste. Tämä selittyy osittain sillä että SharePoint-virustorjunta on kuitenkin varsin uusia asia ja jopa suhteellisen harvassa paikassa käytössä.

Hankinnoista ei myöskään ollut juurikaan käytännön kokemusta joten niihin perehtyminen vei oman aikansa.

Tätä työtä päättäessä emme ole löytäneet muita yhtä kattavia teoksia SharePoint virustorjunnasta suomenkielellä.

LÄHTEET

Valtori, 2015. Tietoa Valtion tieto- ja viestintätekniikkakeskus Valtorista. Viitattu 10.11.2015. Saatavilla www-muodossa: http://www.valtori.fi/fi-FI/Tietoa_Valtorista

PremierPoint Solutions, 2015. What is SharePoint? Viitattu 10.11.2015. Saatavilla www-muodossa: https://premierpointsolutionstraining.wordpress.com/2013/10/24/what-is-SharePoint-introduction/

Microsoft, 2015a. Mikä on SharePoint? Viitattu 10.11.2015. Saatavilla www-muodossa: https://support.office.com/fi-fi/article/Mik%C3%A4-on-SharePoint-97b915e6-651b-43b2-827d-fb25777f446f

SPTechCon, 2015. SharePoint and antivirus protection. Viitattu 10.11.2015. Saatavilla www-muodossa: http://www.sptechcon.com/news/SharePoint-and-antivirus-protection

Taylor - SharePoint & more, 2015. Antivirus for SharePoint 2013. Viitattu 10.11.2015. Saatavilla www-muodossa: http://www.jeremytaylor.net/2015/02/03/antivirus-SharePoint-2013/

Microsoft, 2015b. Overview: Virus Scan Engine API Implementation. Viitattu 10.11.2015. Saatavilla www-muodossa: https://msdn.microsoft.com/en-us/library/office/aa979518%28v=office.14%29.aspx

Microsoft, 2015c. Overview of the Windows SharePoint Services Virus Scan Engine API. Viitattu 10.11.2015. Saatavilla www-muodossa: https://msdn.microsoft.com/en-us/library/dd586612%28v=office.11%29.aspx

Virus bulletin, 2015. The International Publication on Computer Virus Prevention, Recognition and Removal. Viitattu 10.11.2015. Saatavilla www-muodossa: https://www.virusbtn.com/pdf/magazine/2003/200306.pdf

AV Comparatives, 2015. Business security reviews. Viitattu 10.11.2015. Saatavilla www-muodossa: http://www.av-comparatives.org/corporate-reviews/

Microsoft, 2015d. Plan for administrative and service accounts in SharePoint 2013. Viitattu 10.11.2015. Saatavilla www-muodossa: https://technet.microsoft.com/en-us/library/cc263445.aspx

PC World, 2015. How We Test Antivirus Software and Security Suites. Viitattu 10.11.2015. Saatavilla www-muodossa: http://www.pcworld.com/article/248974/how_we_test_antivirus_software_and_security_suites.html

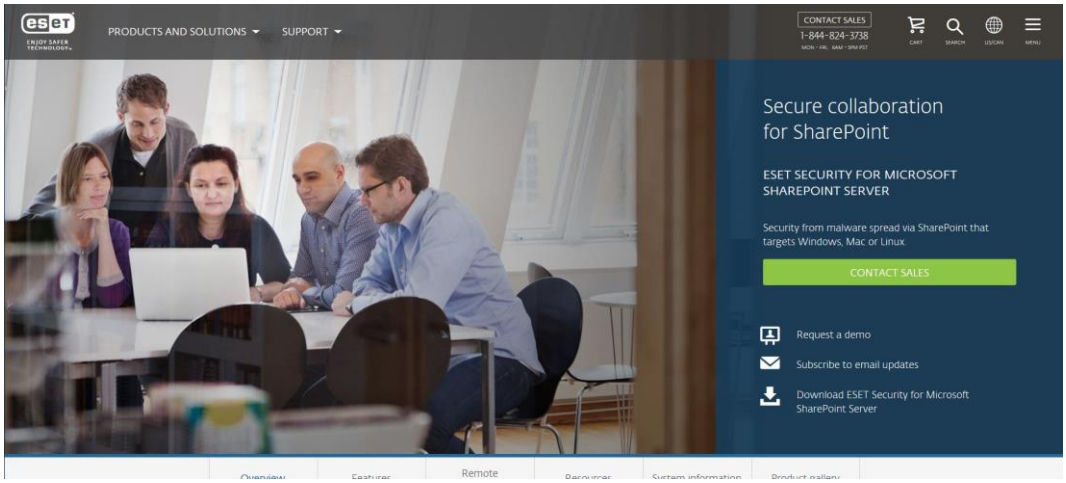
Finlex, 2015. Laki Hansel Oy -nimisestä osakeyhtiöstä. Viitattu 10.11.2015. Saatavilla www-muodossa: http://www.finlex.fi/fi/laki/alkup/2008/20081096

Valtiovarainministeriö, 2015. Valtion hankintakäsikirja. Viitattu 10.11.2015. Saatavilla www-muodossa: http://vm.fi/documents/10623/307565/Valtion+hankintak%C3%A4sikirja+2010/a02ceb72-d9c8-41e2-aed1-5de219b1c433

Symantec, 2015. Government Program. Viitattu 10.11.2015, Saatavilla www-muodossa: https://www.symantec.com/products-solutions/licensing/detail.jsp?detail_id=govern https://www.symantec.com/products-solutions/licensing/detail.jsp?detail_id=governmentment

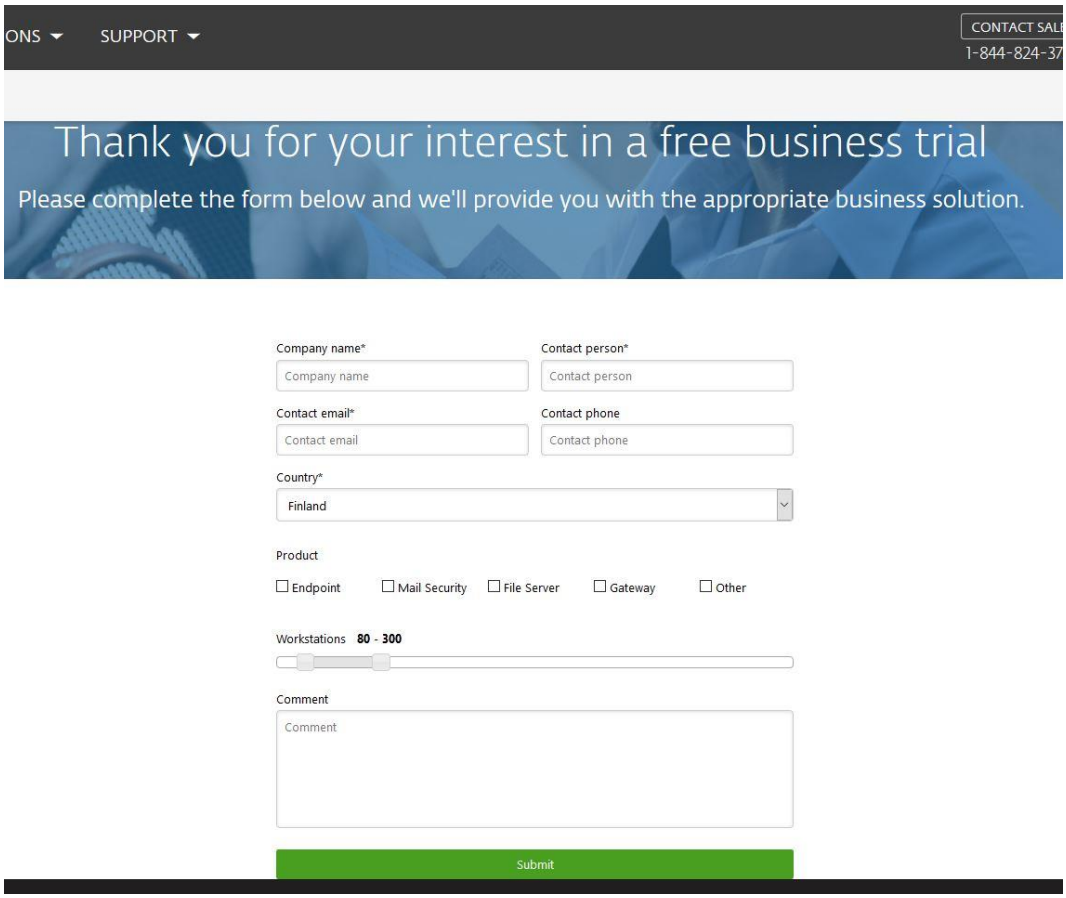
Wiki-Security, 2015. Computer Security. Viitattu 10.11.2015, Saatavilla www-muodossa: http://www.wiki-security.com/wiki/Computer_security/

ESET Security for Microsoft SharePoint Server Asennus

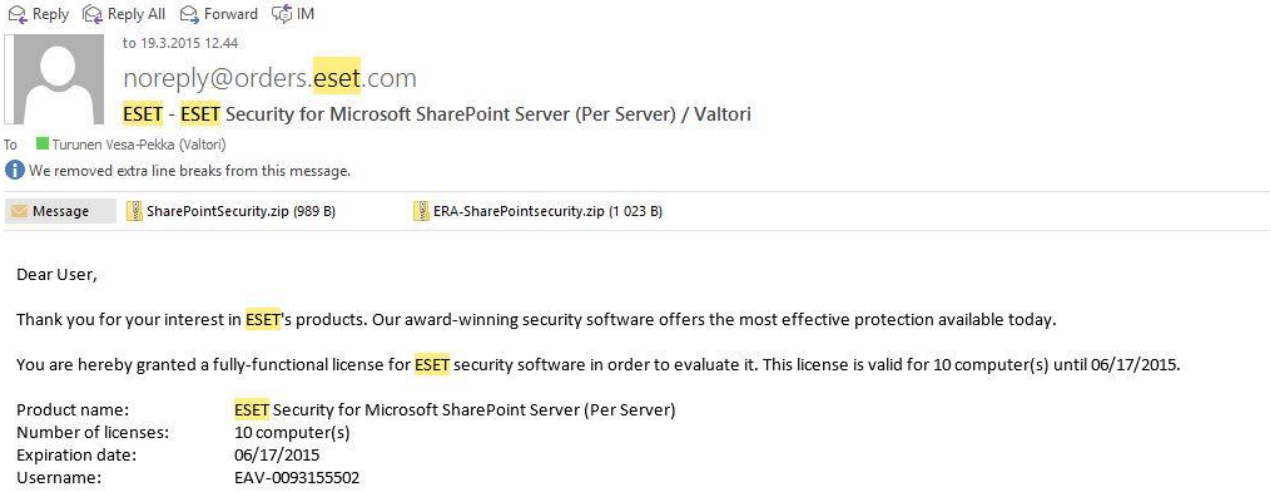


http://www.eset.com/us/products/SharePoint/

Tuotteen verkkosivuilta jätetään koekäyttöpyyntö.



Tietojen lähettämisen jälkeen Esetin edustaja ottaa yhteyttä. Muutaman viestin vaihdon ja peruskysymysten jälkeen lisenssi saapuu sähköpostiin.



Reply Reply All Forward IM

to 19.3.2015 12.44

noreply@orders.eset.com

ESET - ESET Security for Microsoft SharePoint Server (Per Server) / Valtori

To Turunen Vesa-Pekka (Valtori)

We removed extra line breaks from this message.

Message SharePointSecurity.zip (989 B) ERA-SharePointsecurity.zip (1 023 B)

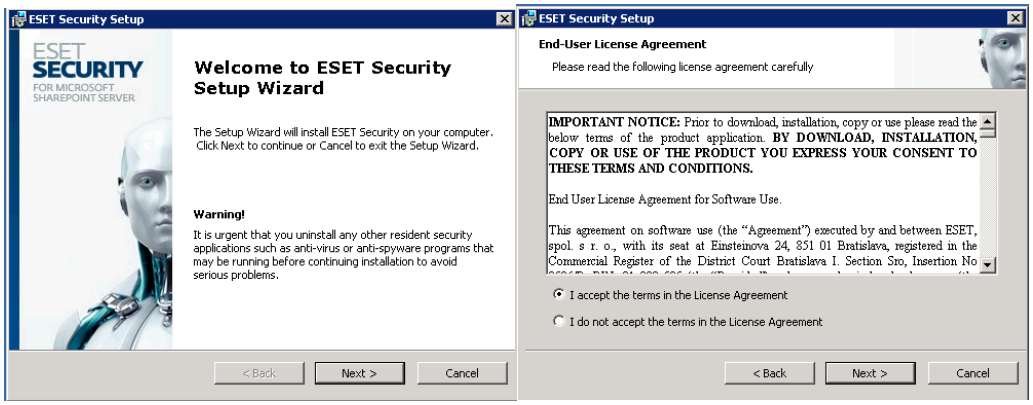
Dear User,

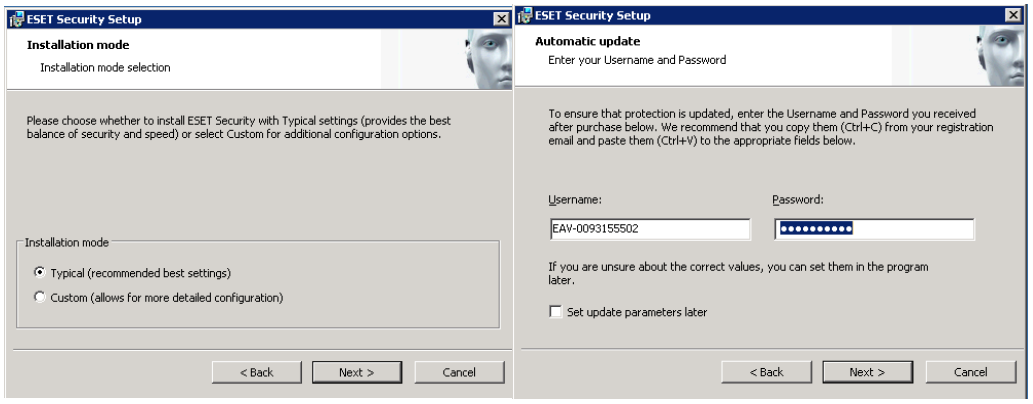
Thank you for your interest in ESET's products. Our award-winning security software offers the most effective protection available today.

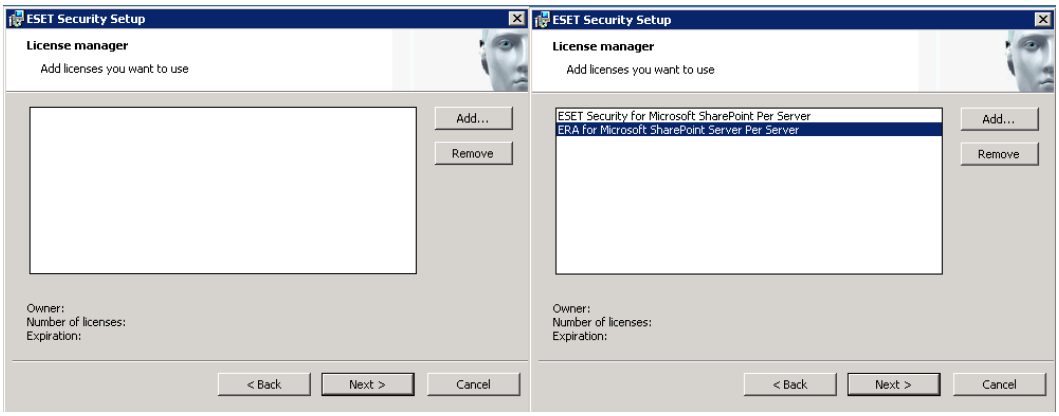
You are hereby granted a fully-functional license for ESET security software in order to evaluate it. This license is valid for 10 computer(s) until 06/17/2015.

Product name:	ESET Security for Microsoft SharePoint Server (Per Server)
Number of licenses:	10 computer(s)
Expiration date:	06/17/2015
Username:	EAV-0093155502

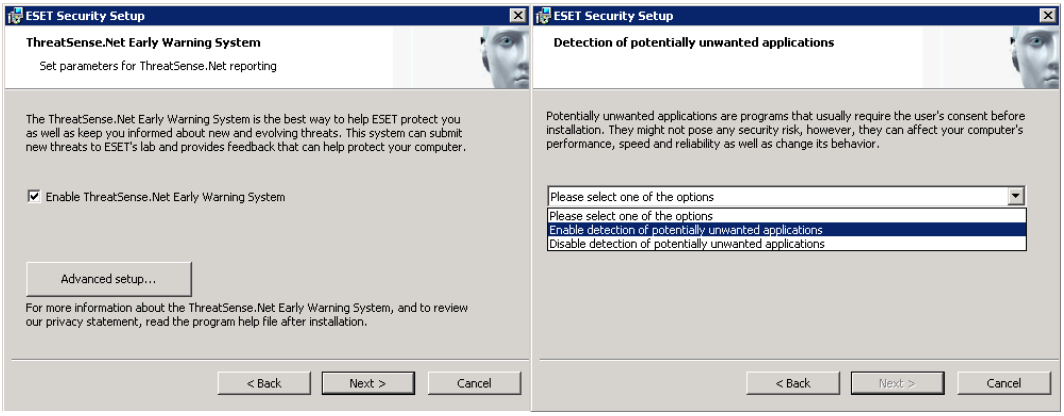
Tämän jälkeen ladataan asennuspaketti verkkosivulta ja aloitetaan asennus.

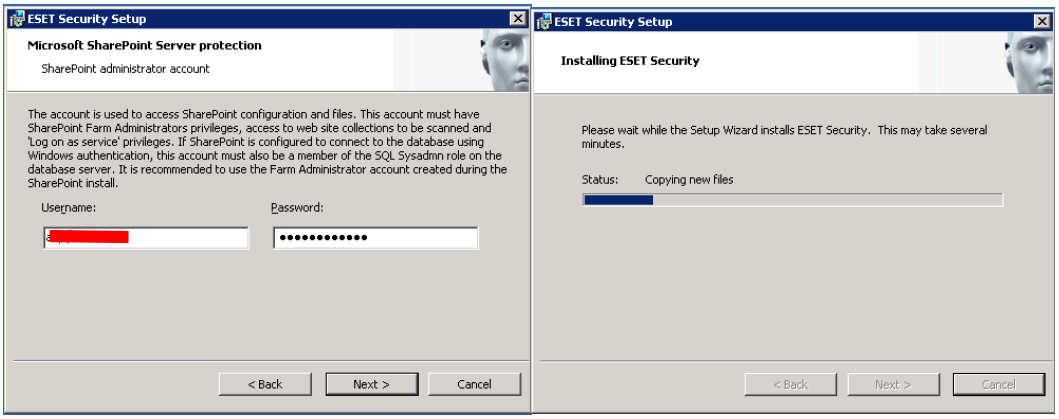






Käyttäjätunnus ja lisenssi saapuivat sähköpostissa. Lisenssi lisätään asennuksen yhteydessä.



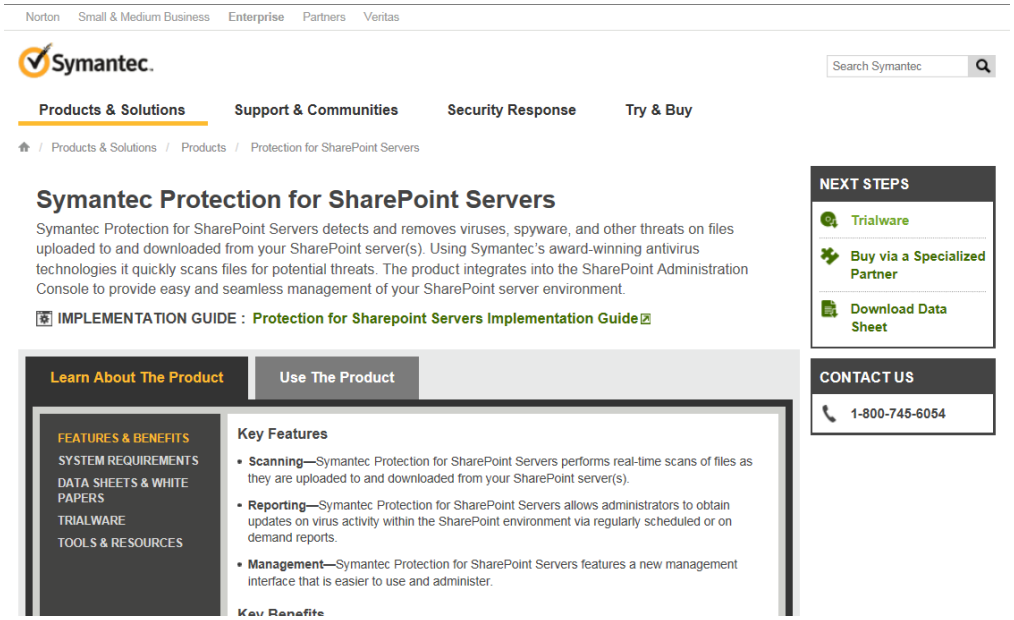


Asennus on valmis ja konfiguroinnin voi aloittaa.

Huom! Asennuksessa annettavalla SharePoint järjestelmänvalvojan tunnuksella täytyy olla oikeudet koko SharePoint farmiin, sivustoihin jotka halutaan suojata (site collections) ja ”log on as service” eli palveluna kirjautumiseen. On suositeltavaa käyttää siis farmin järjestelmänvalvoja tunnusta asennuksessa.

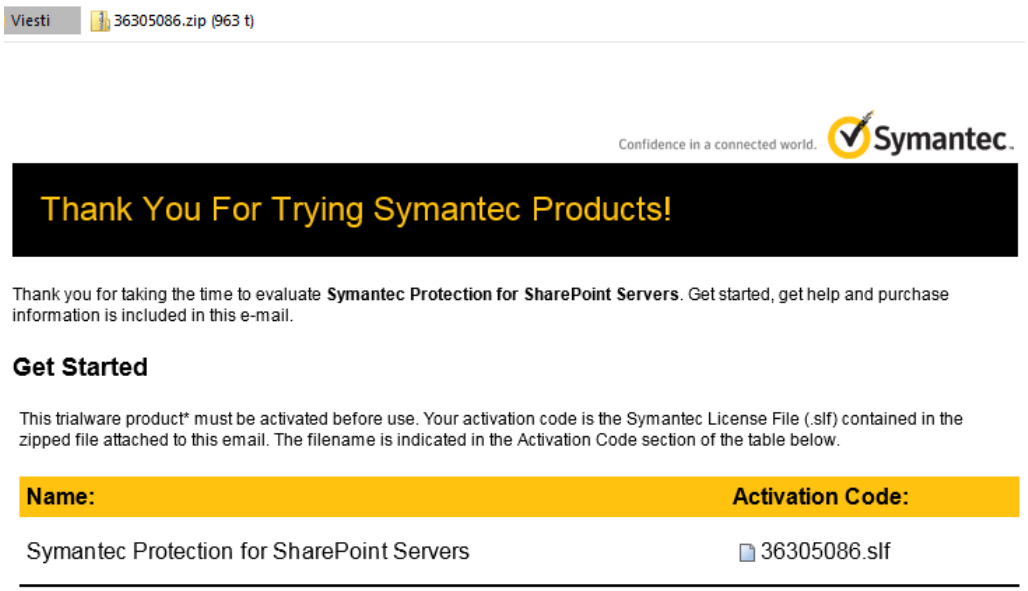
30-päivän koelisenssin saa uusittua melko joustavasti.

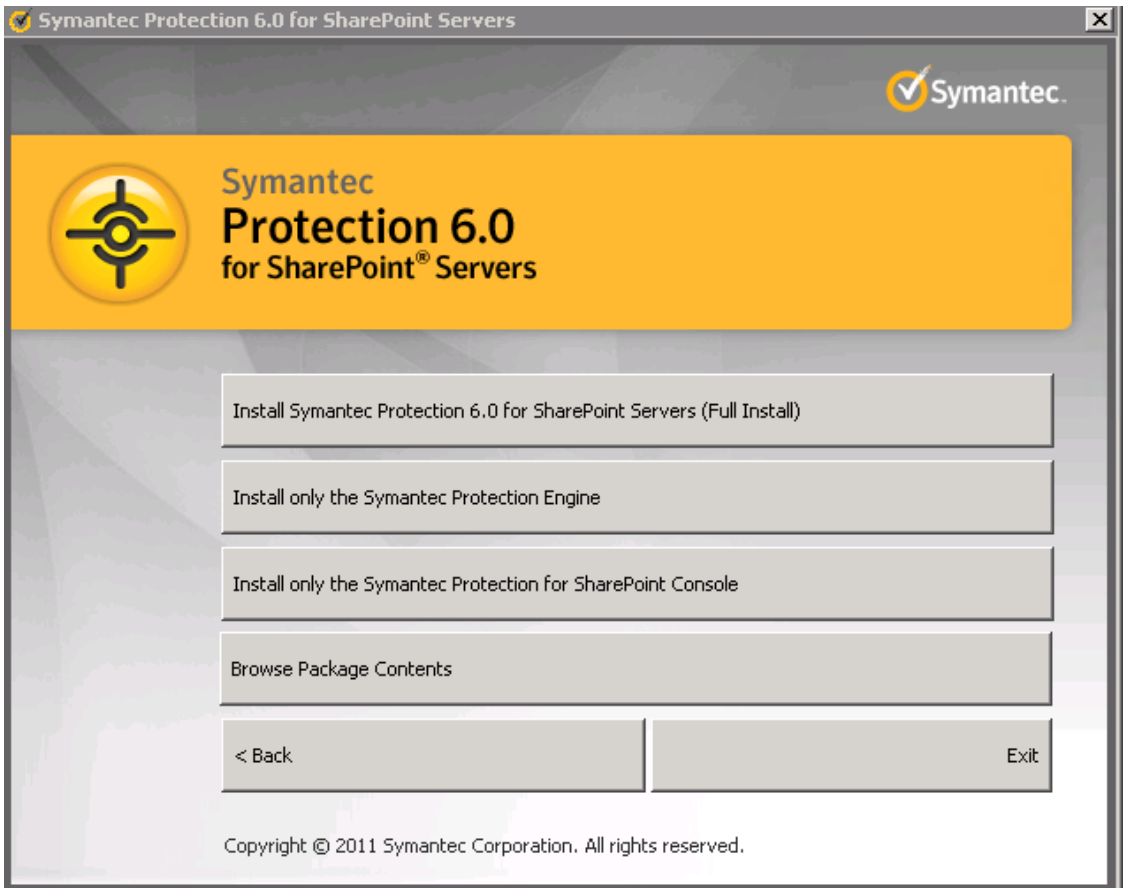
Symantec protection for SharePoint Asennus



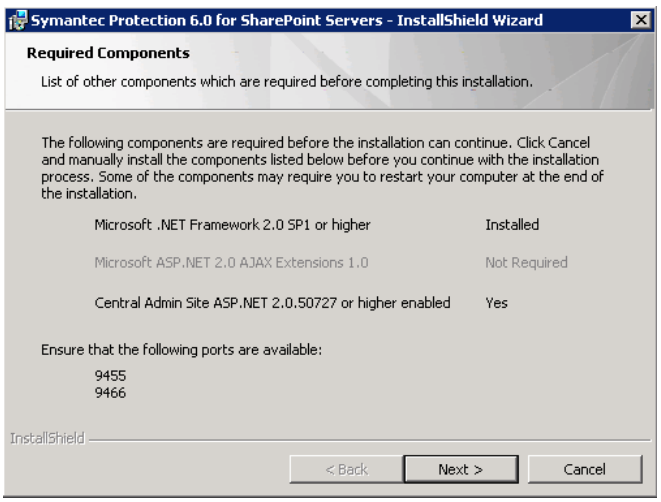
https://www.symantec.com/protection-for-SharePoint-servers/

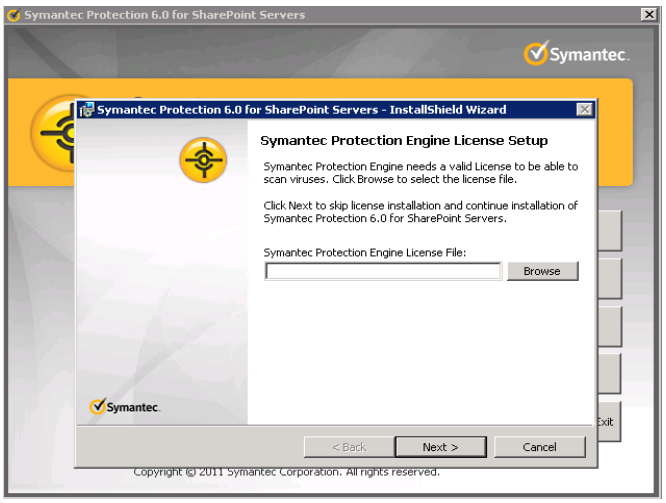
Tuotteen sivustolla täytyy rekisteröityä asiakkaaksi, jotta pääsee lataamaan asennuspaketin. Asennuspaketin lataamisen jälkeen sähköpostiin tulee koekäyttö lisenssi, joka on voimassa kuukauden. Symantecin myyntihenkilö ottaa yhteyttä rekisteröinnin jälkeen.

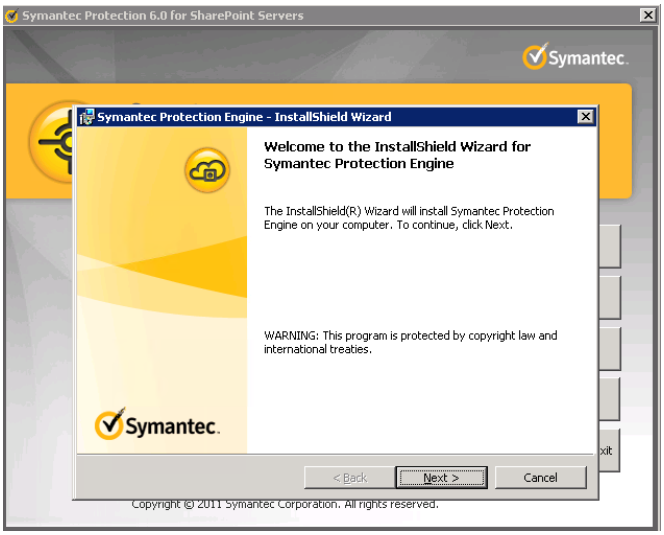


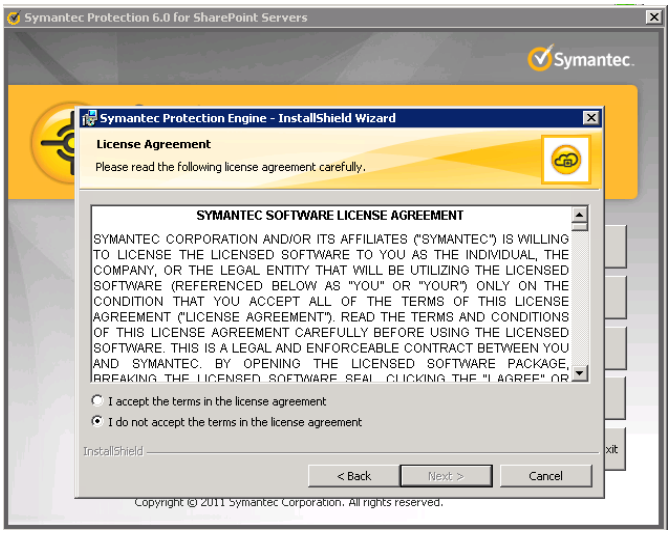


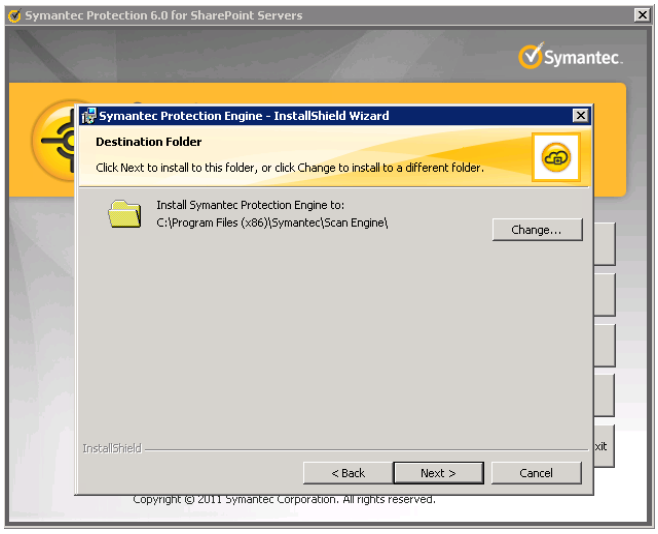
Koska palvelimia on 4, Symantec Protection for SharePoint hallintakonsoli asennetaan kaikkiin palvelimiin ja Symantec Protection Engine(pesukone) asennetaan vain yhdelle palvelimelle.

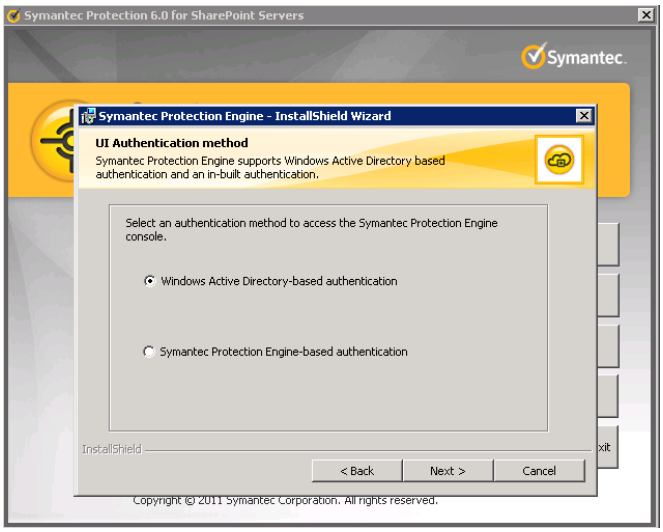


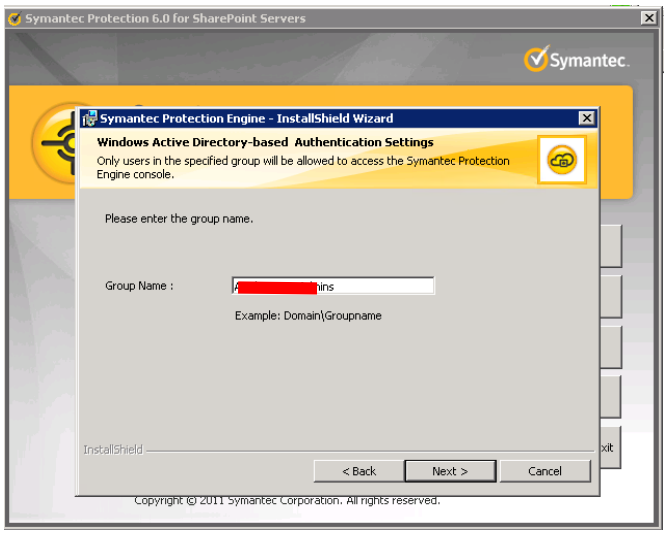


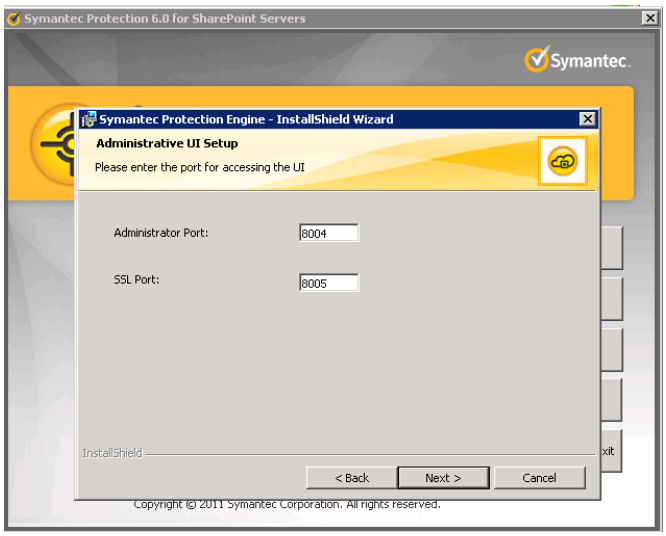

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
Welcome to the InstallShield Wizard for Symantec Protection Engine
The InstallShield(R) Wizard will install Symantec Protection Engine on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
Symantec.
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

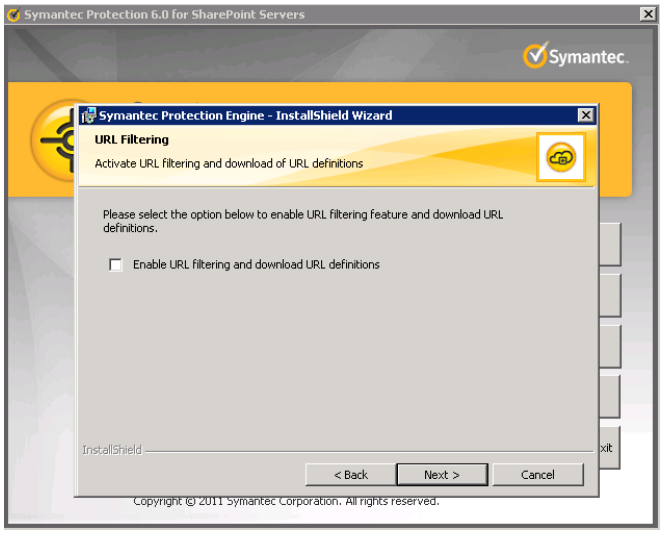

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THE LICENSED SOFTWARE PACKAGE,
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

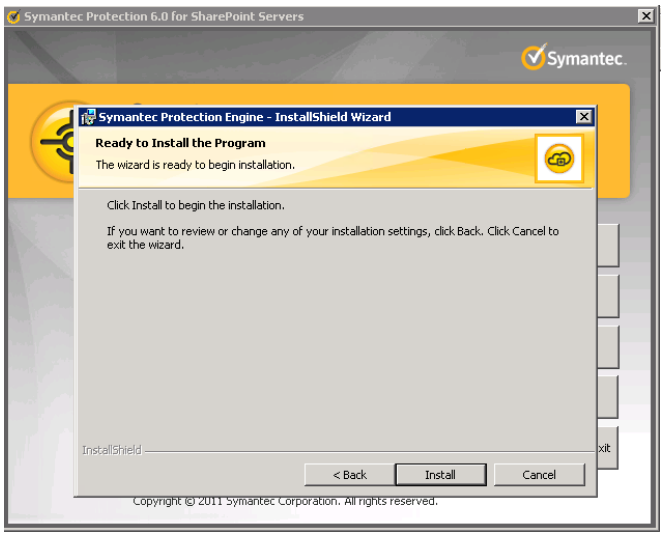

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Symantec Protection Engine to:
C:\Program Files (x86)\Symantec\Scan Engine\
Change...
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

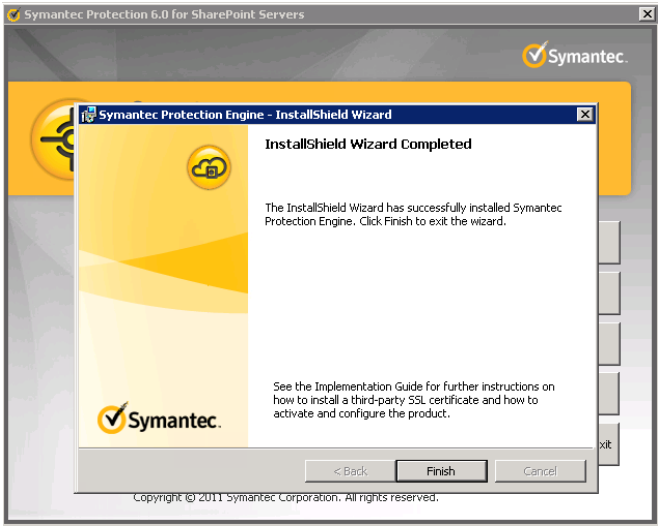

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
UI Authentication method
Symantec Protection Engine supports Windows Active Directory based authentication and an in-built authentication.
Select an authentication method to access the Symantec Protection Engine console.
Windows Active Directory-based authentication
Symantec Protection Engine-based authentication
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

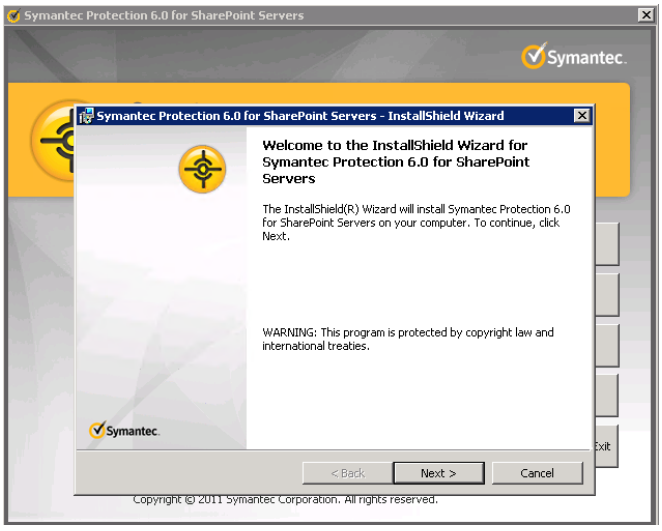

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
Windows Active Directory-based Authentication Settings
Only users in the specified group will be allowed to access the Symantec Protection Engine console.
Please enter the group name.
Group Name :
Example: Domain\Groupname
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

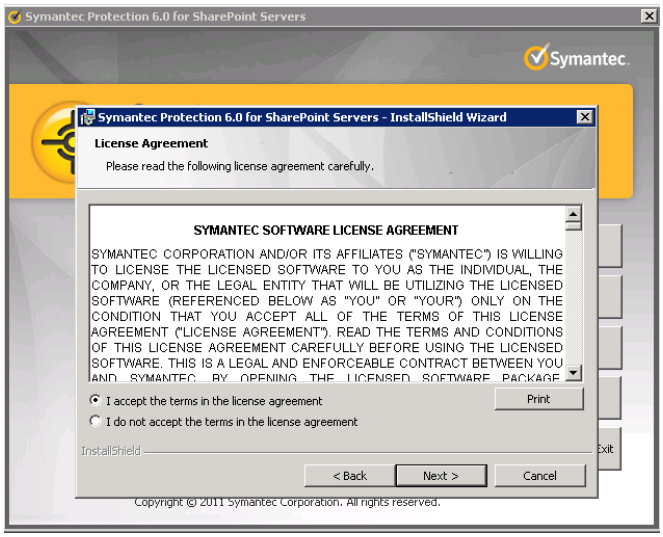

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
Administrative UI Setup
Please enter the port for accessing the UI
Administrator Port:
8004
SSL Port:
8005
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

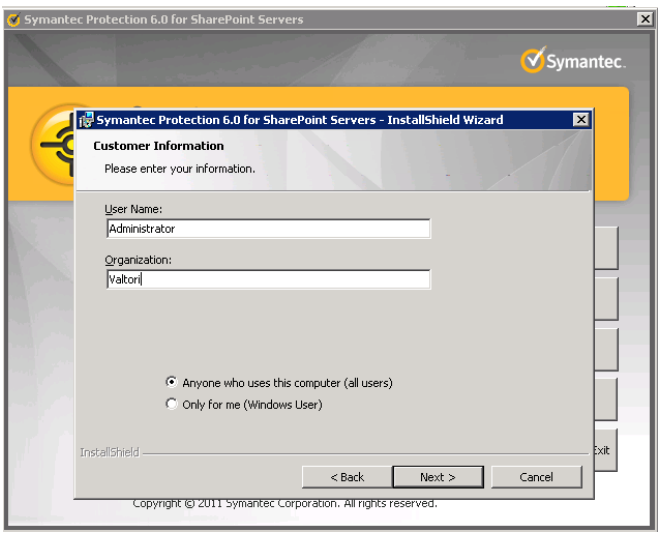

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
URL Filtering
Activate URL filtering and download of URL definitions
Please select the option below to enable URL filtering feature and download URL definitions.
Enable URL filtering and download URL definitions
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

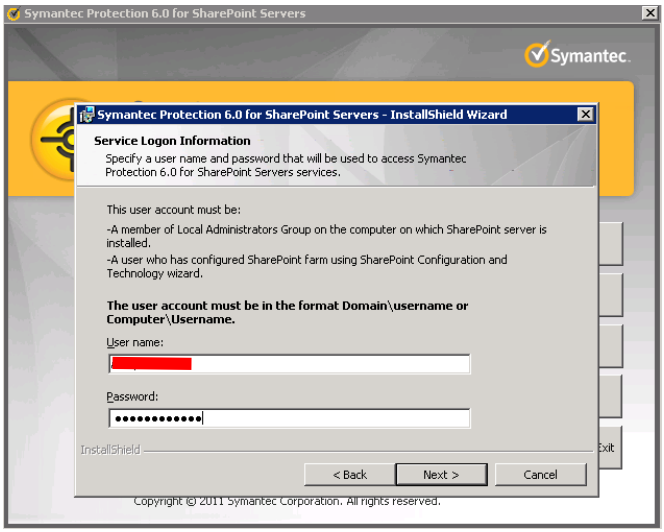

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

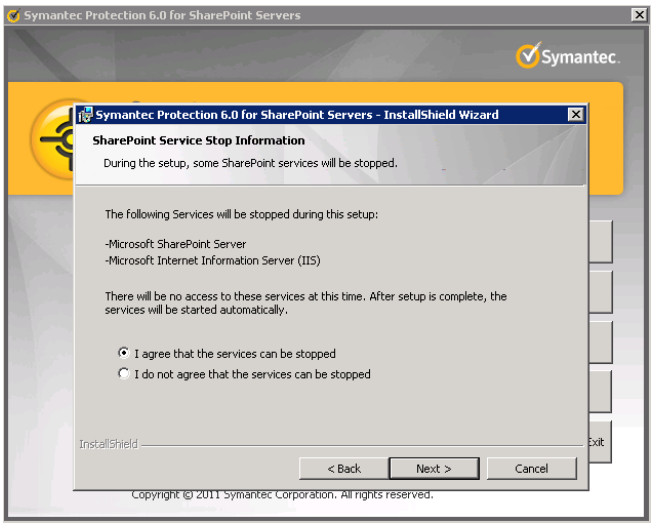

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection Engine - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Symantec Protection Engine. Click Finish to exit the wizard.
See the Implementation Guide for further instructions on how to install a third-party SSL certificate and how to activate and configure the product.
Symantec.
< Back
Finish
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

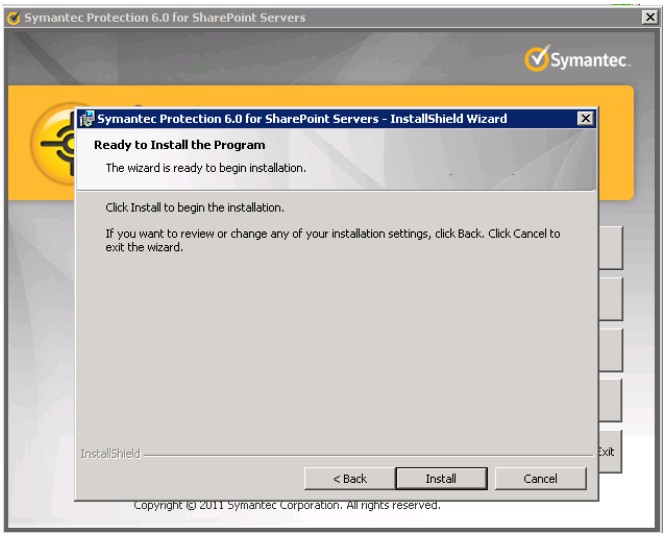

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
Welcome to the InstallShield Wizard for Symantec Protection 6.0 for SharePoint Servers
The InstallShield(R) Wizard will install Symantec Protection 6.0 for SharePoint Servers on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
Symantec.
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

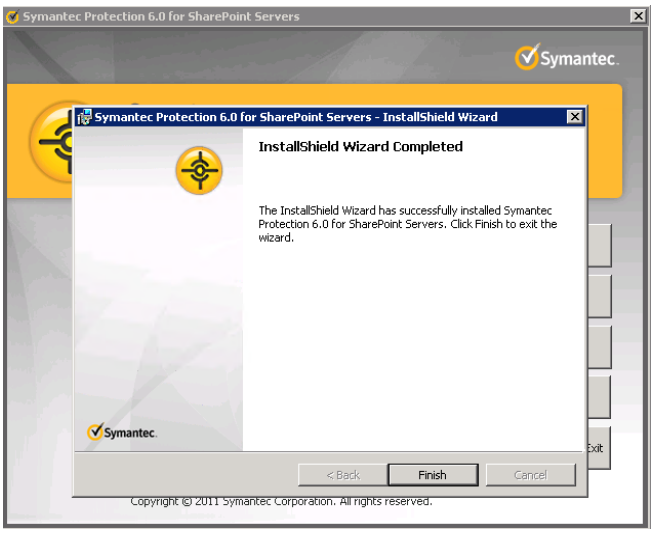

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
SYMANTEC SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THE LICENSED SOFTWARE PACKAGE
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.

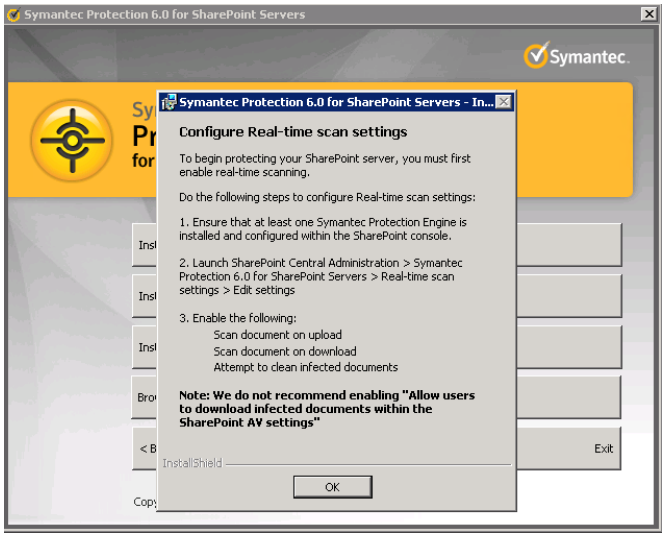

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
Customer Information
Please enter your information.
User Name:
Administrator
Organization:
Valtori
Anyone who uses this computer (all users)
Only for me (Windows User)
InstallShield
< Back
Next >
Cancel
Copyright © 2011 Symantec Corporation. All rights reserved.


Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
Service Logon Information
Specify a user name and password that will be used to access Symantec Protection 6.0 for SharePoint Servers services.
This user account must be:
-A member of Local Administrators Group on the computer on which SharePoint server is installed.
-A user who has configured SharePoint farm using SharePoint Configuration and Technology wizard.
The user account must be in the format Domain\username or Computer\Username.
User name:
Password:
InstallShield
< Back
Next >
Cancel
Exit
Copyright © 2011 Symantec Corporation. All rights reserved.

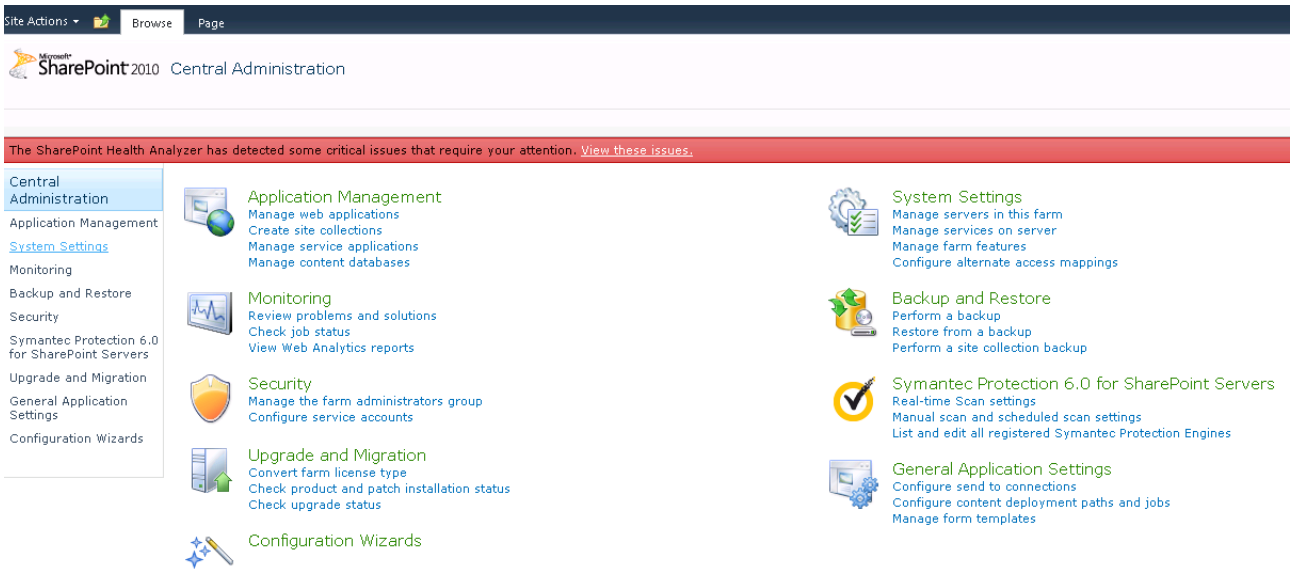

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
SharePoint Service Stop Information
During the setup, some SharePoint services will be stopped.
The following Services will be stopped during this setup:
-Microsoft SharePoint Server
-Microsoft Internet Information Server (IIS)
There will be no access to these services at this time. After setup is complete, the services will be started automatically.
I agree that the services can be stopped
I do not agree that the services can be stopped
InstallShield
< Back
Next >
Cancel
Exit
Copyright © 2011 Symantec Corporation. All rights reserved.

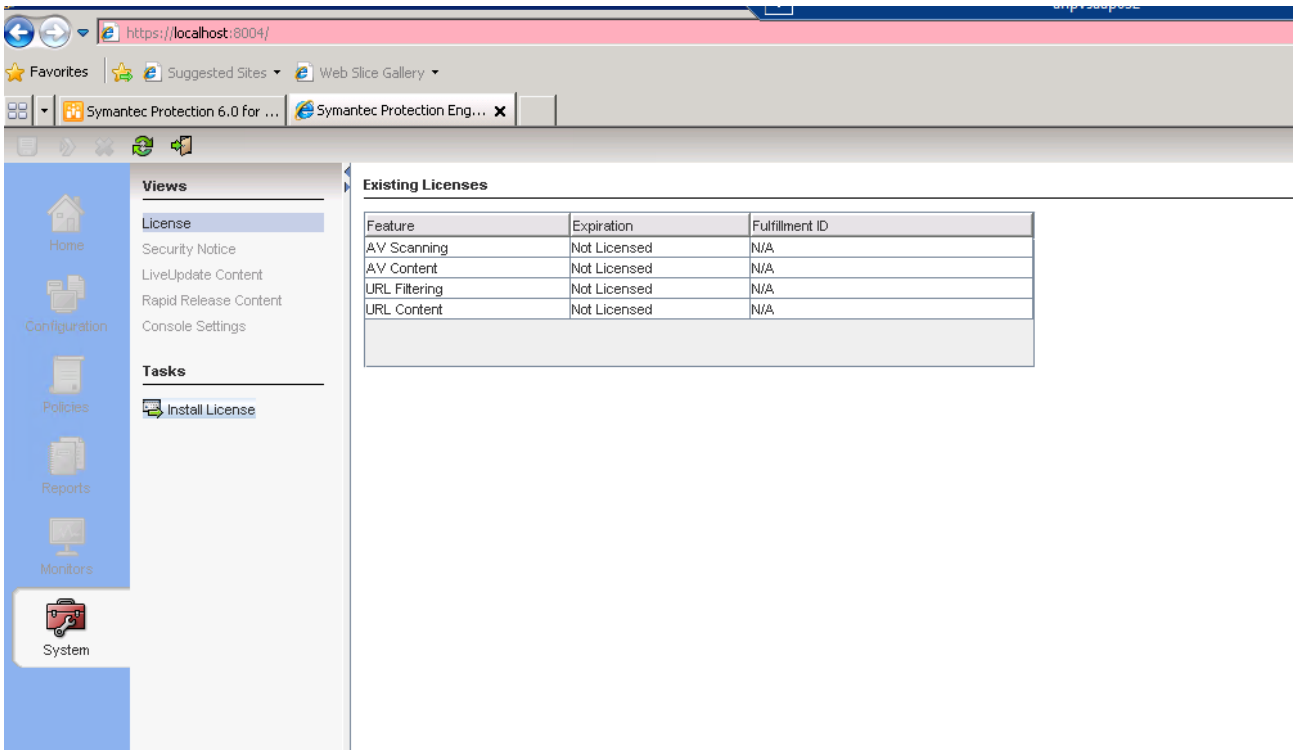

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel
Exit
Copyright © 2011 Symantec Corporation. All rights reserved.


Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Symantec Protection 6.0 for SharePoint Servers. Click Finish to exit the wizard.
Symantec.
< Back
Finish
Cancel
Exit
Copyright © 2011 Symantec Corporation. All rights reserved.

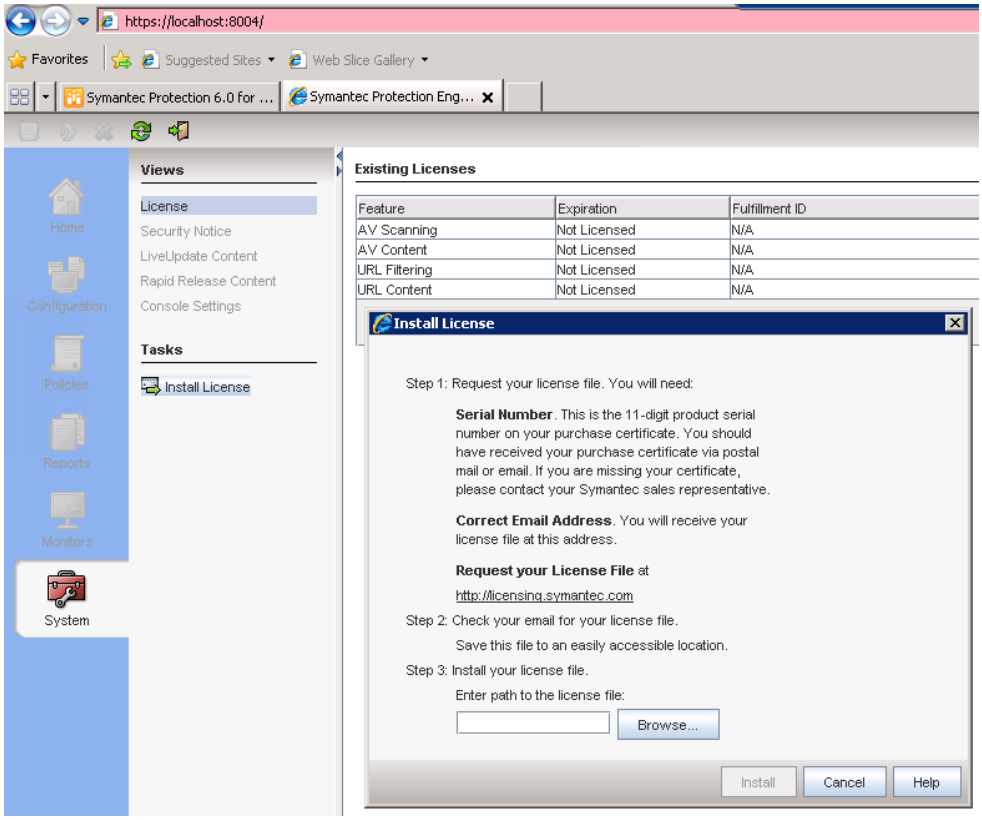

Symantec Protection 6.0 for SharePoint Servers
Symantec.
Symantec Protection 6.0 for SharePoint Servers - In...
Configure Real-time scan settings
To begin protecting your SharePoint server, you must first enable real-time scanning.
Do the following steps to configure Real-time scan settings:
1. Ensure that at least one Symantec Protection Engine is installed and configured within the SharePoint console.
2. Launch SharePoint Central Administration > Symantec Protection 6.0 for SharePoint Servers > Real-time scan settings > Edit settings
3. Enable the following:
Scan document on upload
Scan document on download
Attempt to clean infected documents
Note: We do not recommend enabling "Allow users to download infected documents within the SharePoint AV settings"
InstallShield
OK
Exit

Asennuksen jälkeen hallintakonsoli näkyy SharePointin hallinnassa. Tämän jälkeen voidaan aktivoida lisenssi.

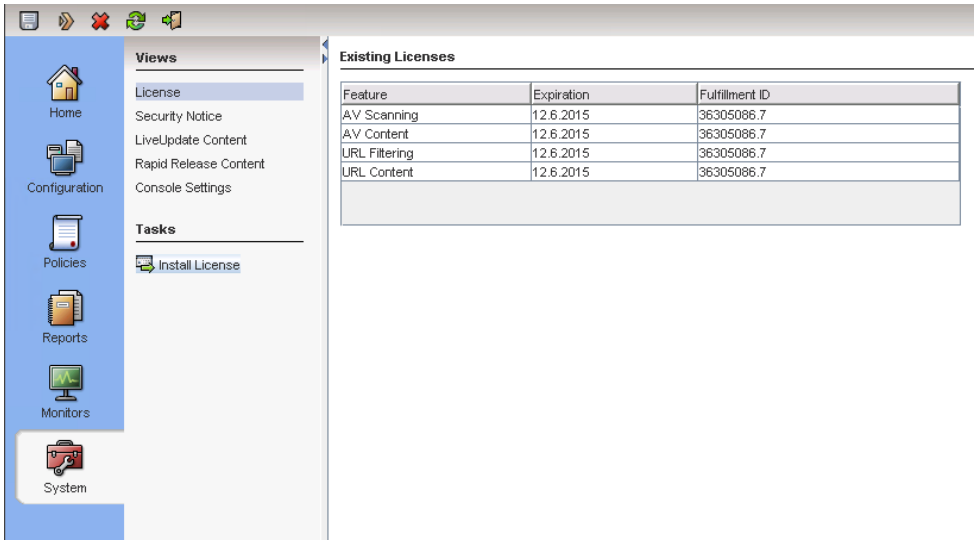




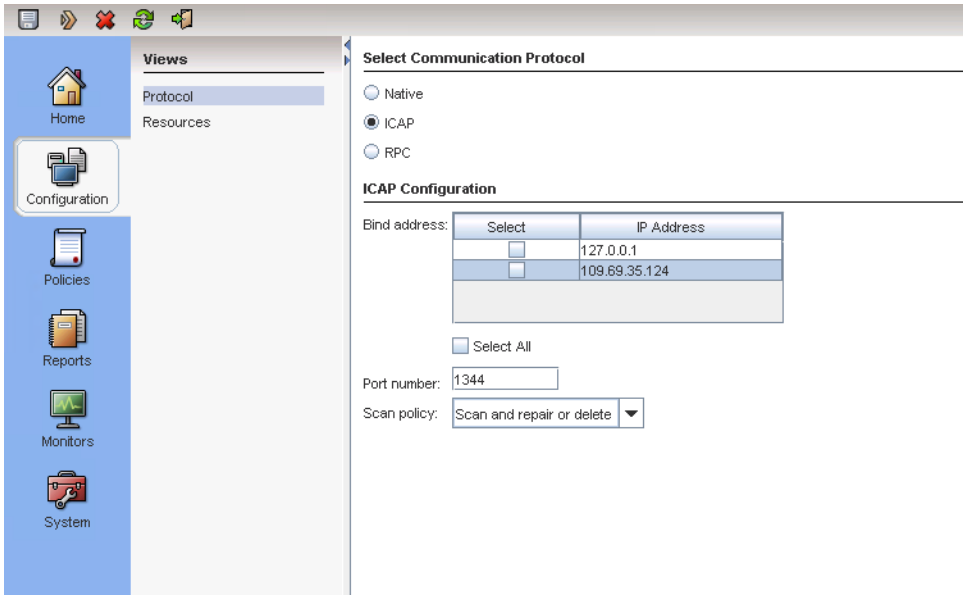
Ilman lisenssiä pesukone ei toimi.



Lisätään sähköpostiin saatu koekäyttölisenssi.

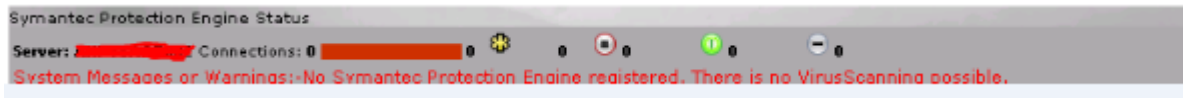


Lisenssi on asennettu, lisenssi menee umpeen 12.6.2015.



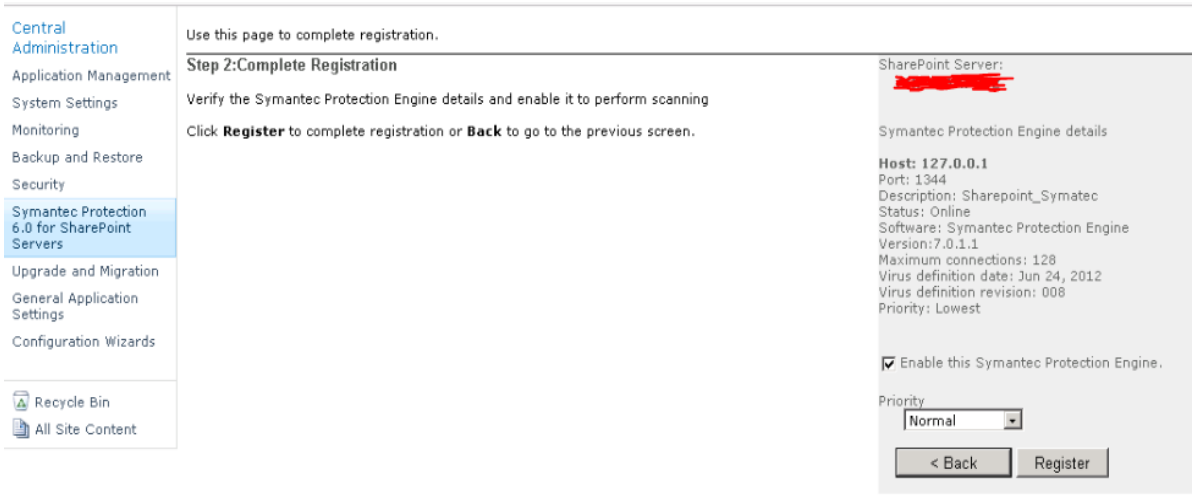
Määritelty IP-osoite 127.0.0.1 & portti 1344 tarvitaan pesukoneen rekisteröinnissä.

Huom. Jos engine/pesukone ei ole rekisteröity, alareunaan tulee seuravanlainen virheilmoitus.

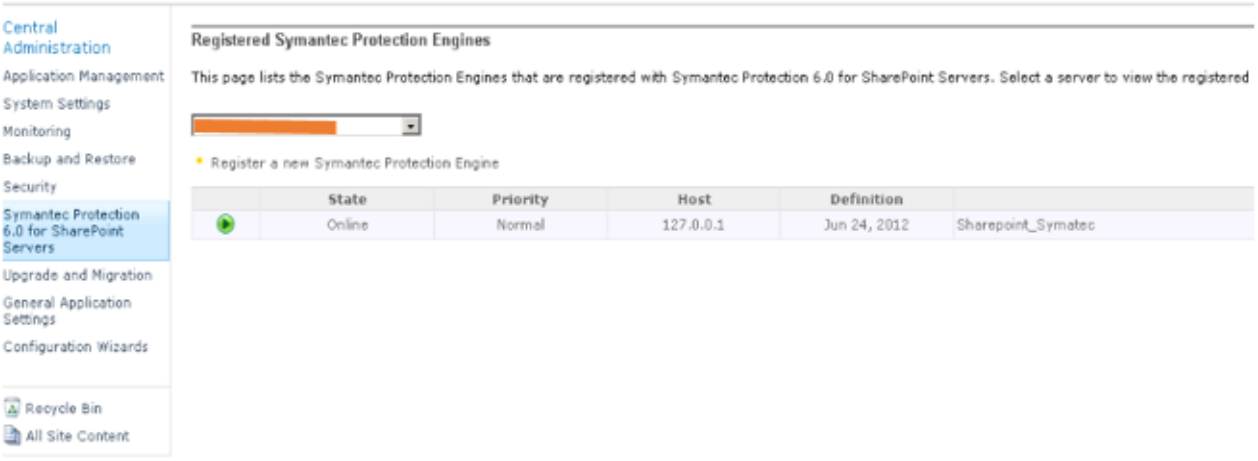


Avaa hallintakonsoli ja valitse ”Register a New Symantec Protection Engine”

Valitse ShraePoint palvelin ja sitten kirjoita palvelin johon on asennettu scan engine ja porttinumero.



Valitse prioriteetti ja paina Register



Engine on aktiivinen nyt ja halutut määritykset voidaan tehdä.