HAAGA-HELIA
ammattikorkeakoulu

Päiväkirjaopinnäytetyö, havaintoja Service Deskistä

Tommi Stadius

Opinnäyte

Tietojenkäsittelyn koulutusohjelma

2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

Raportin palautuksen tai esityksen päivämäärä

Tietojenkäsittely

Tekijä tai tekijät Tommi Stadius	**Ryhmätunnus tai aloitusvuosi** 2010
Raportin nimi Päiväkirjaopinnäytetyö, havaintoja Service Deskistä	**Sivu- ja liitesivumäärä** 83 + 0
Opettajat tai ohjaajat Altti Lagstedt	

Tämän opinnäytetyön tarkoituksena on seurata opiskelijan päivittäisiä työtehtäviä IT-yrityksen Service Deskissä. Tiimi muodostuu tällä hetkellä noin kymmenestä asiantuntijasta. Päivittäiset työtehtävät sijoittuvat ensisijaisesti tietoliikenne -ja tietoturvapalveluiden pariin. Service Deskin päivittäisiin tehtäviin kuuluvat palvelupyynnöt sekä vikatilanteiden selvittämiset. Seurantajakson aikana omaa tekemistä analysoidaan viikoittaisilla analyyseilla. Jakson lopussa käydään läpi seurantajakson aikana tehtyjä havaintoja.

Opinnäytetyön ajankohta on syksy 2014. Työmenetelmä on portfoliomainen päiväkirjaopinnäytetyö. Työssä tehdään päivittäisiä päiväkirjamerkintöjä, joissa pyritään kertomaan mahdollisimman tarkasti omista työtehtävistä. Viikoittain tehdään analyysi kyseisen viikon keskeisimmistä asioista ja pyritään kehittämään omaa tekemistä hyödyntäen eri lähteitä.

Opinnäytetyön aikana opiskelijan tekninen osaaminen kehittyi omien työtehtävien ohella. Opiskelija oppi tiedostamaan paremmin työskentelyssä esiintyviä prosesseja ITIL-viitekehyksen näkökulmasta sekä soveltamaan paremmin alaan liittyviä hyviä käytäntöjä esim. palomuurin toiminnan tietoturvallinen määrittely ja ylläpito. Opiskelija oppi myös uusia menetelmiä langattomien verkkojen vianselvitystä varten sekä hyviä käytäntöjä virtuaalisten palvelimien provisiointiin liittyen.

Asiasanat
Service Desk, ITIL, Palomuuri, VPN, Tietoturva

HAAGA-HELIA
University of Applied Sciences

Abstract

Date of presentation

Business Information Technology

Authors Tommi Stadius	**Group or year of entry** 2010
The title of thesis Diary thesis; Observations about Service Desk	**Number of report pages and attachment pages** 83 + 0
Advisor(s) Altti Lagstedt	

The purpose of this thesis is to follow a student's daily tasks at the Service Desk of a certain IT-company. The team is currently composed of ten engineers. The daily duties consist primarily of tasks related to telecommunication services and data security. Typical assignments for the Service Desk are daily service requests and incident management. In the study, the student's daily work is being analyzed in weekly reports. At the end of the period, all information is reviewed and composed into a final overview.

The timeframe for this study is fall 2014. The working method is portfolio based diary thesis. The thesis consists of daily entries in which the student tries to report all the tasks during that day as accurate as possible. Every week a report is written, where the student analyzes his own work and tries to improve it by reviewing different sources related to work.

During the study the student's work related skills got improved, as more challenging tasks appeared. The student also learned more about the ITIL based processes related to his work and applied the best practices related to daily tasks, for example improving data security when implementing and managing firewalls. The student also improved his skills in troubleshooting wireless network issues and learned the best practices concerning virtual machine provisioning.

Key words
Service Desk, ITIL, Firewall, VPN, Data security

Sisällys

1 Johdanto

Opinnäytetyön aikaväli on 18.8.2014 - 7.11.2014. Päiväkirjaosuuden pituus on 65 työpäivää.

Tämä opinnäytetyö käsittelee IT-alan yrityksessä tehtäviä töitä Service Desk työntekijän näkökulmasta. Työtehtävät perustuvat yrityksen tarjoamiin tietoliikenne -ja tietoturvapalveluihin. Työ kuvailee omia päivittäisiä työtehtäviäni nykyisessä työympäristössä. Työtä seurataan päivittäisillä päiväkirjamerkinnöillä ja viikoittaisilla analyyseillä. Opinnäytetyössä seurattava työskentely sijoittuu tietoliikenne ja tietoturva-alan piiriin. Työ sisältää myös mm. palvelinkeskuspalveluihin ja erilaisiin valvontasovelluksiin liittyviä työtehtäviä.

Yritys on 2000-luvun alussa perustettu tietoliikenne -ja tietoturvaratkaisuja tarjoava yritys. Palveluiden ensisijainen tarkoitus on tarjota lisäarvoa asiakkaan liiketoimintaan. Tämä strategia on valittu aikoinaan yrityksessä, kun tämän kaltaisilla palveluilla ei vielä ollut juurikaan tarjontaa. Tällä pyrittiin erottumaan joukosta muihin alalla toimijoihin nähden. Omat työtehtäväni liittyvät yrityksen tuottamiin palveluihin, joita me Service Deskissä ylläpidämme. Service Desk on osa yrityksen palvelutuotantoja, johon kuuluu myös toisen tason asiantuntijat sekä projektinhallinta.

Työtehtävissä suoriutuminen edellyttää vähintään IT alaan liittyvää ammattikorkeakoulututkintoa tai aiempaa työkokemusta vastaavista työtehtävistä. Itse aloitin kyseisessä tehtävässä koulun loppupuolella työharjoittelija, joten käytännön tason osaamiseni oli melko rajoittunutta. Teorian tasolla minulta löytyi koulussa opittua teorian osaamista. Työpaikka on myös ensimmäinen IT-alan työpaikkani. Olen kokenut menneen vuoden työelämässä erittäin opettavaiseksi.

1.1 Työympäristön esittely

Yritykseni on kasvussa oleva tietoturva -ja lisäarvopalveluita tuottava IT-talo. Yritys tarjoaa palveluitaan maailmanlaajuisesti. Kaikki operatiivinen toiminta tapahtuu kuitenkin Suomessa. Tarjottaviin palveluihin kuulu Service Desk tyyppinen asiakasrajapinta,

joka toimii 24 tuntia vuorokaudessa arkisin. Service Deskin oleellisin tehtävä on toimia ensisijaisena kontaktina asiakkaan palveluihin liittyen. Service Deskissä ratkaistaan suurin osa asiakkaan tekemistä palvelupyynnöistä sekä palveluissa ilmenevät vikatilanteet. Haasteellisimmat ja eniten aikaa vievät työpyynnöt ohjataan toisen tason tukiryhmälle, joka on tiiviissä yhteistyössä Service Deskin kanssa.

Tyypillisiä asiakkaita ovat isot suomalaiset yritykset, joilla on liiketoimintaa myös ulkomailla. Asiakkaille tarjottavilla palveluilla pyritään tehostamaan heidän ydinliiketoimintaansa. Keskeisiä asiakkaille tarjottavia palveluita ovat verkon tietoturvapalvelut, verkon hallinta ja valvonta, vahva tunnistautuminen ja langattomien verkkojen hallinta. Yritys tarjoaa asiakkailleen myös kustannustehokkaista palvelinkeskuspalveluita, joihin Service Deskin päivittäiset työtehtävät myös olennaisesti liittyvät.

Työympäristöni sijoittuu yrityksen Service Desk tiimiin. Tiimi koostuu tällä hetkellä kymmenestä asiantuntijasta. Toimimme ensisijaisena kontaktina asiakkaille myytyihin palveluihin. Työnkuvaan kuuluu erilaisten vikatilanteiden selvitystä sekä asiakkaiden tekemien palvelupyyntöjen suorittamista. Service Deskin työtehtäviin kuuluu myös tiivis yhteistyö myynti -ja projektitiimien kanssa.

1.2 Käsitteet

AD eli Active Directory, Microsoftin palvelinympäristöön liittyvä tietokanta, joka pitää sisällään tietoa käyttäjistä ja eri objekteista.

Anti-Spam, ohjelmisto, jolla voidaan suodattaa ei toivottuja sähköpostiviestejä.

ARP-taulu, verkkolaitteen ylläpitämä taulu, joka näyttää verkon IP-osoitteita vastaavat MAC-osoitteet.

Exchange, Microsoftin kehittämä sähköpostiohjelmisto.

MAC-osoite, laitteen yksilöllinen osoite, joka erottaa sen muista verkon laitteista. MAC-osoite on valmistajan asettama.

MX-tietue, nimipalvelussa määriteltävä tietue, joka osoittaa toimialueessa toimivaan sähköpostipalveluun.

Palomuuri, laite tai ohjelmisto, jolla eristetään yrityksen sisäverkko ja Internet. Palomuuria käytetään suodattamaan liikennettä näiden verkkojen välillä.

Service Desk, sanalla viitataan erilliseen IT-palveluun, joka toimii asiakasrajapintana yrityksen tarjoamiin palveluihin.

System Engineer, sanalla viitataan yrityksen työtekijään, joka toimii teknisenä asiantuntijana.

Virtuaalipalvelin, palvelinohjelmisto, joka pyörii fyysisen palvelinalustan yksittäisen virtuaalisen instanssina. Yksi palvelinalusta voi pyörittää monia eri virtuaalipalvelininstansseja.

VPN eli Virtual Private Network, teknologia, jolla sisäverkkoja voidaan yhdistää Internetin ylitse käyttäen salausta.

Wlan Controller, langattoman verkon ohjain, joka ohjaa tukiasemien toimintaa ja jakelee niille määrittelyjä.

2 Lähtötilanteen kuvaus

Lähtötilanteen kuvauksessa on tarkoitus kuvata omaa tekemistä sekä tarkastella omaa työympäristöä.

2.1 Oman nykyisen työn analyysi

Työnimikkeeni on System Engineer ja toimin osana Service Desk-tiimiä, joka on yksi osa yrityksen palvelutuotantoa. Se on myös näkyvin ja tärkein osa asiakasrajapinnassa. Työhöni kuuluu vaihtelevasti useita eri työtehtäviä:

- Yritysasiakkaiden vikatilanteiden selvittely
- Asiakkaiden esittämien palvelupyyntöjen toteuttaminen
- Service Desk järjestelmässä olevien tikettien seuraaminen ja päivittäminen
- Sisäisen dokumentoinnin päivittäminen

Yritys tarjoaa kansainvälisesti erilaisia palveluita tietoliikenne ja tietoturvapalveluiden alueilta. Isoimpana näistä on yrityksille tarjottavat verkon tietoturvapalvelut, jotka koostuvat erilaisista palomuuriratkaisuista. Näillä palveluilla pyritään tuomaan lisäarvoa asiakkaiden liiketoimintaan. Yritys tarjoaa myös palvelinkeskuspalveluita, joista näkyvimpänä ovat virtuaalipalvelimet ja SAN-verkot.

Työtehtävät Service Deskissä koostuvat enimmäkseen vikatilanteiden selvittelystä ja asiakkaiden tekemien palvelupyyntöjen toteuttamisesta. Näiden kahden osalta varsinaiset työt jakautuvat melko tasaisesti.
Vikatilanteet ilmenevät yleensä esim. asiakkaan verkossa tapahtuvassa väliaikaisesta tietoliikennekatkoksesta tai aktiivilaitteen rikkoutumisesta. Tällöin ruvetaan paikantamaan vikaa asiakkaan verkossa. Tarvittaessa otetaan myös yhteys eri sidosryhmiin, mikäli niiden apua tarvitaan ongelman ratkaisemisessa. Mikäli asiakkaan päätelaitteissa ilmenee vikoja, pyritään ne korvaamaan mahdollisimman pian.

Palvelupyynnöt liittyvät kaikkiin yrityksen tarjoamiin palveluihin. Näitä ovat mm.

- Verkon tietoturvapalvelut
- Palvelinkeskuspalvelut
- Vahvan tunnistautumisen menetelmät
- Verkon ja sovelluksien valvonta
- Erilaiset raportointipalvelut

Palvelupyyntö yksinkertaisuudessa koostuu siitä, kun asiakas tilaa muutoksen tai lisäyksen ostamaansa palveluun. Asiakas voi tehdä tämän joko puhelimitse tai erillisen järjestelmän kautta. Pyyntö voi esim. sisältää muutoksia palomuurin pääsylistoihin tai levytilan kasvattamista asiakkaan virtuaalipalvelimeen. Palvelupyynnön vastaanottamisen jälkeen Service Desk pyrkii suorittamaan pyynnön halutun mukaisesti. Mikäli pyyntö on haastavampi tai vaatii enemmän teknistä suunnittelua, voi Service Desk konsultoida vanhempia asiantuntijoita.

Työtehtävissä pärjääminen edellyttää tuntemusta verkoista sekä niihin liittyvistä teknologioista, tietämystä palvelinympäristöistä ja hyviä asiakaspalvelutaitoja. Yrityksessä pyritään hyvään asiakaskokemukseen. Päivittäisessä työskentelyssä ollaan tekemisissä seuraavien teknologioiden kanssa: palomuurit, LAN-verkot, langattomat verkot ja palvelinympäristöt.

Työtehtävien suorittamiseksi tulee joskus hyödyntää verkosta löytyviä sähköisiä aineistoja, esim. laitevalmistajan oma dokumentaatio. Oppiminen työpaikalla tapahtuu päivittäisten työtehtävien ohella. Lähes päivittäin tulee vastaan uudenlaisia haasteita ratkottavaksi.

Työpaikan puolesta on myös mahdollista kehittää omaa osaamistaan erilaisilla laitevalmistajien tarjoamilla sertifikaateilla. Työssäoloaikanani olen yhden tuollaisen sertifikaatin saanut suoritettua. Jatkossa on myös tarkoitus lisätä tämän tyylistä osaamista.

Olen nyt työskennellyt kyseisessä työpaikassa melkein puolitoista vuotta. Aloittaessani töissä, oli ammattitaitoni aloittelevan toimijan tasolla. Kaikki oli vielä hyvin uutta ja kaikki osaamiseni oli vasta teoreettisella tasolla. Palvelinympäristöjen osalta minulla oli jo koulusta jonkin verran käytännön kokemustakin. Tämän vuoksi tein aluksi lähes pelkästään palvelinpuolen työtehtäviä.

Ajan kuluessa aloin kuitenkin päästä sisään verkkopuolen työtehtäviin ja niihin liittyviin ohjelmistoihin. Osaamiseni kasvoi sitä mukaa, kun otin vastaan uusia työhaasteita. Aloin myös omatoimisesti opiskelemaan työtehtävien vaatimia asioita, jotta ne sujuisivat töissä sulavammin. Nykypäivänä osaamiseni on jo kehittynyt valtavasti. Pystyn työskentelemään paljon enemmän itsenäisesti. Uusien haasteiden kohdalla rupean omatoimisesti ratkomaan ongelmia. Pystyn myös opastamaan omia kollegoita, mikäli he apua tarvitsevat työtehtävissään. Tämän pohjalta arvioisin nykyisin olevan hyvin omien työtehtävieni tasalla.

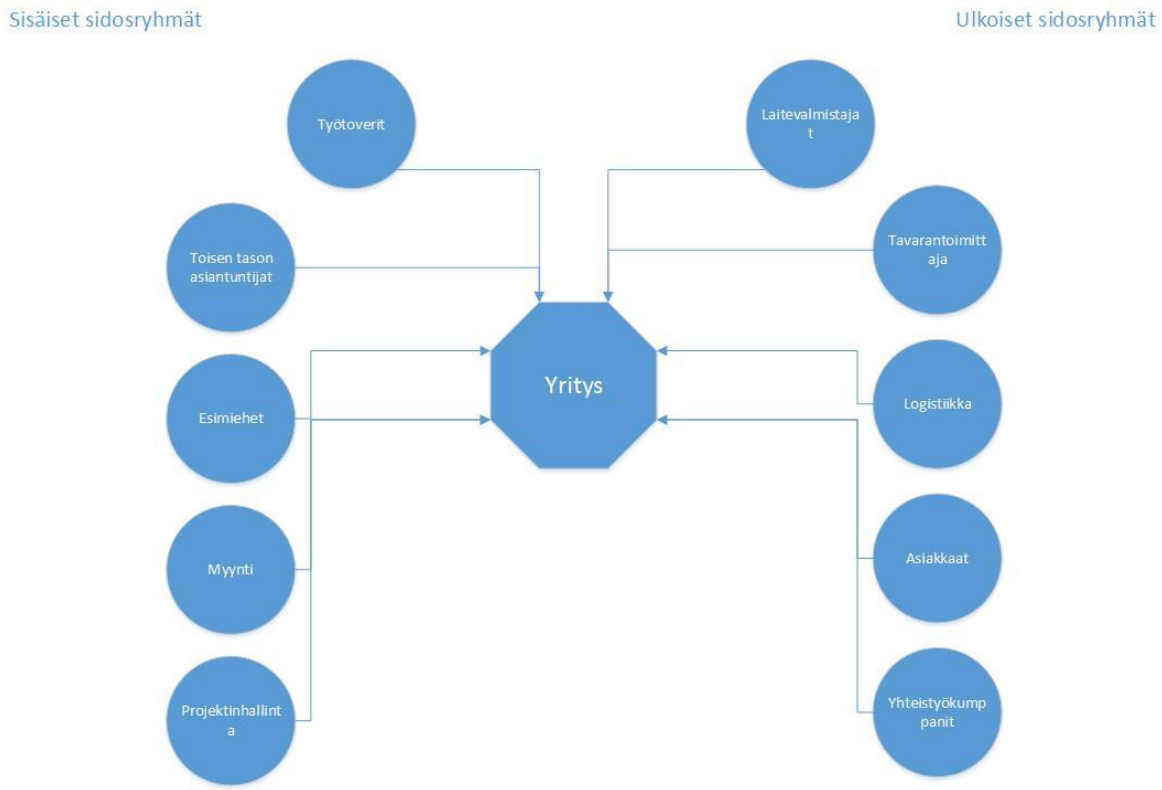
Ammatillinen kehitykseni on vasta aluillaan. Onhan tämä vasta ensimmäinen IT-alan työpaikkani. Tästä huolimatta alku kehityksessä on ollut sulava ja tästä on hyvä jatkaa eteenpäin. Työtehtävien ohella saatu ammattiosaaminen on selvästi kasvattanut itsevarmuutta tarttua haastavampien keikkojen pariin. IT alalla oman kehittymisen tulee olla jatkuvaa, jos haluaa menestyä. Jatkossa aioin panostaa enemmän verkkoteknologioiden opiskeluun, jotta voisin ymmärtää niitä paremmin. Omana suurimpana mielenkiinnon kohteena ovat edelleen palvelinverkot ja ympäristöt, joiden parissa toivon jatkossa tekeväni enemmän töitä.

2.2 Sidosryhmät työpaikalla

Työpaikalta löytyy seuraavia sidosryhmiä omasta näkökulmastani katseltuna

- Asiakkaat
- Tavarantoimittaja
- Kollegat
- Toisen tason asiantuntijat
- Laitevalmistajat
- Logistiikka
- Esimiehet
- Yhteistyökumppanit
- Myynti
- Projektinhallinta

Sidosryhmiä on myös kuvattu alla olevassa kaaviossa(Kuva1). Kaavioon on sisällytetty suoraan omaan työhöni liittyvät oleelliset sidosryhmät.



Kuva 1, Sidosryhmät

Asiakkaat ovat varmasti tärkein sidosryhmä koko yrityksen näkökulmasta. Ilman asiakkaita ei tule liikevaihtoa. Se miten asiakkaat kokevat yrityksen palvelut on erityisen tärkeää. Ensisijaisesti yrityksessäni pyritään parhaaseen mahdolliseen asiakaskokemukseen. Asiakkaille pyritään aina tarjoamaan heidän liiketoiminnalleen sopivia ratkaisua.

Esimiesten mielipiteet ja intressit työtäni ovat myös tärkeitä seikkoja. On tärkeää, että esimiehet ovat tyytyväisiä omaan ja tiimini työskentelyyn päivittäin. Omalta osaltani taas pyrin toteuttamaan parhaani mukaan heidän näkemyksiään ja ohjeistuksia työhön liittyen.

Toisen tason asiantuntijat ovat myös tiiviissä yhteistyössä Service Deskin kanssa. Vaikeimmat työpyynnöt menevät yleensä tämän tiimin selvitettäväksi laajamittaisen ajankäytön vuoksi. Service Desk voi myös tarvittaessa pyytää apua toisen tason asiantuntijoilta erilaisiin työtehtäviin liittyen.

Myynti ja projektinhallinta ovat myös tärkeitä sidosryhmiä Service Deskissä. Välillä asiakkaat saattavat palvelupyynnöissään tiedustella asioista, joihin Service Desk ei suoraan voi ottaa kantaa. Tällöin voidaan olla yhteydessä kyseisen asiakkaan nimettyyn myyjään ja yhdessä viestiä asiakkaan suuntaan yhtenäisesti. Projektinhallinta on yhteydessä Service Deskiin yleisimmin asiakastoimitusten osalta. Heidän tehtävänään on valvoa ja koordinoida uusien palveluiden käyttöönottoa ja toimittaa tarvittavat tiedot eri osapuolille.

2.3 Vuorovaikutustaidot työpaikalla

Service Deskissä vuorovaikutus työtovereiden kanssa on jatkuvaa. Pyrimme auttamaan toisiamme työtehtävissä ja samalla jakamaan tiimin työkuormitusta. Kollegoiden kanssa viestitään yleensä kasvotusten. Joitakin kollegoita työskentelee eri toimipisteissä, joten tällöin kommunikointi tapahtuu puhelimitse tai erilaisilla yrityksen sisäisillä pikaviestimillä. Työtovereiden kanssa keskustellaan yleensä työtehtäviin liittyvistä asioista. Kollegan kanssa voi esim. pyytää avustusta johonkin työtehtävään liittyvään ongelmana tai muuten vain kysyä mielipidettä asiaan.

Myöskin vanhempien asiantuntijoiden kanssa kommunikointi hoituu yleensä parhaiten kasvotusten puhumalla. Heidän kanssaan käydään yleensä keskustelua isommista projekteista ja haastavammista työtehtävistä.

Asiakkaan kanssa kommunikoidessa korostuvat omat vuorovaikutustaidot eniten. Asiakkaalle pitää antaa asiallinen sekä ystävällinen tunnelma palvelusta, erityisesti silloin, kuin kommunikoidaan puhelimitse. Nämä seikat saattavat välillä tuntua haasteellisilta, jos asiat eivät mene tai eivät ole menneet asiakkaan toivomalla tavalla. Asiakas saattaa olla tyytymätön saamaansa palveluun tai tuotteeseen. Tällöin on meidän tehtävämme yrittää saada hankittua asiakkaan luottamus takaisin yritykseen. Tarvittaessa asia voidaan myös eskaloida ylempien tasojen käsiteltäväksi.

3 Päiväkirjaraportointi

Päiväkirjaraportointi-osiossa kirjoitetaan päivittäin omista työtehtävistä. Viikoittain tehdään kattava analyysi kyseisen viikon tapahtumista.

3.1 Työviikko 34

Maanantai 19.8

Työpäivä oli melko hiljainen alkupäivästä. Minulla oli iltavuoro, joten työtehtäväni alkoivat vasta klo. 14.00. Tavoitteenani oli alkaa työstämään uusia jonossa olevia keikkoja kesälomani jälkeen. Hetken aikaa pienempiä hommia tehtyäni sai Service Desk tiimi kriittisen tason vikaselvitystyön. Erään asiakkaan pääyhteys Internettiin oli katkennut eikä vian aiheuttajaa saatu paikannettua äkillisesti. Kollegani aloittivat vianselvityksen yhdessä vanhemman asiantuntijan kanssa, jolla oli asiakkaan ympäristöstä enemmän tietoa. Vika vaikutti asiakkaan Suomen pään Internet yhteyksiin, sekä etäyhteyksiin ulkomaan toimipisteisiin. Ajan kuluessa vian selvittäminen siirrettiin minun vastuulleni, koska olin iltavuorossa.

Vikaa alettiin selvitellä asiakkaan Internetpalveluntarjoajan kanssa ja sieltä suunnalta ei vikaa löytynyt yhteydestä. Meidän tarjoamaan palomuuriin pääsimme kiinni asiakkaan ostaman varayhteyden kanssa. Samalla muutimme palomuurilla oletusreitin käyttämään varayhteyttä, jotta asiakkaan yhteydet toimisivat ainakin puolitasolla. Seuraavaksi vikaa ruvettiin selvittelemään konesalista, missä asiakkaan palomuuri ja reititin sijaitsivat. Samalla, kun tarkastimme asiakkaan julkisen kytkimen tilanteen, tarkasti asiakkaan palveluntarjoaja heidän reitittimensä tilannetta. Hetken tutkittumme tilannetta totesimme, että linkit molemmissa laitteissa olivat ylhäällä, mutta laitteiden ARP-tauluissa näkyneet MAC-osoitteet eivät täsmänneet. Tästä päädyimme johtopäätökseen, että laitteiden kytkennöissä oli tapahtunut muutoksia.
Päätimme seuraavaksi olla yhteydessä konesalista vastaavalle taholle kysyäksemme mahdollisista muutoksista verkossa. Jonkun aikaa asiaa tutkittuaan, he löysivät vian. Konesalissa oli aiemmin päivällä tehty vanhojen liittymien purkamisia ja epähuomiossa asiakkaamme Internet-liittymä oli myös kytketty irti. Kun konesalissa tehtiin kytkennät

uudelleen, alkoi asiakkaamme Internet liittymä taas toimia. Tämän jälkeen ilmoitimme asiakkaalle pikimmiten, että heidän liittymänsä on taas kunnossa ja palomuuripalvelu toimii jälleen normaalisti.
Asian selvittelyssä meni mielestäni turhan kauan aikaa, mutta se oli ihan ymmärrettävää koska mukana oli niin monta eri tahoa. Tällöin kommunikointi ja ajan tasalla pysyminen on erittäin haastavaa.

Tiistai 20.8

Eräs asiakas otti yhteyttä Service Deskiin sähköpostitse. Asiakas halusi tehdä uuden palvelupyynnön. Asia koski heidän ostamaansa Anti-Spam-palvelua, johon tarvittiin muutoksia. Asiakkaalla on monta eri toimipistettä ympäri maailmaa ja Suomessa sijaitsee heidän pääkonttorinsa. Palvelupyynnössä asiakas mainitsi haluavansa liittää heidän Espanjan toimipisteensä Anti-Spam palvelun piiriin.

Tämä muutos ei meidän kannalta ollut kovinkaan vaativa. Ensiksi pyysimme asiakasta muuttamaan heidän julkisessa nimipalvelussaan MX-tietueet niin, että ne osoittavat meidän tarjoamaan Anti-Spam palveluun. Tällöin saadaan sähköposti kulkemaan meidän järjestelmien kautta. Omassa järjestelmässämme lisäsimme asiakkaan uuden domainin sekä Exchange-palvelimen julkisen IP-osoitteen. Tämän jälkeen lisäsimme muutamia suodatussääntöjä ja Antivirus ominaisuuksia asiakkaan sisään tulevalle postiliikenteelle.
Palomuurin osalta tämä ei vaatinut muutoksia, koska Internetistä tulevan sähköpostiliikenne oli jo sallittu heidän Exchange-palvelimelleen. Muutoksien jälkeen asiakas huomasi, että mailit eivät vielä kulkenut perille asti. Asiakas sai virheilmoituksia, että maileja ei pystytty välittämään heidän postipalvelimelleen. Asia kuitenkin korjaantui myöhemmin itsekseen, kun uudet MX-tietueet olivat päivittyneet Internettiin. Yleensä nimipalvelutietueiden TTL-arvot ovat oletuksena monia tunteja, mistä johtuen niiden päivittyminen eri nimipalvelimiin voi kestää jopa vuorokauden.

Keskiviikko 21.8

Asiakas lähetti Service Deskiin palvelupyynnön, jossa he ilmoittivat yhteysongelmista eri toimipisteidensä välistä. He yrittivät ottaa Unkarin toimipisteestä yhteyttä palvelimeen, joka sijaitsi Venäjällä. Tämä ei kuitenkaan jostain syystä onnistunut. Asiakas lähestyi meitä ja kysyi miten näiden toimipisteiden välinen yhteys on toteutettu. Lähdin tutkimaan asiaa molempien toimipisteiden dedikoiduilta palomuureilta. Selvisi, että suoraa VPN-yhteyttä toimipisteiden välillä ei ollut olemassa ja kaikki yrityksen sisäinen liikenne kulki Suomen pääpalomuurin kautta VPN-tunnelin sisällä.

Tiedustelin asiakkaalta heidän käyttämiään sisäverkkoja. Asiakas toimitti tiedot ja tämän jälkeen pääsin tekemään muutoksia palomuureihin. Ensiksi lisäsin Suomen pääpalomuurille palomuurisäännön, joka salli kaiken liikenteen Ukrainan aliverkosta kohti Venäjän aliverkkoa. Venäjän palomuurilla tarkastin sisään tulevan liikenteen säännöt VPN-tunnelin osalta. Kaikki näytti olevan kunnossa, mutta reititys Ukrainan aliverkkoon näytti puuttuvan. Lisäsin palomuurille staattisen reitin tuohon verkkoon ja ilmoitin asiakkaalle, että testaisivat toimivuutta. Myöhemmin asiakas vahvisti yhteyden nyt toimivan.

Torstai 22.8

Olin iltavuorossa ja noin puoli tuntia ennen vuoron loppumista sain puhelun asiakkaaltamme Yhdysvalloista. Asia liittyi kollegani hoitamaan tikettiin, jossa asiakas oli pyytänyt VPN-etäkäyttötunnuksia uudelle työtekijälleen. Asiakas oli pyytänyt myös ohjeistusta VPN-yhteyden käyttöön. Kollegani oli jo merkinnyt tiketin ratkaistuksi, mutta asiakkaalla oli vielä käytännön haasteita VPN-yhteyden muodostamisen kanssa.

Puhelimessa asiakas ilmoitti, että hänen tunnuksensa eivät toimineet ja VPN-ohjelmiston asennuskaan ei onnistunut. Tarkastelin tilannetta palomuurilta ja samalla luin tiketiltä asiakkaan kanssa vaihdeltuja sähköpostiviestejä. Niistä ilmeni nopeasti, että annetut ohjeet VPN-yhteyden käyttöön olivat ihan oikeat. Asiakkaan palomuurissa VPN-yhteyteen oli asetettu LDAP-autentikointi, jolloin palomuuri tekee kyselyn käyttäjätunnuksesta asiakkaan AD-palvelimelle. Tällöin mahdollisen virheen selvittäminen

palomuurin osalta on aika rajallista. Tarkastin kuitenkin palomuuriasetukset ja ne näyttivät olevan kunnossa. Ohjeistin asiakasta olemaan yhteydessä heidän IT-osastoonsa ja tarkastamaan, että käyttäjä kuuluu oikeaan AD-ryhmään, jonka perusteella VPN-autentikointi tehdään. Tämä todennäköisesti oli syy tunnuksien toimimattomuuteen. Asiakas ei myöskään saanut VPN-ohjelmaa ladattua palomuurin portaalisivun kautta. Tutkiessani tätä huomasin, että palomuurilta puuttui koko asennuspaketti, joka jaellaan käyttäjille kirjautumisen yhteydessä. Nopeana ratkaisuna keksin ehdottaa asiakkaalle VPN-ohjelman lataamista valmistajan nettisivuilta. Asiakas sai ladattua ohjelmiston ja asennettua sen. Opastin myös asiakasta laittamaan tarvittavat määrityksen ohjelmaan, jotta VPN-yhteys voitaisiin muodostaa. Asiakas testasi yhteyden toimivuuden eri tunnuksella.

Viikkoanalyysi

Ensimmäinen työviikko kesäloman jälkeen sujui melko rauhallisissa merkeissä. Kesälomakausi vaikutti vielä näkyvästi työtehtävien määrään. Työtehtävät jakautuivat melko tasaisesti palvelupyyntöihin ja vikaselvittelyihin. Viikosta jäi kuitenkin enemmän mieleen erilaiset vikatilanteiden selvittelyt. Ammatillinen kehitys kuluneen viikon aikana oli melko vähäistä. Sen sijaan viikon aikana tuli muistuteltua paljon asioita eri teknologioista, jotka olivat kesäloman aikana päässeet unohtumaan.

Viikon aikana opin ainakin uusia asioita käyttämästämme Anti-Spam palvelusta. Viikon alussa tullutta palvelupyyntöä varten oli minun opeteltava järjestelmästä uusia ominaisuuksia, joita en vielä aiemmin ollut päässyt käyttämään. Työviikon vuorostani johtuen en voinut konsultoida kollegoita suoraan ongelmiin liittyen vaan minun piti kääntyä yksikköni oman sisäisen dokumentoinnin puoleen. Tämän dokumentoinnin avulla pääsin asiasta jonkinlaiseen käsitykseen ja sain konfiguraatiot tehtyä halutulla tavalla.

3.2 Työviikko 35

Maanantai 25.8

Eräs asiakas oli jättänyt sähköpostilla vianselvityspyynnön Service Desk järjestelmäämme. Vikatilanne liittyi heidän ostamaansa virtuaalipalvelimeen ja sen toimintaan. Tiketissä asiakas ilmoitti, että Remote Desktop yhteys heidän palvelimelleen ei enää onnistunut. Asiakas ilmoitti myös, että palvelin oli myös uudelleenkäynnistetty edellisenä yönä. Kyseessä oli asiakkaan SQL-tietokantapalvelin, jossa oli käyttöjärjestelmänä Windows Server 2008 R2.

Pääsin itse tarkastelemaan tilannetta virtuaalipalvelimen hallinnan kautta VMwaren Vsphere-ohjelmalla. Tätä kautta palvelimeen pystytään ottamaan konsolisessio, joka toimii samoin kuin konetta käytettäisiin paikallisesti. Yleensä virtuaalipalvelimen vikatilanteessa tämä on ainut vaihtoehto saada jotain näkyvyyttä koneen tilaan. Avasin session ja näin, että Windows oli jäänyt jumittamaan kirjautumisikkunaan. Tämä näytti estävän kaikkien palveluiden käynnistymisen ja koneen normaalin toiminnan. Ainut vaihtoehto tässä tilanteessa oli uudelleenkäynnistää virtuaalikone. Resetoinnin jälkeen Windows käynnistyi normaalisti ja testasin myös sisäänkirjautumisen, joka näytti nyt jälleen toimivan normaalisti. Kuittasin asiakkaalle, että heidän palvelimensa toimii jälleen normaalisti.

Tiistai 26.8

Asiakas teki palvelupyynnön koskien heidän etäkäyttöpalveluaan. Kyseinen etäkäyttöpalvelu perustuu Juniperin SSL-VPN teknologiaan. Palvelu voi olla virtuaalisena sovelluksena erillisessä virtuaalikoneessa tai dedikoituna fyysisenä laitteena asiakkaan tiloissa. Tässä tapauksessa asiakkaalla oli oma dedikoitu laite, joka ajaa palvelua. Tiketissä asiakas halusi lisätä pääsyn kahdelle konsultille heidän sisäverkon resursseihinsa. Lisäykset tein ensin SSL-VPN laitteelle.

Ensiksi tehtiin uusi rooli kyseisiä käyttäjiä varten. Roolissa määritellään sen nimi, erilaiset ominaisuuksia roolille ja itse pääsyominaisuudet. Pääsyominaisuuksia saa määriteltyä

monia erilaisia, mutta tässä tapauksessa pääsytavaksi määriteltiin normaali VPN-tunnelointi. Tunnelointia varten tarvitsee määrittää pääsylistat, joissa taas määritellään sallittavat kohdeverkot ja portit. Asiakas halusi määritettäväksi vain yhden kohdepalvelin, johon avattiin kaikki portit. Tämän lisäksi VPN-tunnelointiin määriteltiin vielä Split Tunneling ominaisuus, jossa pääsylistoissa määritellyt kohdeverkot reititetään salatun VPN-tunnelin läpi ja muu liikenne menee käyttäjän aktiivisen Internet yhteyden kautta. Seuraavaksi tehtiin Role Mapping, jossa määritellään minkä roolin käyttäjät saavat kun he kirjautuvat järjestelmään. Tähän kohtaan valittiin uusi luotu rooli. Asiakkaalla oli käytössä vielä erillinen kaksivaiheinen autentikointi, joten käyttäjät piti vielä lisätä erilliselle autentikointipalvelimelle. Palvelimella määritellään käyttäjätunnukset ja käyttäjien puhelinnumerot. Kun käyttäjä kirjautuu SSL-VPN laitteen web-portaaliin, lähettää palvelin kertakäyttöisen PIN-koodin, jonka käyttäjä joutuu syöttämään järjestelmään kirjautuakseen.

Keskiviikko 27.8

Työskentelin yövuorossa ja olin saanut kollegalta tiketin, joka oli ollut auki jo hieman pidemmän aikaa. Tiketti kosketti erään isomman asiakkaan ongelmaa heidän langattoman verkkoratkaisunsa kanssa. Teknologiana käytetään Aruban langattoman verkot ratkaisuja. Asiakkaan Australiassa sijaitsevassa toimipisteessä oli yksi etätukiasema, joka toimii yhteyspisteenä yrityksen resursseihin Internetin yli. Tukiasemaan oli tullut jotain vikaa ja käyttäjät eivät saaneet yhdistettyä tukiasemaan. Ilmeisesti asiakas oli tehnyt toimipisteessä jotain uudelleenjärjestelyitä. Paikallisten käyttäjien avulla tukiasemaa diagnosoitiin, mutta mitään selvää toimimattomuutta ei havaittu. Myöskin tukiaseman fyysinen tila näytti olevan kunnossa. Lopulta päädyttiin ratkaisuun missä loppukäyttäjiä ohjeistettiin resetoimaan tukiasema oletusasetuksille konsolikaapelin avulla. Tämän toimenpiteen jälkeen tukiasema konfiguroitiin samoille asetuksille ja se alkoi taas toimia normaalisti.

Asiakas valitteli vielä, että yhdellä käyttäjällä ei yhdistäminen tukiasemaan onnistunut Ethernet-kaapelin välityksellä, mutta langattoman yhteyden kautta yhteys toimi. Päätin soittaa käyttäjälle Australiaan ja selvittää asiaa puhelun aikana. Pyysin käyttäjää kytkemään langattoman verkkokortin pois päältä ja kytkemään Ethernet-kaapelin tukiase-

man ja läppärin välille. Samalla tutkin lokia Controllerilta, johon tukiasema ottaa yhteyden. Näin lokista, että käyttäjän koneen MAC-osoite ei ollut sallittu tukiaseman pääsylistassa. Lisäsin kyseisen MAC-osoitteen tukiaseman pääsylistaan ja pyysin käyttäjää testaamaan yhteyden uudelleen. Muutoksen jälkeen käyttäjän yhteys alkoi toimia halutulla tavalla.

Viikkoanalyysi

Viikko kului taas työelämässä ja töitä riitti aiempaa enemmän. Menneellä viikolla työskentelin yövuorossa, joten suorat kontaktit asiakkaiden kanssa jäivät hyvin vähäisiksi. Koko työviikko, kuten aina yövuorossa, muodostui pääosin sähköpostin lukemisesta ja lähettämisestä asiakkaiden kanssa. Yövuorossa harvemmin ollaan puhelimitse tekemisissä asiakkaiden kanssa, ellei asiakas satu sijaitsemaan toisella puolella maapalloa, jolloin heillä saattaa olla päiväsaika.

Työtehtävien tekeminen yövuorossa on hyvin itsenäistä, sillä muita työtekijöitä ei samaan aikaan toimistolla ole. Kaikki työtehtäviin liittyvät kysymykset tulee lähes poikkeuksetta yrittää selvittää itse. Tapanani on ollut, että haastavamman keikan sattuessa siirrän asian käsittelyn päivävuorolle, jolloin käytettävissä on enemmän resursseja asian selvittämiseksi.

Viikon aikana merkittävimmät haasteet liittyivät yrityksemme tarjoamiin langattoman verkon ratkaisuihin. Itselleni tekemiset kyseisten teknologioiden kanssa on jäänyt vähemmälle ja näin ne tuottavat yleensä eniten haasteita, varsinkin erilaisissa ongelmatilanteissa. Päätin tähän analyysiin tarkastella hieman valmistajan(Aruba) omaa ja yleisempää dokumentaatiota keskiviikkona kohtaamani ongelmaan liittyen. Löytämääni tietoa aion käyttää hyväksi seuraavilla kerroilla, kun vastaavia ongelmia tulee vastaan. Päätin tarkentua tällä kertaa erityisesti tukiaseman(AP) ja tietokoneen(Client) väliseen yhteyteen ja tarkastella yleisimpiä yhteysongelmia näihin liittyen. Jatkan aihealueen käsittelyä seuraavassa analyysissä.

Valmistajan omasta dokumentaatiosta löytyy hyödyllisiä vinkkejä yhteysongelmien ratkomiseen. Ongelman selvittely kannattaa aloittaa aina itse ongelman paikantamisesta.

Yleensä ongelmat voidaan rajata neljään eri osa-alueeseen: itse Wlan Controller, tukiasema, langaton päätelaite ja Backend serverit. Nämä neljä kokonaisuutta voidaan taas rajata kahdenlaisiin ongelmiin, jotka ovat infrastruktuuriongelmat ja käyttäjäkohtaiset ongelmat. (Aruba 2014.).

Infrastruktuurin ongelmia ovat esim. tukiasemien yhteysongelmat Controlleriin, Controllerien väliset yhteysongelmat tai Controllerin ja serverien väliset yhteysongelmat. Käyttäjäkohtaisia ongelmia voivat olla esim. langaton verkko ei näy käyttäjälle, kirjautuminen verkkoon ei onnistu tai langaton verkko pätkii. (Aruba 2014.)

Ongelman rajaaminen helpottaa huomattavasti vianselvityksen etenemistä. Jos ongelma ilmenee yhdellä päätelaitteella, on vika luultavasti sen asetuksissa. Mikäli sama ongelma esiintyy monella päätelaitteella, voi ongelma olla itse tukiasemassa. Päätelaiteen osalta ongelmat voivat liittyä esim. verkkokortin ajureihin tai sen asetuksiin. Tukiaseman lähettämään radiosignaaliin voivat vaikuttaa monet eri materiaalit toimitiloissa. Mikäli toimitilojen kuuluvuuden kanssa ilmenee ongelmia, on syytä tehdä toimitilojen kuuluvuudelle uusi skannaus käyttäen siihen tarkoitettua ohjelmistoa. (HP 2014.)

Itse tukiaseman vianselvitys kannattaa aina aloittaa tarkastamalla sen virransaanti. Tukiasemat toimivat joko vaihtovirralla tai POE(Power Over Ethernet):lla, jolloin tukiasema saa virtansa Ethernet-kaapelin välityksellä kytkimestä. Vikatilanteessa voi siis kokeilla vaihtaa virtalähdettä tai kokeilla kytkimessä toista vapaana olevaa porttia. Seuraavaksi tukiasemasta voidaan tarkistaa, että onko se saanut IP-osoitteen. Tämä tulee lähes poikkeuksetta aina DHCP-palvelimelta. Jos tukiasema ei saa IP-osoitetta, kannattaa ongelman selvitys aloittaa DHCP-palvelimen päästä ja tutkia onko kysely tullut sinne asti. Tukiasemalle voidaan myös määritellä staattinen IP-osoite, jos dynaamista osoitetta ei saada toimimaan. (Aruba 2014.)

Seuraavaksi voidaan tarkistaa tukiaseman ja Controllerin välinen yhteys. Tukiasemalta tulisi voida pingata Controllerin julkista IP-osoitetta. Tämä on yleensä määritelty yrityksen sisäisessä DNS-palvelimessa nimellä aruba-master, jota tukiasemat oletuksena kyselevät. Mikäli yhteys perille asti ei muodostu, on tällöin tarkastettava reitin varrelta kaikki verkon aktiivilaitteet. Mikäli perusvaatimukset yhteyden muodostumiselle ovat kunnos-

sa, voidaan seuraavaksi tarkistaa mainostaako tukiasema sille konfiguroituja verkkoja. Mahdollisessa virhetilanteessa on tarkistettava, että jokaiselle langattomalle verkolle on määritetty oma VLAN lähimmällä Controllerilla. Viimeisenä vaiheena tarkastetaan tukiaseman tila. Tämä voidaan helpoiten tehdä Controllerilta. Tukiaseman tila on joko ylhäällä tai alhaalla. Mikäli tukiasema näkyy alhaalla Controllerilta, voidaan lokista nähdä mahdolliset syyt tälle. Yleisempänä ongelma lienee, että tukiasema ei saa haettua itselleen konfiguraatiota tai yhteys pätkii pahasti. (Aruba 2014.)

Nämä lukemani ohjeistukset olivat osa minullekin täysin uutta informaatiota, joten koin ne myös itse hyvin hyödyllisenä tietona. Aion myös jatkossa käyttää vastaavaa ohjeistusta työni tukena, mikäli tilanne näin vaatii.

3.3 Työviikko 36

Maanantai 1.9

Otin tikettijärjestelmästämme tiketin itselleni käsittelyyn. Tiketti sisälsi erään asiakkaan palvelupyynnön, joka vaatisi hieman enemmän tekemistä. Halusin kuitenkin hieman haastavamman tehtävän ratkottavaksi. Tiketissä asiakas ilmoitti, että heidän yhteen toimipisteeseensä, joka sijaitsi Romaniassa, oli hankittu uusi Internet-yhteys. Asiakas halusi ottaa tämän uuden linjan käyttöön, mutta säilyttää samalla olemassa olevan Internet-yhteytensä toiselta palveluntarjoajalta. Uusi yhteys tuli määrittää ensisijaiseksi linjaksi Internettiin päin. Kohteessa on yrityksemme toimittama palomuuripalvelu sekä muutama hallittu kytkin. Tämä muutos siis vaatisi muutoksia sekä julkisen puolen kytkimeen sekä palomuuriin. Päätin ensin tehdä tarvittavat konfiguraatiot kytkimeen. Aluksi kuitenkin menin kysymään hieman neuvoja konfigurointiin liittyen vanhemmalta asiantuntijalta.

Yhdessä kollegani kanssa tarkastelimme kytkimen nykyistä konfiguraatiota. Tilanne näytti siltä, että kaksi ensimmäistä porttia oli määritelty nykyiselle Internet-yhteydelle. Portit oli määritelty VLAN 20:een. Seuraavat kaksi porttia taas oli määritelty yrityksen MPLS-yhteydelle. Nämä portit olivat taas määritelty VLAN 30:een. Päätimme yhdessä kollegani kanssa, että laitamme määrittelyt uudelle yhteydelle seuraavin vapaisiin port-

teihin, jotka olivat siis portit viisi, kuusi ja seitsemän. Kyseiset portit laitettiin siis uudelle yhteydelle ja portit laitettiin uuteen VLAN:iin 40. Portit on tarkoitus kytkeä niin, että ensimmäiseen porttiin tulee ensimmäinen palomuuri ja toiseen porttiin tulee toinen palomuuri. Palomuurit muodostavat yhdessä eräänlaisen klusterin, joka tuo vikasietoisuutta niiden toimintaan laiterikon sattuessa. Kolmanteen vapaaseen porttiin on tarkoitus kytkeä itse reititin.

Kytkimen konfiguroinnin jälkeen oli seuraavan vuorossa palomuurin konfigurointi. Tutkin palomuurin konfiguraatiota ja paikansin sieltä ensimmäisen vapaan portin, joka oli numero kaksi. Asiakas oli tiketissä toimittanut uudet IP-aliverkon, joka tuli määritellä palomuurille. Määrittelin halutun IP-osoitteen ja aliverkon uudelle portille ja tein palomuurin reititystauluun uuden nollareitin, jotta yhteys ulospäin uutta linjaa käyttäen voisi toimia. Koska palomuurilla oli jo kaksi oletusreittiä käytössä, laitoin uuden nollareitin prioriteetin niin, että se ei yliaja vanhoja reittejä. Tässä vaiheessa ei enempää konfiguraatiota ei vielä pystytty tekemään, koska asiakas ei ollut vielä kytkenyt uusia kaapeleita kiinni palomuuriin. Ohjeistin asiakasta sähköpostitse tekemään kytkennät palomuurilla määrittelemälläni tavalla ja jäin odottamaan asiakkaan vastausta. Päätin jatkaa palvelupyynnön toteuttamista seuraavana päivänä.

Tiistai 2.9

Jatkoin edellisenä päivänä aloittamaani työpyynnön suorittamista. Eilen olin saanut jo suuren osan konfiguraatiosta tehtyä palomuuriin ja kytkimeen. Olin myös lähettänyt asiakkaalle ohjeistuksen sähköpostilla uuden yhteyden kytkemiseksi. Asiakas kuitenkin vielä pyysi hieman tarkennusta asiaan, jotta he saisivat kytkennät varmasti tehtyä oikein ensimmäisellä kerralla. Lähetin asiakkaalle uuden sähköpostin missä ohjeistin vielä kerran kytkennät palomuurin, kytkimen ja reitittimen välillä. Ilmoitin, että palomuuriklusterin ensimmäisen laitteen portti kaksi tulisi kytkeä kytkimen porttiin viisi ja toisen palomuurilaitteen portti kaksi tulisi kytkeä porttiin kuusi. Uuden reitittimen vapaa Ethernet-portti taas tulisi kytkeä kytkimen porttiin seitsemän. Määrittelemällä uuden yhteyden ja sen käyttämät portit kytkimellä omaan VLAN:iin vähentää yleislähetys-paketteja ja näin selkeyttää sen toimintaa.

Asiakas vastasi pian sähköpostiin ja ilmoitti, että kytkennät oli nyt tehty halutulla tavalla. Tarkastin tilanteen palomuurilta ja kytkimeltä. Kaikki linkit näyttivät olevan ylhäällä ja palomuurin ARP-taulussa näkyi uuden reitittimen MAC-osoite. Reititystä ei ollut vielä käännetty uudelle linjalle ja kysyinkin asiakkaalta, että milloin tämän voisi tehdä. Ilmoitin myös, että reitityksen muuttamisesta koituu paikan päälle muutaman sekunnin mittainen yhteyskatkos, joka näkyy käyttäjillä sessioiden katkeamisena. Asiakas vastasi, että muutos voitaisiin tehdä kuuden aikaan illalla, jonka jälkeen asiakkaan yhteyshenkilö voisi testata uuden yhteyden toimivuuden.

Aloitin tekemään sovittuja muutoksia illalla kuuden aikaan. Ensimmäiseksi päätin tehdä palomuurisäännöt uudelle yhteydelle. Luonnollisesti uudesta yhteydestä pitäisi olla samat pääsyt ulospäin kuin vanhasta yhteydestä. Muutoksen sain kätevämmin tehtyä, kun kopioi olemassa olevat palomuurisäännöt palomuurin konfiguraatiosta Notepad ohjelmaan. Notepadissa muutin sääntöihin vain kohdeportin nimen. Tämän jälkeen ajoin säännöt sisään palomuurin komentorivin kautta. Palomuurin reititystaulussa tein muutoksen, jossa muutin uuden tekemäni oletusreitin prioriteettia. Laitoin oletusreitin prioriteetiksi arvon 10 ja vanhaan yhteyteen osoittavan oletusreitin prioriteetiksi arvon 20. Tämän lisäksi palomuurilla oli vielä oletusreitti, joka oli kohdistettu yrityksen MPLS verkkoon. Muutin kyseisen reitin prioriteetille arvon 30, jolloin se toimii kolmantena vaihtoehtona, kun palomuuri valitsee oletusreittiä. Muutoksien jälkeen uusi linja ja reititys lähtivät toimimaan odotetulla tavalla. Ajoin myös palomuurilta traceroute-komennon, jolla pystyin todentamaan, että liikenne tosiaan kulki tämän uuden yhteyden kautta. Myöskin uudet tekemäni palomuurisäännöt näyttivät saavan osumia.

Asiakas oli aiemmin maininnut vielä, että palomuurilla olevat VPN-tunnelit voisi myös siirtää käyttämään uutta Internet-yhteyttä. Muutos vaati palomuurilla määrittelyn VPN-tunnelin parametreihin, jossa portiksi määriteltiin uusi yhteys, joka siis oli portissa kaksi. Tämän lisäksi muutoksia piti vielä tehdä Suomen pääpalomuurissa, jonne asiakkaan VPN-tunneli oli terminoitu. Suomen palomuurissa VPN-tunnelin Remote Gateway osoite piti vaihtaa osoittamaan uuden Internet-yhteyden käyttämään IP-osoitteeseen. Romanian palomuurissa oli vielä meidän hallinta VPN-tunneli, jota käytämme palomuurin hallinnointiin. Päätimme jättää VPN tunnelin käyttämään vanhaa yhteyttä, jotta se ei kuluttaisi asiakkaan kaistanleveyttä.

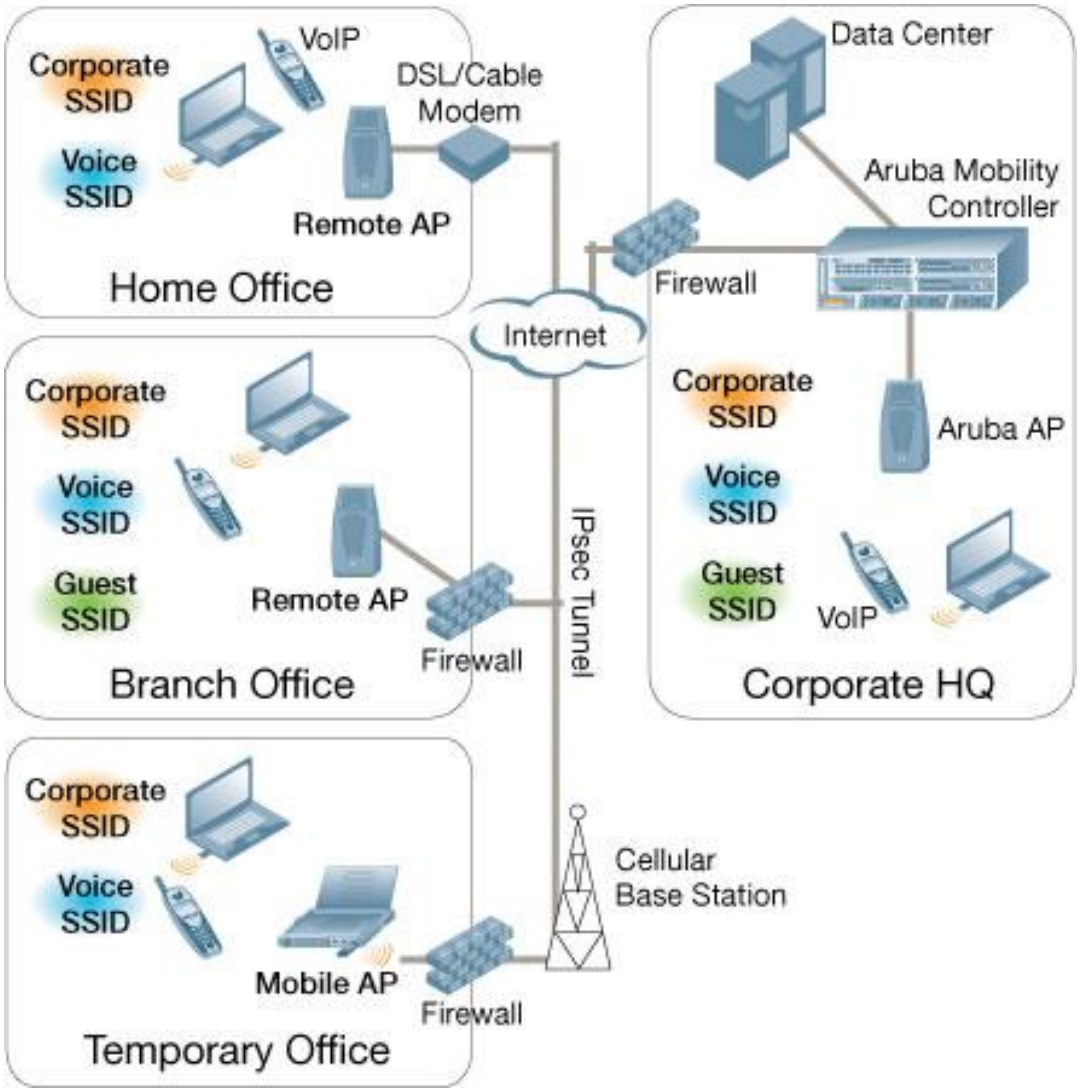
Viikkoanalyysi

Kuluneella viikolla työtehtäviä oli paljon. Tämän huomaisi hyvin Service Desk tiimimme työjonosta, joka alkoi täyttymään erilaisista työpyynnöistä. Valitettavasti oma työpanokseni viikon ajalta jäi melko vähäiseksi, koska sairastuin kesken työviikon ja loppuviikko meni kotona lepäillessä. Tämä olennaisesti rajoitti myös uusien haasteiden kohtaamista ja uusien asioiden oppimista.

Lyhyen työviikon aikana ei juurikaan mitään merkittäviä haastavia asioita tullut vastaan, josta en itsenäisesti olisi selvinnyt. Päällimmäisenä mieleeni jäi kuitenkin alkuviikosta ollut työpyyntö, josta päiväkirjamerkintöjäkin kirjoittelin. Työpyynnön suorittamisen edellytyksenä oli, että konsultoin vanhempaa kollegaani teknisiin asioihin liittyen. Minulla oli hieman epäselvyyksiä kytkimen konfigurointiin liittyen ja totesin, että oma käsitykseni asiasta tarvitsi vahvistusta kokeneemmalta asiantuntijalta. Pienen konsultoinnin jälkeen sain asiaan liittyen vahvemman käsityksen. Katsoin vielä omatoimisesti valmistajan omasta dokumentaatiosta tukea näille käsitteille.

Viime viikon analyysissä tarkastelin langattoman verkkoteknologioihin liittyvää dokumentaatiota. Tarkastelin erityisesti dokumentaatiota vianselvitykseen liittyen. Jatkan nyt asian tutkimista eri osa-alueelta. Langattomien verkkoteknologioiden käyttöön voi liittyä erinäisiä ongelmia. Ongelmat voivat esiintyä monella eri tasolla infrastruktuurissa. Kuten aiemmin jo sanottu, ongelmien selvittäminen kannattaa aina aloittaa ongelman paikantamisella.

Alla näkyvässä kuvassa(Kuva 2) näkyy esimerkki mahdollisesta langattoman verkon toteutuksesta.



Kuva 2, esimerkki langattoman verkon toteutuksesta. (Unique Micro Design 2014.)

Kuvasta ilmenee millä eri tavoin käyttäjät voivat yhdistää yrityksen resursseihin käyttäen langattomia verkkoja. Perinteiset tukiasemat ovat yleensä tavalla tai toisella suoraan kytköksissä Wlan-kontrolleriin. Kuvan esimerkissä nämä perinteiset tukiasemat on sijoitettu yrityksen pääkonttoriin. Tämä on yleisimmin käytetty tapa tuota langaton verkko käyttäjien saataville. Käyttäjiä voi olla myös sivutoimistoissa tai kotitoimistoissa. Tällöin käytetään perinteisesti etätukiasemia, jotka eroavat perinteisistä tukiasemista siinä, että ne muodostavat IPSEC VPN-tunnelin Wlan-kontrolleriin julkisen Internetin ylitse. Jotta tunneli voidaan muodostaa, täytyy yhteyden välillä oleviin palomuureihin sallia tarvittavat protokolla tunnelin muodostusta varten. Yhteyden muodostuttua etä-

käyttäjät voivat käyttää tukiaseman mainostamia langattomia verkkoja samaan tapaan kuin olisivat toimistolla.

Kuvasta puuttuu vielä yksi vaihtoehtoinen toteutustapa, jota isommissa yrityksissä on tapana käyttää. Kun yrityksellä on monia eri konttoreita, on tavallista, että eri konttoreille hankintaan paikalliset Wlan-kontrollerit, johon konttoreissa sijaitsevat tukiasemat yhdistävät ensisijaisesti. Tässä toteutustavassa kontrollerit kommunikoivat keskenään Internetin yli. Kaikki muutokset tukiasemiin tehdään pääkontrollerin kautta, jolloin tehdyt muutokset kopioituvat paikallisille kontrollereille. Tämä toteutustapa lisää myös vikasietoisuutta langattoman verkon toimintaan. Jos tukiasemat eivät saa yhteyttä paikalliseen kontrolleriin, voivat ne muodostaa yhteyden pääkontrolleriin ja langattoman verkon toiminta jatkuu.

Kontrollerien välillä voi joskus olla yhteysongelmia, jolloin mahdollinen vikasietoisuuskaan ei toimi halutulla tavalla. Valmistajalla on tällaiseen tilanteeseen muutamia perustavia ohjeita, kun aletaan selvittää yhteysongelmaa.

Mahdollisen yhteysongelman sattuessa on syytä tarkastaa sekä pääkontrollerilta, että paikalliselta kontrollerilta, että tarvittavat määrittelyt yhteyden muodostamiseksi ovat kunnossa. Paikallisella kontrollerilla tulee olla määriteltynä pääkontrollerin IP-osoite ja reititys. Pääkontrollerilla tulee olla myös vastaavat määrittelyt kunnossa. (Aruba 2014.)

Seuraavaksi on syytä tarkistaa fyysisen yhteyden toimivuus kahden kontrollerin välillä. Kontrollerilta voidaan pingata toista kontrolleria ja katsoa onnistuuko se. Tässä vaiheessa voidaan myös tarkistaa kontrollerilta, että reititys ja porttien konfiguraatiot ovat oikein. Jos niistä ei löydy vikaa, pitää vikaa tutkia verkkotopologian seuraavista laitteista, esim. reitittimet, kytkimet ja palomuurit. (Aruba 2014.)

Fyysisen yhteyden tarkastamisen jälkeen voidaan tarkastaa VPN määritykset kontrollerien välillä. Kontrollerit ottavat yhteyden toisiinsa IPsec VPN yhteyden ylitse. Kontrollerilta voidaan komentorivin kautta tarkastaa VPN yhteyden tilanne ja laittaa myös tarvittaessa debuggaus päälle. Tällöin saadaan helpommin selville, jos ongelmat liittyvät

IPsec yhteyden muodostamiseen. Yleinen ongelma tällaisessa tilanteessa voi olla, että VPN tunnelin salausavain on väärin määriteltynä kontrollereilla. (Aruba 2014.)

Viimeisimpänä vaihtoehtona on tarkastaa pääkontrollerilta, että kaikki siihen yhteyttä ottavat paikalliset kontrollerit on sallittuja ottamaan yhteyden. Jos määrittelyt on tehty oikein, tulisi pääkontrollerin nähdä kaikki siihen yhteydessä olevat paikalliset kontrollerit. Ohjelmistoversiot ovat yksi tärkeä seikka, joka tulee ottaa huomioon ongelmaa selvittäessä. Kaikkien kontrollereiden tulee olla samassa ohjelmistoversiossa, jotta ne voivat onnistuneesti kommunikoida keskenään. Mahdollinen vikatilanne voi syntyä esim. epäonnistuneen ohjelmistopäivityksen myötä, jolloin jokin kontrolleri on jäänyt eri versioon kuin muut. Mikäli ohjelmistoversioista johtuvat ongelmat voidaan rajata pois, on tällöin tarkasteltava verkossa olevien palomuurien määrityksiä. On hyvinkin mahdollista, että jokin palomuuri verkon topologiassa estää kontrollereiden keskisen kommunikoinnin. Tarvittavat palomuuriavaukset yhteyden muodostamista varten löytyvät valmistajan omasta dokumentaatiosta. (Aruba 2014.)

3.4 Työviikko 37

Maanantai 8.9

Eräs asiakkaistamme jätti sähköpostitse palvelupyynnön, jossa pyydettiin selvittelemään verkkoon liittyviä ongelmia. Asiakas ilmoitti, että heidän kumppaniinsa eivät päässeet käsiksi eräisiin tulostimiin asiakkaan MPLS-verkossa. Asiakas myös epäili, että tämä liikenne olisi estetty palomuurilla ja pyysi meitä tekemään tarvittavat korjaukset heidän verkkoonsa. Aloitin tiketin käsittelyn tarkastelemalla asiakkaan pääpalomuuria, joka sijaitsee Helsingissä. Asiakkaan MPLS-yhteydet on liitetty suoraan palomuuriin ja kaikki Internet-liikenne menee palomuurin kautta.

Aluksi tein havainnon, että palomuuri oli jaettu kahteen ns. Virtual Domainiin tai Vdomiin. Tällä tekniikalla palomuuri voidaan eritellä moniin virtuaalisiin instansseihin, jolloin ne toimivat kaikki yksityisinä palomuureina eristettynä toisistaan. Vdomeilla on omat palomuurisäännöt ja reititykset. Vdomit voidaan yhdistää toisiinsa käyttämällä Vdom-linkkiä, joka on eräänlainen ohjelmistotason virtuaalinen kytkentä. Näin teke-

mällä kaksi eri Vdomia voivat liikennöidä keskenään. Liikennettä voidaan säädellä palomuurisäännöillä ja reitityksillä.

Asiakkaan tapauksessa heidän yrityksensä kaksi eri toimintayksikköä oli tällä tekniikalla eristetty toisistaan. Joitakin verkkoja oli reititetty näiden Vdomien kautta. Tiketissä asiakas oli pistänyt kuvakaappauksen tietokoneelta tehdystä traceroute komennosta, josta kävi ilmi verkko, josta yritettiin ottaa yhteyttä erääseen verkkotulostimeen. Tarkastin toisen Vdomin reititystaulua ja löysin käytetyn lähdeverkon asiakkaan MPLS-liitännän takaa. Kohdeverkko mihin yritettiin ottaa yhteyttä, oli kuitenkin toisen Vdomin takana ja sieltä puuttui myös staattinen reitti, joka osoittaisi lähdeverkkoon. Lisäsin kyseisen verkon reititystauluun ja laitoin sen osoittamaan kohti Vdom-link porttia. Palomuurisäännöissä oli sallittu kaikki sisään tuleva liikenne toisesta Vdomista. Kävin vielä toisen Vdomin palomuurisäännöt läpi ja totesin, että sieltä puuttui pääsy kohdeverkkoon, joka sijaitsi toisen Vdomin takana. Tein palomuurisäännön, jossa sallittiin kaikki liikenne asiakkaan mainitsemasta lähdeverkosta kohdeverkkoon, jossa verkkotulostimet sijaitsivat. Muutoksien jälkeen pyysin asiakasta testaamaan yhteyden toimivuutta uudemman kerran. Otin palomuurista myös konfiguraation talteen ja tallensin sen meidän yhteiselle verkkolevylle. Tapanamme on ollut ottaa konfiguraatiot talteen jokaisen muutoksen jälkeen.

Tiistai 9.9

Tänään minulla oli vuorossa erään palomuuripalvelun käyttöönotto asiakkaalle. Service Deskissä teemme toisinaan erilaisia toimituksia uusille asiakkaille. Kyseessä oli ns. kapasiteettipalvelu, eli asiakkaalle tehdään virtuaalinen palomuurin instanssi keskitettyyn alustaan. Yhdessä alustassa voi olla kymmeniä eri asiakkaita. Palvelua myydään muutamalla eri tasolla, jolloin siihen saadaan tiettyjä lisäominaisuuksia käyttöön. Asiakas oli myös tilannut MPLS-verkon kahteen toimipisteeseensä ja nuo verkot olisi tarkoitus yhdistää palomuuriin, josta reititetään liikenne Internettiin.

Palvelun käyttöönotto oli asiakkaasta johtuen lykkääntynyt jo useamman kuukauden. Olin tehnyt konfiguraatiot palomuuria varten jo hyvissä ajoin, joten tässä vaiheessa ei omalta osaltani paljon tehtävää enää ollut. MPLS-verkon konfiguroiminen on eri yksi-

kön vastuulla. Tässä vaiheessa minun tuli vain odotella, että asentaja käy asentamassa päätelaitteet asiakkaan toimitiloihin, jotta uusi yhteys voidaan ottaa käyttöön. Asiakaan sisäverkon reititys MPLS-verkossa hoidetaan BGP protokollalla, jolloin kaikki sisäverkot mainostuvat suoraan palomuurille ja niitä ei tarvitse erikseen reitittää staattisesti. Dynaamisen reityksen toimivuus vaatii, että BGP-yhteys konfiguroidaan palomuurin ja runkoverkon reitittimen välillä. Käyttöönoton yhteydessä MPLS-verkosta vastaava yksikkö aktivoi BGP-mainostuksen palomuurille ja meidän tehtävänä on konfiguroida asiakkaan julkisen verkon mainostus palomuurille, josta se viedään taas eteenpäin kohti reunareititintä. Palomuurisääntöihin meillä on valmiina olevan lista, joka tehdään kaikille asiakkaille. Asiakas voi myös pyytää omia palomuurisääntöjä, jos sellaisille on tarvetta.

Itse käyttöönotto sujui hyvin, eikä mitään ongelmia ilmennyt. Asiakas testasi yhteyden toimivuuden vielä toimipisteestä suoraan. Asennuksen jälkeen asiakas mainitsi vielä, että heillä olisi käyttöä muutamalle VPN-tunnukselle. Asiakkaalle myytyyn tuotteeseen kuului kymmenen VPN-tunnusta ja asiakas halusi niistä ottaa käyttöön viisi. Asiakkaan määritysten mukaisesti tein heille viisi VPN tunnusta ja toimitin ne asiakkaan yhteyshenkilölle. Salasanat toimitin hänelle SMS-viestillä. Kaikkien muutosten jälkeen tein tarvittavan dokumentoinnin valmiiksi ja jatkoin muiden työtehtävien parissa.

Keskiviikko 10.9

Olin ollut muutaman tunnin töissä aamupäivällä ja sain puhelinsoiton eräältä asiakkaaltamme. Asiakas kyseli erään avoimen tiketin perään ja pyysi kiireisiä toimenpiteitä asiaan liittyen. Asia koski heidän palomuuriaan ja siellä yhtä VPN-tunnelia kolmannen osapuolen kanssa. Ongelmana oli, että liikenne tunnelin läpi ei näyttänyt toimivan asiakkaalle. Rupesin tutkimaan asiaa asiakkaan kanssa puhelimitse. Seurasin verkkoliikennettä palomuurilla, kun asiakas yritti ottaa SSH-yhteyttä resurssiin tunnelin toisessa päässä. Tämä ei kuitenkaan näyttänyt onnistuvan.

Sanoin asiakkaalle tutkivani asiaa ja palaavani takaisin, kun jotain selviää. Tarkastin läpi palomuurisäännöt ja reitityksen ja kaikki näytti olevan kunnossa. VPN-tunnelikin oli pystyssä. Katsoin myös läpi aiemmin kaappaamaani verkkoliikennettä ja totesin, että

liikenne tosiaan lähti tunneliin päin, mutta toisesta päästä ei vaan tullut vastausta kyselyyn. Ilmoitin tämän tiedon asiakkaalle. Asiakas oli ollut yhteydessä kolmanteen osapuoleen, joka hallinnoi tunnelin toista päätä ja heidän mukaansa kaikki pitäisi olla kunnossa. Asiakas ilmoitti, että liikenne pitäisi saada toimimaan mahdollisimman pian ja ehdotti, että palauttaisimme vanhemmista varmuuskopioista tunnelin konfiguraation, jolla se oli aikaisemmin toiminut.

Rupesin tutkimaan vanhoja varmuuskopioitamme ja löysin tunnelin vanhan konfiguraation. Päätin palauttaa tunnelin konfiguraation ja siihen liittyvät palomuurisäännöt suoraan komentorivin kautta kopioimalla. Tein vielä muutaman pienen muutokset ja tämän jälkeen tarkastin tilanteen. Kaikki tunnelit nousivat ylös ja palomuurisäännöt olivat oikein määritetyt, joten lähdin testaamaan yhteyden toimivuutta eräältä asiakkaan palvelimelta. Tilanne näytti vieläkin samanlaiselta, kun monitoroin liikennettä palvelimelta tunneliin. Jälleen kaikki liikenne näytti menevän tunneliin, mutta toisesta päästä ei tullut vastausta. Ilmoitin asiasta jälleen asiakkaan yhteyshenkilölle ja pyysin häntä olemaan yhteydessä kolmanteen osapuoleen, jotta he voisivat selvitellä tilanteen siellä päässä. Tässä vaiheessa asiakkaasta ei vielä kuulunut mitään takaisin ja oma työvuoroni oli loppumassa, joten annoin tiketin jatkoselvittelyn kollegani vastuulle.

Torstai 11.9

Saimme Service Deskin jonoon kiireisen palvelupyynnön ja päätin sen ottaa itselleni selvitettäväksi. Kyseessä oli erään asiakkaan vikatilanne heidän palvelimensa kanssa. Asiasta ilmoitti asiakkaan kumppani, joka ylläpiti palvelinta. Tiketissä ilmoitettiin, että asiakkaan palvelimelle oli edellisenä yönä ladattu uusia tiedostoja. Tiedostot olivat nettisivua varten, jotka pyörivät palvelimella. Tiedostojen lataaminen palvelimelle oli yöllä keskeytynyt, kun asiakas oli menettänyt yhteyden palvelimeen äkillisesti. Tämän jälkeen uutta yhteyttä ei heti saatu muodostettua uudelleen. Aamulla he saivat taas tiedostotason yhteyden palvelimeen, jossa he liittivät yhden palvelimen levyn paikalliselle koneelle. Tämä levyjako kuitenkin käyttäytyi oudosti, sillä palvelimen ylläpitäjä ei nähnyt kansiossa mitään tiedostoja mitä siellä oli aiemmin vielä ollut. Tähän ongelmaan asiakas pyysikin apua meiltä.

Aloin tutkia tilannetta ensin käymällä hieman palvelimen Windows lokia läpi, josko sieltä löytyisi mitään tuohon ongelmaan liittyen. Lokista ei kuitenkaan mitään selkeää ilmennyt ja palvelimen tilassa ei ollut havaittavissa mitään poikkeavaa. Päätin varmuuden vuoksi uudelleen käynnistää palvelimen. Tämän jälkeen tarkastelin palvelimen tilannetta uudelleen ja tarkastin myös että kaikki palvelut olivat käynnistyneet automaattisesti. Otin yhteyttä asiakkaaseen ja pyysin testaamaan yhteyttä uudelleen. Asiakas testasi levyjaon mappausta ja ilmoitti, että siinä ei vieläkään näkynyt mitään tiedostoja. Ilmoitin asiakkaalle, että tutkin vikaa lisää. Huomasin, että palvelimella oli eräs IIS-palvelinohjelmistoon liittyvä palvelu pois päältä ja päätin käynnistää sen manuaalisesti. Tämänkään ei tuntunut auttavan ongelmaan, joten päätin olla yhteydessä erääseen kollegaani, joka oli kokeneempi Windows ympäristöjen kanssa. Hänen kanssaan tutkimme yhdessä palvelinta ja sen tilaa. Testasimme itse myös levyjaon mappaamista ja emme löytäneet siitä mitään poikkeavaa.

Kollegani alkoi epäilemää, että ongelma olisikin asiakkaan paikallisella koneella, mistä he kyseistä levyjakoa yrittivät käyttää. Kollegani soitti asiakkaalle ja kyseli hieman lisätietoa tilanteesta. Kävi ilmi, että he tosiaan käyttivät levyjakoa paikalliselta palvelimelta ja siinä saattoi olla jotain vialla. Asiakasta pyydettiin uudelleenkäynnistämään heidän paikallinen palvelimensa uudelleen ja testaamaan yhteyttää jälleen. Näiden toimenpiteiden jälkeen asiakas ilmoitti, että yhteys toimii taas normaalisti ja levyjaossa näkyi taas kaikki tiedostot paikoillaan.

Viikkoanalyysi

Taas on yksi viikko kulunut lisää päiväkirjamerkintöjä ja analyysejä tehdessä. Opinnäytetyön ensimmäinen kolmas alkaa tulla täyteen. Työn edistyessä on aika käydä kolmatta viikkoanalyysiä läpi.

Viikko on taas mennyt myös työelämässä ja työtehtävät vain lisääntyvät mitä edemmäs syksyä mennään. Viimeisinkin osa asiakkaista on aktivoitunut taas kesälomakauden jälkeen. Yleensä syksymmällä asiakkailla on tapana käynnistää isompia muutosprojekteja ja tämä näkyy vahvasti koko yrityksemme työtilanteessa.

Viikkoon on sisältynyt iso määrä erilaisia tikettejä. Suurin osa ajasta viikon aikana on mennyt erilaisten vikatilanteiden selvittämiseen ja aikaa varsinaisten muutospyyntöjen suorittamiseen jäi vähemmän aikaa, kun olisin toivonut. Vikatilanteiden selvittelyt ovat pääosin liittyneet asiakkaiden tietoliikenneyhteyksiin ja palomuuripalveluihin. Kyseisten tilanteiden selvittelyssä ei sinällään ollut mitään erityisen haastavaa, vaikka joka keikka onkin yleensä erilainen. Tilanteista selviää parhaiten, kun noudattaa aina samanlaista lähestymistapaa ja pyrkii paikantamaan ongelman aiheuttajan. Tämän jälkeen ongelmien korjaaminen helpottuu huomattavasti. Viikon aikana vastaan tulleista haasteista selvittiin yhdessä eri kollegoiden kanssa.

Service Desk työskentelyssä kommunikointi kollegoiden kanssa nousee aina hyvin keskeiseen rooliin. Aina on hyvä kysyä apua kollegoilta, mikäli tilanne näin vaatii. Olen huomannut, että kyseinen menettelytapa on yleensä paljon tehokkaampaa, kuin itsenäisesti erilaisten asioiden opiskelu työaikana. Omat haasteensa tähän tuo vielä ajoittain hektinen työympäristö, jossa työpyyntöjä on paljon jonossa ja yksittäisiin keikkoihin ei voida keskittyä hetkeä kauemmin.

Tämän viikon analyysiin olen päättänyt nostaa teemaksi Service Desk työskentelyn yleisemmällä tasolla. Ajattelin tutkia sen toimintaa ja eri prosesseja kirjallisuuden näkökulmasta. Yrityksessäni Service Deskin työskentele perustuu hyvin pitkälti ITIL-viitekehyksen mukaiseen toimintaan ja aionkin kyseistä aihetta tarkastella nyt hiukan tarkemmin.

ITIL on maailmanlaajuisesti eniten käytetty viitekehys IT-palveluiden hallintaan. Se tarjoaa käytännöllisen ja asianmukaisen viitekehyksen, joka sisältää kaikki oleellisimmat asiat IT-palveluiden tuottamiseen. Keskeisimpiä alueita ovat palvelun tunnistaminen, suunnittelu, toimitus ja ylläpito. ITIL:n keskeisimpänä ajatuksena on lähtökohta, jossa IT-palveluiden päätehtävänä on tukea yrityksen ydinliiketoimintaa. (ITIL 2014.)

Palvelun elinkaari alkaa Palvelustrategia nimisellä prosessilla, jossa pyritään tunnistamaan asiakastarpeet ja vaatimukset IT-palvelulle. Seuraavaksi on vuorossa palvelunsuunnittelu ja toteutus, joka pohjautuu ensimmäiseen vaiheeseen. Lopulta päädytään itse tuotantovaiheeseen, jota seuraa palvelun seuranta -ja kehitysprosessit. (ITIL 2014.)

Service Desk itsessään ei ole prosessi vaan funktio, jonka tarkoituksena on toimia rajapintana IT-palvelun tuottajan ja asiakkaan välillä. Päätehtävänä Service Deskillä on tarjota tukea IT-palveluihin. Service Deskin keskinäisiin prosesseihin kuuluu Incident management eli häiriöhallinta ja Event management eli herätteiden hallinta. Häiriönä pidetään tapahtumaa, joka ei kuulu palvelun normaaliin toimintaan. Service Deskin tehtävänä on korjata tällaiset tilanteet ja saattaa palvelu takaisin normaalitilaan. Sama toimintapa pätee myös Event management prosessiin. (ITIL Foundation 2014.)

Yrityksessäni Service Desk funktio sijoittuu Service Operation prosessin alaisuuteen. Häiriönhallinnan lisäksi Service Deskin päivittäisiin työtehtäviin kuulu myös Service Requestit eli palvelupyynnöt. Näiksi voidaan laskea mikä tahansa normaali päivittäinen muutos asiakkaan ostamaan palveluun. Muutospyyntöjä voidaan luokitella niiden laajuuden mukaan, mikä taas huomioidaan erikseen laskutuksessa. Mittavammat muutospyynnöt eskaloidaan yleensä Service Operations tasolle, jossa muutokselle varataan tarpeelliset resurssit.

ITIL-prosessikehys on siis vahvasti mukana yritykseni päivittäisessä toiminnassa. Siitä on poimittu parhaat käytännöt ja sovellettu niitä yrityksen omiin tarpeisiin sopiviksi. Olen nyt käsitellyt alustavasti ITIL-viitekehyksen olemusta ja sen soveltamista omalla työpaikallani. Seuraavassa analyysissä aion jatkaa aiheen läpikäymistä tarkemmalla tasolla.

3.5 Työviikko 38

Maanantai 15.9

Työskentelin päivävuorossa ja sain asiakkaalta soiton erääseen aktiiviseen tikettiin. Tiketti kuului kollegalleni, joka ei juuri kyseisellä hetkellä ollut työvuorossa. Päätin ottaa asian selvittelyn itselleni. Kyseessä oli jälleen VPN-tunneliin liittyvä muutospyyntö. Asiakkaan palomuurille oltiin tekemässä uutta tunnelia kolmannen osapuolen kanssa. Kolmannella osapuolella oli hiukan erikoisempi ympäristö käytössään, sillä heidän Internet yhteytensä muodostettiin mobiililaitteella ja heillä oli dynaaminen IP-osoite käytössään. Tällöin perinteinen VPN-tunneli kahden laitteen välillä ei onnistu, koska mo-

lemmilla ei ole kiinteää IP-osoitetta, johon tunnelin muodostus terminoidaan. Asiakkaan kumppani oli ehdottanut käytettäväksi Dynamic DNS pohjaista ratkaisua, missä heidän laitteensa käy jossain julkisessa palvelussa päivittämässä IP-osoitteensa ja palvelu antaa IP-osoitteelle vastaavan DNS-nimen. Tämä nimi DNS-nimi oli toimitettu meille aiemmin ja kollegani oli sen määrittänyt VPN tunnelin asetuksiin. Puhelun aikana, koitimme nostaa VPN tunnelin ylös, mutta se ei näyttänyt onnistuvan. Katsoin samalla omalta palomuuriltani lokia, josko sieltä olisi löytynyt jotain vikaan liittyvää.

Kävimme asiakkaan kanssa läpi puhelimessa molempien puolten VPN asetukset ja tarkastimme, että määritykset olivat vastaavat. Näistä ei löytynyt mitään vikaa, mutta tunneli ei vaan noussut ylös, koska neuvottelu ei onnistunut. Aloin myös monitoroida verkkoliikennettä asiakkaan suuntaan ja ainakin ICMP-paketit näyttivät menevän perille. Seuraavaksi tutkin UDP liikennettä portissa 500, jossa VPN-yhteyden neuvottelu suoritetaan. Monitorista näin, että liikennettä takaisinpäin ei koskaan tullut.

Tässä vaiheessa ehdotin asiakkaalle, että vaihdetaan tunnelin määritys Dialup-tyyppiseksi. Tällä määritystavalla vastapään IP-osoitetta ei tarvitse määrittää ja VPN tunnelin muodostus aloitetaan aina toisesta päästä. Tein vaadittavat muutokset palomuuriin ja testasimme toimintaa uudelleen. Tällä kertaa VPN tunneli muodostui saman tien ja liikennekin tunnelin läpi alkoi muodostua. Asiakas oli hyvin tyytyväinen valitsemaani ratkaisuun. Sovimme asiakkaan kanssa, että he palaavat seuraavana päivänä asiaan, jos tunneliin pitäisi tehdä vielä jotain hienosäätöä.

Tiistai 16.9

Tänään olin varannut työpäivästäni suurimman osan minulle allokoitujen toimisten tekemiseen. Päätin, että toimitusten tekemiseen pitää varata useampi tunti aikaa, että ehdin tekemään tarvittavat toimenpiteet määräajassa. Sain toimitukset äkillisesti omalle vastuulleni ja tekemistä oli jo viime viikolta kertynyt jonkin verran.

Toimitukset koskivat tukiasemien lähettämistä muutamalle eri asiakkaalle. Hyvä puoli kyseisissä toimituksissa oli se, että niissä ei konfiguraation osalta tarvinnut tehdä toimenpiteitä. Aloitin urakan suuntaamalla meidän laitevarastolle, joka sijaitsee vähän

matkan päästä toimistolta. Varastolle tulevat kaikki uudet laitteet, joita asiakkaille lähetetään. Menin varastolle ja etsin sieltä minulle allokoidut paketit, jotka sisälsivät tukiasemia, PoE-adaptereita ja kiinnitystelineitä tukiasemille. Otin paketit mukaani ja lähdin takaisin toimistolle jatkamaan hommia.

Toimistolla avasin paketit ja rupesin käsittelemään tukiasemia. Ennen kuin tukiasemat voidaan lähettää asiakkaalle, ne täytyy merkitä tarralla asiakkaan antaman tunnisteen mukaan. Näin asiakkaat pystyvät tunnistamaan kunkin tukiaseman sen nimen mukaan. Tukiasemien merkitsemisen ohella niistä otetaan talteen sarjanumerot ja MAC-osoitteet, jotka syötetään laitetietokantaan. Jokaisesta tukiasemasta tehdään oma laitekortti ja sen yksilölliset tiedot syötetään järjestelmään. Näiden toimenpiteiden jälkeen pakkasin tukiasemat ja oheistarvikkeet takaisin pahvilaatikoihin ja aloin varaamaan niille noutotilausta. Sain tilaukset tehtyä valmiiksi ja vein paketit talon aulaan odottamaan noutoa. Tämän jälkeen jatkoin vielä hetken muiden työtehtävien tekemistä ennen päivän loppua.

Keskiviikko 17.9

Tänään oli jälleen vuorossa toimitusten tekemistä. Minulla oli yksi palomuuritoimitus, joka piti saada lähtemään perjantaihin mennessä. Aikaa ei siis ollut paljoa, joten ryhdyin hommiin heti työpäivän alkupuolella, kun muut hommat antoivat periksi. Toimitukseen kuului konfiguroida ja lähettää matkaan palomuurit. Ne olivat menossa eräälle isommalle asiakkaalle, jolla oli uusi toimipiste Etelä-Koreassa.

Aloitin hommat avaamalla pakkaukset ja kytkin palomuurit työpisteeseeni. Kävin myös tulostamassa itselleni eräänlaisen muistinlistan, joka on luotu palomuuritoimituksia varten. Tätä käyttämällä tulee varmasti tehtyä kaikki tarvittavat toimenpiteet toimitukseen liittyen. Käynnistin palomuurit ja kytkin ne saman tien toisiinsa Ethernet kaapelilla. Kyseiset palomuurit oli tarkoitus konfiguroida klusteriksi, jolloin ne toimivat yhtenä loogisena yksikkönä. Yksi palomuuri toimii Master-noodina ja toinen toimii Slave-noodina. Palomuurit konfiguroidaan ns. Active-Passive asetukseen, jolloin Master-noodi käsittelee kaiken liikenteen palomuurilla. Vikatilanteessa, jos Master-noodi jostain syystä putoaa klusterista, rupeaa Slave-noodi prosessoimaan kaiken liikenteen. Täl-

löin verkon liikenteessä pitäisi näkyä vain hyvin pieni katkos. Tämä asetelma vaatii verkkoympäristöltä sen, että palomuurit kytketään kytkimeen, jolloin liikenne ei katkea jos toinen palomuuri putoaa pois pelistä.

Konfiguroin palomuurille klusterin toimintaan, jotta muutokset menevät automaattisesti molemmille noodeille. Tämän jälkeen asetin palomuurin eri porteille IP-osoitteet, jotka asiakas oli meille aiemmin toimittanut. Palomuuriin tuli staattinen julkinen IP-osoite, sillä tulevassa toimipisteessä on oma Internet-yhteys. Kyseisen asiakkaan menettelyihin kuuluu, että kaikki etätoimipisteet liikennöivät kaiken liikenteen aluekohtaisen pääpalomuurin kautta VPN-tunnelin välityksellä. Tätä asetelmaan varten asetin palomuurille siis VPN-tunnelin ja määrittelin sinne kohdeosoitteeksi asiakkaan palomuurin, joka tässä tapauksessa sijaitsee Kiinassa. Palomuurisäännöt tällaisessa asetelmassa on hyvin helppo tehdä, koska liikenne menee VPN-tunnelin kautta. Tein palomuurisäännöt, jotka sallivat kaiken liikenteen ulos -ja sisäänpäin VPN-tunnelin kautta.

Seuraavaksi siirryin määrittämään reitityksiä. Asiakkaan määrittelyihin kuului, että palomuurilla ajetaan BGP-reititystä VPN-tunnelin ylitse. Palomuurilla BGP-naapuriksi määritellään Kiinan päässä oleva palomuuri. Reititys verkossa toimii niin, että palomuuri mainostaa VPN tunneliin omaa sisäverkkoaan ja kaikki muut yrityksen sisäverkot mainostuvat pääpalomuurin kanssa. Näin kaikista toimipisteistä voidaan liikennöidä toisiin ja ylimääräistä määrittelyä reitityksiä varten ei tarvita.

Reitityksien jälkeen konfiguroin palomuurille kaikki meidän omaa hallintaa varten oleelliset asiat, kuten palomuurien nimet, SNMP-asetukset valvontaa varten sekä VPN-tunnelit meidän omasta palomuurista. Päivitin palomuurien ohjelmistot myös uusimpaan versioon. Tarkastelin muistilistaa ja totesin, että kaikki tarvittavat toimenpiteet oli tehty tässä vaiheessa, joten siirryin valmistelemaan palomuurien lähetystä maailmalle.

Pakkasin palomuurit ja kaikki niiden sisältämät oheistarvikkeet takaisin laatikoihin ja pakkasin ne huolellisesti. Tämän jälkeen siirryin tekemään noutotilausta paketeille ja kun se tuli valmiiksi, vein paketit toimiston aulaan odottamaan noutoa.

Torstai 18.9

Olin päivävuorossa töissä ja minulle oli allokoitu konferenssipuhelu asiakkaan kanssa klo. 9.00 aamulla. Puhelun kestoksi oli mitoitettu yksi tunti ja puhelun aikana oli tarkoitus selvittää yhteysongelmia heidän verkossaan. Liityin puheluun yhdeksän aikaan, kuten oli sovittu. Kyseessä oli Lync-kokous, johon liityin työasemallani. Äänet sain käyttööni soittamalla puhelimella kokouksen numeroon.

Puhelun alussa kaikki osapuolet esittelivät itsensä ja kävimme läpi agendan. Asiakas ilmoitti, että heillä oli muutamia eri kohdeosoitteita verkossaan, johon he yrittivät saada yhteyttä. Minun tehtäväni oli monitoroida liikennettä palomuurilla ja ilmoittaa havainnoistani asiakkaan edustajille. Tämän jälkeen oli tarkoitus käydä asiakkaan teknisen yhteyshenkilön kanssa tarvittavat palomuurisäännöt läpi ja tehdä niitä tarpeen mukaan. Puhelussa oli mukana asiakkaan toinen kumppani, joka myös seurasi tilannetta heidän palomuurillaan ja teki vastaavia muutoksia tarpeen mukaan.

Aloitimme ensimmäiset testauksen, jossa asiakas testasi etätyöpöytäyhteyttä muutamaan eri palvelimeen heidän sisäverkostaan. Näin palomuurin monitorista heti miten liikenne meni ja huomasin, että sitä ei ollut sallittu jo olevissa palomuurisäännöissä. Kävimme tämän asiakkaan kanssa läpi ja päätimme lisätä yhteyden sallituksi. Seuraavaksi asiakas testasi samaa yhteyttä VPN-yhteyden yli. Tässäkin ilmeni sama asia, eli RDP-liikennettä ei ollut sallittu palomuurilla Päätimme asiakkaan kanssa, että tämäkin liikenne voidaan sallia.

Seuraavaksi asiakas testasi sisäverkosta jälleen SQL-yhteyksiä muutamille palvelimille heidän verkossaan. Tämä olikin hieman haastavampi selvittää, koska yhteys näytti käyttävän useita eri portteja TCP -ja UDP protokollalla. Kävimme näitä läpi hetken aikaa asiakkaan kanssa ja teimme kokoelman porteista, jotka päätettiin avata palomuurilla. Avausten jälkeen asiakas testasi toimintaa ja yhteydet näyttivät toimivan halutulla tavalla.

Olimme edistyneet ongelmien selvittelyssä hyvin asiakkaan kanssa, mutta aika näytti loppuvan kesken. Kartoitimme jäljelle jääneet ongelmakohdat ja asiakkaan yhteyshenkilö ilmoitti tilaavansa tarvittavat palomuurimuutokset myöhemmällä ajankohdalla. Näiden toimenpiteiden jälkeen kiitimme toisiamme avusta ja lopetimme konferenssipuhelun.

Perjantai 19.9

Tänään minulla oli sovittuna kahden aikaa iltapäivällä eräs muutostyö. Yksi asiakas oli tehnyt tilauksen, jossa pyydettiin kasvattamaan keskusmuistin kokoa kahteen heidän virtuaalipalvelimeensa. Asiassa oli ensin oltu yhteydessä myyjiin, jotta saatiin hinnat sovittua tarvittaville toimenpiteille. Asiakas oli myös tiedustellut yksityiskohtia muutoksesta. Heille oli ilmoitettu, että muistinkasvatusta varten palvelimet tulee sammuttaa ensin. Koska asiakkaan palvelimet olivat tuotannossa ja niillä ajettiin kriittisiä sovelluksia, oli asiakas halunnut tehdä muutokset päiväsaikaan hallitusti, jotta he voisivat testata palvelimien ja palveluiden toimivuuden muutoksien jälkeen.

Vähän ennen kello kahta soitin asiakkaan yhteyshenkilölle, joka oli tilauksen tehnyt ja ilmoitin, että olin valmis tekemään muutokset. Pyysin asiakasta sammuttamaan palvelimelta kaikki tarvittavat palvelut. Tämän jälkeen sammutin koneen käyttöjärjestelmän kautta. Muistinlisäys tehtiin virtuaalipalvelimen hallinnan kautta, jossa muistinmääräksi asetettiin kahdeksan gigatavua vanhan neljän gigatavun sijasta. Tämän jälkeen muutokset tallennettiin ja kone käynnistettiin. Pyysin asiakasta puhelimessa testaamaan, että hän pääsi etäyhteydellä koneeseen kiinni ja kaikki palvelut käynnistyivät normaalisti.

Tämän jälkeen siirryimme tekemään muutoksia toiseen palvelimeen. Tässä päätimme mennä samalla menettelyllä, että asiakas sammutti ensin kaikki oleelliset palvelut ja tämän jälkeen sammutin itse virtuaalikoneen. Tähän koneeseen muistia kasvatettiin saman verran. Muutoksen jälkeen käynnistin koneen ja asiakas taas testasi toimivuuden. Kaikki näytti toimivan normaalisti ja asiakas oli tyytyväinen muutoksiin. Lopetimme puhelun ja kuittasin järjestelmässä tiketin suoritetuksi.

Viikkoanalyysi

Kulunut viikko kului enimmäkseen erilaisten toimitusten osalta ja aikaa palvelupyyntöjen suorittamiseen ei juurikaan jäänyt. Alkuviikosta tekemäni tukiasemien toimituksen olivat helppoja, koska niissä ei toimenpiteitä juuri tarvittu. Tukiasemat vain piti dokumentoida ja tämän jälkeen lähettää kohteeseen.

Loppuviikosta pääsin tekemään palomuuritoimitusta, jossa pääsinkin jo tekemään enemmän toimenpiteitä. Palomuuri piti konfiguroida alusta loppuun ja lähettää maailmalle. Mielestäni tämä oli mieluisaa työtä ja mukavaa vaihtelua päivittäisille työtehtäville. Olin jo aiemmin tehnyt muutamia toimituksia, joten teknisesti tämä toimitus ei tuottanut minulle mitään haasteita. Kävin kaikki tarvittavat muutokset läpi järjestelmällisesti, jotta mitään vaihetta ei jäisi tekemättä.

Viime analyysissä kävin läpi ITIL-viitekehystä. Nyt olisi tarkoitus tarkastella miten se näkyy omassa työnkuvassani. ITIL on laajalti käytetty viitekehys ICT-alalla ja soveltuu erinomaisesti yrityksille, jotka tarjoavat Service Desk muotoista IT-palveluita.

ITIL-viitekehyksen avulla voidaan saavuttaa seuraavia hyötyjä prosessien elinkaaren aikana.

Service Strategy

- IT-palveluiden arvon tunnistaminen liiketoiminnan tukena
- Kustannuksien parempi suunnittelu ja ylläpito
- Palvelun vaatimuksen, resurssit ja kustannukset menevät käsi kädessä liiketoiminnan kanssa

(The Stationary Office 2014.)

Service Design

- IT-palvelun suunnitteleminen liiketoiminnan tueksi
- Palvelu, joka on suunniteltu vastaamaan siihen laitettuja sijoituksia
- Palvelun tasaisuus ja ennalta-arvattavuus.

(The Stationary Office 2014.)

Service Transition

- Muutokset palveluun ovat hallittuja
- Vähemmän katkoksia palvelussa

(The Stationary Office 2014.)

Service Operation

- Jatkuva IT-palvelu, joka palvelee liiketoiminnan elinehtoja
- IT-palvelut hallitaan keskitetysti ja luotettavasti
- Vastuullinen ja tehokas toiminta häiriöiden selvittämisessä

(The Stationary Office 2014.)

Continual service improvement

- Palvelun jatkuvat kehitys aiemman kokemuksen avulla
- IT-palveluiden muuntautuminen liiketoiminnan tarpeisiin
- Uuden teknologian hyödyntäminen tilanteen mukaan

(The Stationary Office 2014.)

Yrityksessäni ITIL-viitekehystä sovelletaan asiakkaiden palveluissa aina suunnittelusta ylläpitoon ja kehitykseen asti. Käytämme viitekehystä myös tiiviisti omissa sisäisissä prosesseissamme. Viimeisimpänä konkreettisena esimerkkinä tulee mieleeni prosessi, jonka otimme sisäisesti käyttöön reilu vuosi sitten. Kyseessä oli Service Improvement tyyppinen prosessi, jossa kuka vain yrityksen työntekijöistä sai antaa kehitysideoita kaikkiin tarjoamiimme palveluihin ja järjestelmiin.

Ehdotukset kirjattiin meidän omaan tikettijärjestelmään, jonne annettiin tarkka kuvaus parannusehdotuksesta. Tämän jälkeen Service Development tiimimme kävi läpi säännöllisesti kaikkia ehdotuksia ja nosti niitä esille. Viimeisenä vaiheena nämä käytiin läpi palvelutuotannon esimiehen kanssa ja samalla päätettiin otetaanko ehdotettu parannus käyttöön vai ei. Prosessin käyttöönoton jälkeen kehitysideoita alkoi ilmestymään järjestelmään aika lailla. Joitakin niistä otettiin käyttöön tuotannossa.

Yrityksemme tuottamissa palveluissa voi myös nähdä eräänlaisen viittauksen ITIL-viitekehykseen. Tuottamamme palvelut ovat lisäarvopalveluita, joiden ensisijainen tehtävä on tehostaa asiakkaan ydinliiketoimintaa. Tämä on myös keskeinen lähtökohta ITIL-viitekehyksessä, jossa IT-palveluilla pyritään tukemaan yrityksen liiketoimintaa.

Kaikki uudet asiakkaille myydyt palvelut menevät tarkasti prosessien mukaan. Koko homma lähtee liikkeelle, kun asiakkaalle myydään palvelu. Lähes poikkeuksetta kaikki palvelumme ovat asiakaskohtaisesti mukautettuja sopimaan kyseisen asiakkaan ympäristöön ja toimintamalliin. Tästä päästään palvelun suunnitteluun, jossa myydyt palvelut pyritään saattamaan mahdollisimman lähelle asiakkaan tarpeita. Suunnittelussa tehdään tiiviisti yhteistyötä teknisten asiantuntijoidemme kanssa, jotta asiakaskin saa tarkemman kuvauksen palvelusta, jota ovat ostamassa.

Seuraava vaihe on käyttöönoton suunnittelu, jossa pyritään löytämään paras mahdollinen ajankohta palvelun käyttöönotolle. Tähän sovitaan myös tarkka suunnitelma tehtävistä muutoksista ja varataan tarvittavat resurssit muutokselle, jotta palvelun käyttöönotto olisi asiakkaan kannalta mahdollisimman sujuva.

Palvelun käyttöönoton jälkeen se on hetken aikaa Testing Period nimisessä statuksessa, jolloin asiakas voi ilmoittaa mahdollisista ongelmista tai parannuksista palveluun. Kun testiaika on hyväksytty, siirtyy palvelu varsinaisesti tuotantoon. Tällöin voidaan ITIL-viitekehyksessä puhua Service Operation vaiheesta palvelun elinkaaressa.

Tässä oleellisimpana funktiona tulee esiin Service Desk, joka toimii asiakkaan ensisijaisena rajapintana kaikkiin asiakkaan palveluihin liittyen. Service Desk vastaa palvelun päivittäisestä toiminnasta, johon kuuluvat Incident Management ja Service Request prosessit. ITIL-viitekehystä soveltaen asiakkaan palveluihin on myös sisällytetty SLA-palvelutasosopimus, joka kuvaa tasoa, jolla palvelun tulee toimia päivittäin. Service Desk vastaa ensisijaisesti siitä, että palvelu toimii SLA-sopimuksessa määritetyllä tavalla, johon kuuluu esim. palvelun saatavuus. Jos palvelussa esiintyy vikaa, pyritään se saamaan toimintaan mahdollisimman nopeasti, jotta SLA-sopimuksessa määritetyt ehdot täyttyvät. Mikäli asiakkaalla esiintyy samassa palvelussa usein ongelmia, voidaan

tässä soveltaa Problem Management prosessia, jossa Service Desk kirjaa ylös asiakkaalla ilmenneet ongelmat ja tämän jälkeen asian selvittely eskaloidaan Service Operations tiimille tutkittavaksi.

ITIL-viitekehyksen mukainen jatkuva palveluiden kehitys näkyy myös aktiivisesti asiakkaiden palveluissa. Asiakkaiden kanssa käydään säännöllisesti palavereita, joissa käydään läpi viimeaikaiset tapahtumat palveluihin liittyen. Näissä tapaamisissa asiakas voi antaa suoraa palautettua palveluihin liittyen. Asiakkaalla on myös mahdollisuus ehdottaa parannuksia heille tarjottavaan palveluun. Asiakkaan esittämiä toiveita pyritään aina toteuttamaan mahdollisuuksien mukaan.

ITIL:in soveltaminen näkyy myös yrityksemme sisäisissä prosesseissa. Kaikille tärkeimmille prosesseille löytyy Service Owner roolin omaava henkilö, joka vastaa, että prosessia noudatetaan sovitun mukaisesti. Lisäksi kaikki muutokset järjestelmissä ja palveluissa pyritään tekemään ITIL-viitekehyksen parhaiden käytäntöjen mukaisesti.

Analyysin loppuun päätin hieman tarkastella lähteitä siitä, mitä hyötyjä ITIL-viitekehyksen soveltaminen IT-palveluiden tuottamisessa on. Eräs IT-konsultointifirma mainitsee viisi eri hyötyä ITIL-viitekehyksen käyttöönottamiseen liittyen.

ITIL on käytössä maailmanlaajuisesti ja se soveltuu kaiken tyyppisiin ja kokoisiin organisaatioihin. ITIL itsessään jo koostuu IT-alan parhaista käytännöistä ja näin sitä voidaan soveltaa missä tahansa organisaatiossa. Toisena seikkana on IT:n ja liiketoiminnan yhtenäistäminen. Kun liiketoiminnan oleelliset vaatimukset havainnoidaan, pystytään näihin kehittämään niitä tukevia IT-palveluita. Kolmantena seikkana pidetään vähennettyjä resurssien tarpeita. ITIL-viitekehyksen ansiosta palveluiden keskeytymättömyys voidaan taata luotettavammin. Toipuminen mahdollisista palveluiden vikatilanteista hoituu tehokkaammin, kun niiden ratkaisemiseksi löytyy selvä prosessi. Palvelun laadun paraneminen on myös yksi oleellinen asia, jota voidaan ITIL:in avulla parantaa. Ympäristöjen heikkoudet voidaan paikantaa ja niihin voidaan ennaltaehkäisevästi kehittää parannusehdotuksia. Viimeisimpänä tekijänä pidetään palvelun johdonmukaisuutta.

ITIL tarjoaa työkalut palveluiden jatkuvaan valvontaan, arviointiin ja kehitykseen. (Ashford Global 2014.)

3.6 Työviikko 39

Maanantai 22.9

Olin ottanut itselleni tiketin meidän järjestelmästä, koska se oli ollut jonossa jo jonkin aikaa. Tiketti oli eräälle isolle asiakkaalle ja se koski heidän palomuurejaan muutamissa toimipisteissä. Asiakkaalla oli toimipisteissä kaksi eri palomuuria, mutta normaalista käytännöstä poiketen palomuurit eivät olleet klusteroituja, vaan toinen palomuureista toimi käytännössä varalaitteena, jota säilytettiin hyllyllä. Nämä kyseiset varalaitteet olivat olleet hyllyillä käyttämättömänä jo hieman pidemmän aikaa ja sillä välin aktiivisessa käytössä olleisiin palomuureihin oli tehty hieman muutoksia.

Hyllyssä olleet palomuurit eivät siis olleet käytössä, joten muutoksia ei ollut synkronoitu varalaitteisiin. Näiden konfiguroiminen yksitellen joka toimipisteellä olisi haastavaa saada aikaan. Tätä varten tarvittaisiin jonkinlainen etäyhteys asiakkaan koneelle, joka kytkettäisiin taas suoraan palomuuriin. Olimme ehdottaneet asiakkaalle aiemmin, että yksi hyvä ratkaisu olisi lähettää kaikki tällaiset palomuurit meille keskitetysti ja tämän jälkeen me määrittelisimme varalaitteeet vastaamaan aktiisivia palomuureja toimipisteillä. Asiakas oli hieman pidemmän ajan jälkeen saanut palomuurit toimitettua meille keskitetysti. Palomuureissa oli merkitty tarkasti, että missä toimipisteessä ne sijaitsivat, jotta konfiguraation laittaminen oikein olisi helpompaa. Laitteitta oli yhteensä kuusi kappaletta.

Aloitin urakan avaamalla paketin, jossa kaikki laitteet olivat ja otin kasan päältä pari ensimmäistä palomuuria ja vein ne työpisteelleni. Otin palomuurit yksitellen käsittelyyn ja kytkin niihin virtalähteen, konsolikaapelin ja Ethernet kaapelin. Ensimmäiseksi käynnistin palomuurin ja katsoin konsoliyhteyden kautta, että se käynnistyi normaalisti ja palomuurin nimi vastasi paperissa lukenutta nimeä. Tämän jälkeen katsoin meidän tietokannasta laitteeseen asetetun käyttäjänimen sekä salasanan, jotta pääsin kirjautumaan sisään palomuurin hallintaan. Samalla aukaisin vastaavan laitteen joka oli käytössä asi-

akkaan toimipisteellä. Aloitin vertailemaan konfiguraatioita ja joidenkin palomuurien kohdalla huomasin, että ohjelmistoversiot eivät täsmänneet. Tästä syystä päätin päivittää palomuurien ohjelmiston vastaamaan aktiivisten palomuurien konfiguraatiota.

Päivitysten jälkeen kirjauduin asiakkaan käytössä oleville palomuureille eri toimipisteillä ja otin niiden konfiguraatiot talteen. Tämän jälkeen latasin nämä kyseiset konfiguraatiot pöydälläni oleviin palomuureihin. Tarkastin vielä, että palomuurit lähtivät toimimaan oikein konfiguraation lataamisen jälkeen ja sitten laitoin ne takaisin pakettiin. Toistin samat toimenpiteet kaikille paketissa olleille palomuureille. Tämän jälkeen tiedustelin asiakkaalta osoitteen johon palomuurit tulisi lähettää. Asiakas ilmoitti yhden osoitteen johon laitteet tulisi toimittaa, josta asiakas lähettää ne eteenpäin lopullisille sijoituspaikoilleen. Tiedon saatuani aloitin valmistelemaan laitteiden lähetystä.

Tiistai 23.9

Olin työskentelemässä iltavuorossa ja noin kello neljän maissa sain eräältä asiakkaan yhteyshenkilöltä puhelinsoiton. Asiakas ilmoitti, että heidän muutamassa toimipisteessään ei toiminut langaton verkko. Ilmoituksen mukaan toimipisteiden tukiasemissa ei palanut led-valot, jotka osoittavat langattoman verkon taajuutta. Asiakas pyysi asian pikaista tutkimista.

Katsoin ympärilleni ja huomasin, että toimistolla oli vielä yksi kokeneempi asiantuntija paikalla, joten pyysin hänet mukaan vianselvitykseen. Aloimme tarkastella tilannetta ensin asiakkaan langattoman verkon Controllerilta. Teimme havainnon, että se oli täysin toimintakunnossa, mutta kaikki siihen kytköksissä olleet tukiasemat, joita oli reilu sata kappaletta, olivat alhaalla. Tämä siis viittasi tosiaan yhteysongelmaan tukiasemien ja Controllerin välillä. Yhteys näytti kulkevan asiakkaan MPLS verkon lävitse ja suoraan emme osanneet sanoa missä kohtaa vika oli.

Aloimme tutkia asiaa eri asiakkaan laitteilta, jotka käyttävät MPLS-yhteyttä liikennöintiin. Totesimme, että normaalisti liikenteen pitäisi tulla asiakkaan pääpalomuurin läpi MPLS-verkosta. Monitoroimme liikennettä Controllerin suuntaan, mutta mitään ei nä-

kynyt. Aloimme epäilemään, että vika olisi jossain kohti asiakkaan verkkoa ennen palomuuria.

Kävimme läpi vielä muutaman laitteen ja eräällä toisella Suomen palomuurilla näimme hieman outoa käyttäytymistä. Siellä näkyi, että kaikki lähes koko asiakkaan sisäverkon liikenne näytti tulevan kyseiselle palomuurille ja tämä ei ollut haluttu tilanne. Näimme, että palomuurilla oli reititetty staattisesti iso A-luokan sisäverkko osoittamaan asiakkaan DMZ-vyöhykkeelle. Palomuuri oli konfiguroitu jakamaan staattiset reittinsä BGP-protokollalla ja näin se levisi koko asiakkaan sisäverkkoon. Selvitimme hieman mistä tämä johtui ja selvisi, että eräs kollegamme oli tämän reitityksen tehnyt muutamaa tuntia aiemmin asiakkaan toisen yhteyshenkilön pyynnöstä toisessa tiketissä. Tässä ei kuitenkaan ollut huomioitu, että se voisi sotkea koko asiakkaan sisäverkon. Poistimme kyseisen reitityksen sekä lisäsimme asiakkaan pääpalomuurin BGP-reititykseen mainostuksen Controllerin käyttämästä verkosta, jotta se näkyisi kaikille asiakkaan laitteille ensisijaisesti.

Tämän jälkeen katsoimme tilannetta Controllerilta ja näimme, että tukiasemat rupesivat nousemaan linjoille ja yhteydet toimimaan. Ilmoitin asiakkaalle tilanteesta ja hän oli tyytyväinen tilanteeseen. Päätimme sulkea keikan näillä tiedoilla.

Keskiviikko 24.9

Olimme saaneet Service Deskiin muutaman tiketin Service Operations tiimiltä. Tiketit oli merkitty Maintenance-merkinnällä meidän järjestelmässä ja ne koskivat erään asiakkaan etäyhteyslaitteiden päivitystä. Laitteet ovat merkiltään Juniperin SA-sarjan laitteita, joita käytetään SSL-VPN yhteyksiin. Asiakkaalla on käytössään kolme kyseistä laitetta, joista Suomessa sijaitseva on itseasiassa virtuaalinen versio laitteesta. Laite pyörii VMWare virtuaaliympäristössä virtuaalisena instanssina. Otin tuon kyseisen laitteen päivityksen itselleni, koska huomasin, että tässä pääsisi tekemään joitakin uusia asioita. Normaalisti laiteet päivitetään niiden web-käyttöliittymän kautta yksinkertaisesti, mutta tämän laitteen kanssa prosessi oli hieman erilainen, johtuen muutamista ongelmista virtualisoinnin kanssa kyseisessä ohjelmistossa.

Kävin toimenpiteitä läpi hieman kokeneemman kollegan kanssa ja yhdessä katsoimme, että mitä kaikkea päivitykseen liittyen tulisi tehdä. Päädyimme ratkaisuun, että tehdään uusi virtuaalinen laite ja lisätään siihen olemassa olevan konfiguraatio varmuuskopioista ja tämän jälkeen päivitetään laitteen ohjelmisto viimeisimpään versioon.

Aloitin toimenpiteet luomalla uuden virtuaalikoneen ja tämä tehtiin valitsemalla Juniperin oma levytiedosto meidän verkkolevyltä. Tämän jälkeen määrittelin uuden virtuaalikoneen sopiviin asetuksiin. Virtuaalikoneelle määritettiin keskusmuistin kooksi kaksi gigatavua ja siihen asetettiin kaksi suoritinydintä. Laitteelle annettiin sopiva nimi ja määriteltiin virtuaaliset verkot, jota laite tulee käyttämään. Nämä määriteltiin samoiksi, kuin asiakkaan nykyisessä virtuaalikoneessa, mutta portit laitettiin alas, jotta ne eivät häiritse nykyisen laitteen toimintaa. Laitteen luomisen jälkeen käynnistin ja aloitin konfiguroimisen laitteen komentoriviltä. Laitteelle tuli määrittää admin käyttäjätunnus sekä uusi IP-osoite laitteen hallintaa varten. Näiden määrittelyiden jälkeen pääsin laitteeseen käsiksi web-pohjaisen käyttöliittymän kautta. Täällä menin laitteen huoltoasetuksiin ja tiputin sisään asiakkaan konfiguraation, joka oli meillä tallessa verkkolevyllä.

Muutoksien jälkeen tarkastelin, että kaikki näytti normaalilta. Kaikki näytti olevan kunnossa joten päivitin seuraavaksi laitteen ohjelmistoversion tuoreempaan. Tässä vaiheessa laite alkoikin olemaan valmis käyttöönottoa varten. Itse käyttöönotto menisi hyvin yksinkertaisesti, sillä nykyisestä laitteesta täytyisi vain sammuttaa kaikki portit ja tämän jälkeen uudessa virtuaalikoneessa kaikki portit taas nostettaisiin ylös. Muutoksia ei kuitenkaan vielä voitu tehdä, koska asiakkaan kanssa oli sovittu että huoltokatko pidetään seuraavana päivänä klo. 16.00 jälkeen. Laitoin keikan siis odottamaan itse toteutusta.

Torstai 25.9

Service Deskillämme oli eräs asiakkaan vikailmoitusta koskeva tiketti auki. Tiketti oli kollegallani, joka oli yövuorossa ja asiakas oli tähän useaan otteeseen soitellut ja kysellyt päivitystä. Asiakkaan Yhdysvalloissa sijaitseva palomuuriklusteri oli mennyt alas ja yhteyttä siihen ei enää saatu. Asiakkaan yhteydet yrityksen verkkoon eivät myöskään siis toimineet. Asiakkaan oma Help Desk soitteli meille säännöllisin väliajoin ja pyysi, että asia ratkaistaisiin mahdollisimman pian.

Olimme pyytäneet loppukäyttäjää toimipisteellä käynnistämään uudelleen palomuurit sekä reitittimen, mutta tämän ei ollut auttanut asiaan. Soitin vielä käyttäjälle ja pyysin häntä tarkastamaan, että kaikki kytkennät ovat paikallaan. Kaikki näytti päällisin puolin olevan kunnossa. Seuraavaksi yritimme saada jonkinlaisen yhteyden palomuuriin. Pyysin asiakasta kytkemään kannettavan tietokoneen kiinni palomuuriin ja muodostamaan etäyhteyden, jotta pääsisimme hänen koneelleen kiinni. Käyttäjällä ei kuitenkaan ollut oikeuksia asentaa ohjelmia koneelleen, joten jouduimme pyytämään asiakkaan Help Deskiä hoitamaan tämän asennuksen. Asennus saatiin tehtyä onnistuneesti, mutta emme silti näyttäneet saavan minkäänlaista yhteyttä palomuuriin vaikka se oli suoraan kytketty tietokoneeseen.

Päädyimme seuraavaksi ratkaisuun, että asiakkaan tulisi seuraavaksi hommata Mini USB-kaapeli, joka voitaisiin kytkeä palomuurin hallinnointia varten. Tämä oli viimeinen vaihtoehto mitä oli mahdollista käyttää. Hieman myöhemmin toimipisteen henkilö oli saanut hommattua kyseisen kaapeli, jotta yhteys palomuurille voitaisiin mahdollisesti muodostaa. Aloitimme puhelun asiakkaan Help Deskin ja toimipisteen loppukäyttäjän kanssa. Pyysin käyttäjää yhdistämään USB-kaapelin palomuuriin ja avaamaan erillisen hallintaohjelmiston palomuuria varten. Yhteyshenkilö kytki USB-johdon palomuuriin, mutta mitään ei näyttänyt tapahtuvan ja emme saaneet palomuuriin edelleenkään yhteyttä. Palomuurit myös käynnistettiin uudelleen ja kytkettiin muutamia johtoja irti useaan otteeseen, mutta tämäkään ei auttanut. Seuraavaksi Help Desk keksi ehdottaa, että irrottaisimme toisen palomuurin kokonaan irti, jotta se ei kommunikoisi ollenkaan. Käyttäjä myös vaihtoi yhden Ethernet kaapelin paikkaa. Tämän jälkeen palomuurin hallinta ilmestyi hallintaohjelmaan ja pääsin kirjautumaan siihen sisälle. Kaikki näytti päällisin puolin olevan kunnossa. Yhteydet ulospäin alkoivat toimia, mutta meidän oma hallinta laitteeseen ei vieläkään toiminut kunnolla.

Hetken aikaa tarkasteltuamme tilannetta huomasimme, että palomuurit rupesivat aina jumittamaan, kun ne kytkettiin tiettyihin kytkimen portteihin. Tätä ilmiötä tutkittiin vielä tarkemmin hetken aikaa kun loppukäyttäjä kokeili eri kytkentöjä paikan päällä. Lopulta tulimme siihen johtopäätökseen, että asiakkaan sisäverkon kytkimessä tuli jonkinlainen silmukka ja tämä aiheutti valtavan määrän liikennettä palomuurille. Suuresta

liikennemäärästä johtuen palomuuri ei pystynyt vastaamaan Internetistä tulevaan liikenteeseen. Asiakkaan Help Desk ilmoitti harkitsevansa kytkimen vaihtoa parempaan. Lopetimme asian selvittelyn siltä erää.

Viikkoanalyysi

Kulunut viikko meni melko kiireisissä tunnelmissa. Tikettejä oli jäänyt paljon meidän Service Deskin jonoon edellisestä viikolta ja lisää tuli viikon edetessä. Lisäksi itselläni oli vielä muutamia hiukan enemmän aikaa vieviä tikettejä omassa työjonossani. Työviikko oli kokonaisuudessaan mieluisan opettava. Pääsin tekemään muutamia uusia asioita ensimmäistä kertaa ja jouduin soveltamaan aiempaa osaamistani näissä.

Päällimmäisenä viikosta jäi mieleen tiketti, jossa pääsin luomaan uuden virtuaalikoneen ja tekemään erilaista konfigurointia siihen liittyen. Tämä oli mielestäni erittäin opettavaista ja olin hyvin mielissäni, kun pääsin pitkästä aikaa soveltamaan omia tietoja ja taitojani. Lopuksi koin hienon onnistumisen tunteen, kun katselin omaa aikaansaannostani. Tämä haaste oli mielestäni juuri sopiva, sillä ei ollut liian helppo eikä vaikea. Sain tehtävään alustavan ohjeistuksen vanhemmalta kollegalta, mutta ohjeistuksesta jäi puuttumaan paljon merkittäviä yksityiskohtia, jotka kuitenkin onnistuin itse selvittämään aikaisempia tietojani muistelemalla. Loput tehtävään liittyvistä haasteista osasin ratkaista ihan pohtimalla. Ongelmia ei tehtävän aikana juurikaan esiintynyt, enkä joutunut kääntymään kirjallisuuden puoleen asian ratkaisemisen kannalta.

Tämän kertaiseen analyysiin olen päättänyt tuoda esille hieman erilaisia parhaita käytäntöjä palomuurien operointiin liittyen. Työtehtävissämme olemme hyvin paljon tekemisissä Fortinetin tuoteiden kanssa ja tähän liittyen suunnittelinkin käyväni valmistajan näkemyksiä hyvistä käytännöistä. Pyrin löytämään myös yleisempiä näkemyksiä hyvistä käytännöistä analyysissäni. Näillä tiedoilla pyrin jatkossa parantamaan toimintaani palomuurien operointiin liittyen.

Ensimmäisenä voitaisiin tarkastella palomuurin suorituskykyyn liittyviä seikkoja. Palomuurin operoija voi toimillaan helposti optimoida palomuurin suorituskyvyn parhaaseen mahdolliseen. Palomuurin toiminnan optimointi korostuu varsinkin silloin, kun kyseessä on pienempi ja suorituskyvyltään heikompi palomuuri.

Palomuurin hallinnointiin liittyvistä ominaisuuksista kannattaa kytkeä pois päältä ne joita ei tarvitse omassa ympäristössä. SSH ja SNMP ominaisuudet voi kytkeä pois, mikäli niille ei ole tarvetta. Lisäksi SSH hallinnan pitäminen julkiseen Internettiin päin suunnatussa portissa voi tuoda omat tietoturvariskinsä. Eniten käytetyt palomuurisäännöt kannattaa aina sijoittaa listan järjestyksessä ensimmäisiksi. Tämä johtuu siitä, että palomuuri prosessoi palomuurisäännöt järjestyksessä ylhäältä alas ja lopettaa prosessoimisen, kun sopiva sääntö löytyy. (Fortinet 2014.)

Palomuurilla on mahdollista lokittaa erilaisia tapahtumia. Lokitus onnistuu myös erikseen palomuurisäännöissä. Näissä kannattaa miettiä tarkkaan mitä halutaan lokittaa. Jos palomuuri generoi lokia kiintolevylle, voi se rasittaa merkittävästi suorituskykyä. Palomuurien tietoturvaan liittyvät päivitykset kannattaa ajastaa menemään ympäristölle sopivin ajoin. Mikäli palomuurin läpi menee päivisin paljon liikennettä Internettiin päin, kannattaa päivitykset ajastaa menemään vaikka yöaikaan, jolloin kaistanleveyttä on enemmän käytettävissä. (Fortinet 2014.)

Palomuurisäännöissä on mahdollista suorittaa erilaisia tietoturvaominaisuuksia, kuten Antivirus skannausta ja websivujen filtteröintiä. Valmistajan mukaan näiden profiilien käyttöä kuitenkin suositellaan rajoittamaan aina kun mahdollista. Mikäli jotain profiilia ei tarvitse, ei sitä kannata tällöin kytkeä turhaan päälle palomuurisääntöön. Myös kaikenlaisten kaistanhallintaan liittyvien ominaisuuksien käyttämistä tulisi oletuksena rajoittaa, sillä ne oletuksena hidastavat palomuurin suorituskykyä. (Fortinet 2014.)

Tässä oli muutamia hyviä käytäntöjä liittyen palomuurien suorituskyvyn optimointiin. Osaa näistä käytännöistä käytetään meillä töissä aktiivisesti juurikin sen takia, että useilla asiakkailla on melko paljon suorituskyvyltään heikompia laitteita käytössään. Tällaisessa tilanteessa palomuuri halutaan optimoida kaikin mahdollisin keinoin, jotta sillä

saavutetaan paras mahdollinen suorituskyky menettämättä tietoturvallisuutta. Seuraavaksi käsitellään hieman palomuurisääntöihin ja tietoturvaan liittyviä käytäntöjä.

Palomuurisäännöissä on mahdollista käyttää osoiteobjekteja sekä objektiryhmiä. Palomuurisäännöissä tulisi välttää käyttämästä objektia, joka käsittää kaikki lähde -tai kohdeosoitteet. Osoitteissa tulee käyttää objekteja, jotka käsittävät kuhunkin tilanteeseen sopivat IP-avaruudet. Yleisesti ottaen palomuurisäännöt tulisi rakentaa mahdollisimman tarkoiksi. Isoja porttiavaruuksia ei myöskään kannata avata turvallisuussyistä. Palomuurisääntöjen lokitusta kannattaa myös miettiä tarkoin. Palomuurin hylkäämien yhteyksien lokittaminen yleisesti ei ole hyvin kannattavaa. (Fortinet 2014.)

Mikäli verkossa suoritetaan Antivirus skannausta, on se suositeltavaa tehdä verkon reunalla. Antivirus skannauksessa pystytään määrittämään skannattavien tiedostojen enimmäiskoko. Nykyaikana haittaohjelmat leviävät yleensä pienissä tiedostoissa, joten profiilit kannattaakin säätää tarkistamaan kaikki megatavun tai kahden megatavun kokoiset tiedostot. Tätä suuremmat tiedostot voidaan päästää ohi ilman skannausta, jotta suorituskykyyn ei tule merkittävää rasitetta. Myös IPS pohjaiset skannaukset kannattaa rakentaa palomuurille järkevästi. Kaikkein parhaiten ne soveltuvat liikenteeseen Internetistä sisäverkkoon. Tällöin on myös hyvä määritellä mitä liikennettä halutaan tarkastella. Hyvän käytännön mukaisesti Internetistä sisäverkkoon kohdistuva epäilyttäväksi luokiteltu liikenne kannatta estää erilaisilla IPS sensoreilla. (Fortinet 2014.)

3.7 Työviikko 40

Maanantai 29.9

Otin meidän Service Deskin työjonosta mielenkiintoisen tiketin itselleni työn alle. Tiketti oli meidän isoimmalle Hosting-palveluiden asiakkaalle. Työpyynnössä pyydettiin tekemään asiakkaan omaan virtuaaliseen ympäristöön uusi virtuaalikone. Normaalista toimintatavasta poiketen tämä uusi virtuaalikone tuli kloonata olemassa olevasta virtuaalikoneesta, joka oli Windows 7 työpöytäversiossa.

Työpyynnössä asiakas oli määrittänyt mistä koneesta kloonaus tehdään, nimen uudelle virtuaalikoneelle ja IP-osoitteen, joka sille määritetään. Virtuaalikoneen kloonaus tarkoittaa käytännössä sitä, että järjestelmän sanan mukaisesti kloonaa olemassa olevan virtuaalikoneen koko konfiguraation niin, että siitä voidaan tehdä toinen täysin samanlainen virtuaalikone. Kloonaus myös jäädyttää virtuaalikoneen toiminnan hetkeksi, kun järjestelmä tallentaa koneen sen hetkisen tilan snapshotiksi. Tämän takia joskus kloonaukselle määritetään sopiva aika jolloin se voidaan suorittaa. Tässä tapauksessa kyseessä oli vain työasema, joten ajankohdalla ei ollut merkitystä.

Aloitin toimenpiteet valitsemalla VMWare ympäristössä Clone-toiminnon. Tämä käynnisti eräänlaisen konfigurointiohjelman, jossa uudelle koneelle tehdään tarvittavat määritykset. Asetin uudelle koneelle halutun mukaisen nimen sekä valitsin sille klusterin, johon virtuaalikone sijoitetaan. Klusteri muodostuu virtuaalikonealustoista, jotka ovat yhteydessä toisiinsa ja toimivat yhtenä loogisena yksikkönä.

Seuraavaksi määritin virtuaalikoneelle levyjärjestelmästä sopivan NFS-jaon. Ohjelma kysyi vielä, että halutaanko virtuaalikoneelle tehdä muita muutoksia. Valitsin, että ei tehdä lisää muutoksia. Tämän jälkeen uuden virtuaalikoneen luonti alkoi ja siinä kesti noin viisi minuuttia. Kloonauksen valmistuttua käynnistin uuden virtuaalikoneen ja kirjauduin sisään Windowsiin. Koska kyseessä oli klooni toisesta Windows-koneesta, piti järjestelmälle tehdä eräänlainen resetointi. Käytin tähän tehtävään Windowsin omaa Sysprep-ohjelmaa, joka valmistelee käyttöjärjestelmän samaan tilaan, kuin ensiasennuksessa. Tämän toimenpiteen valmistuttua asetin koneelle vielä nimen ja liitin sen asiakkaan AD-domainiin. Lopuksi määritin koneelle vielä oikeat IP-asetukset ja katsoin, että yhteydet muihin palvelimiin toimivat. Koneen ollessa kokonaan valmis, laitoin asiakkaalle kuittauksen sen valmistumisesta.

Tiistai 30.9

Tänään otin itselleni jonostamme erään toisen Hosting-palveluihin liittyvän tiketin. Tiketti oli samalle asiakkaalle kuin edellisenä päivänä, mutta tällä kertaa he halusivat poistaa yhden vanhemman tuotannosta poistuneen virtuaalisen palvelimen. Asiakas halusi myös poistaa kaikki siihen liittyvät valvonta -ja varmistuspalvelut sekä nimipalvelussa

ollut tietue. Asiakas pyysi myös ottamaan palvelimen konfiguraation talteen joksikin aikaa.

Aluksi kirjauduin asiakkaan VMWare-ympäristöön ja paikallistin palvelimen. Asiakas oli jo valmiiksi sammuttanut palvelimen, koska se ei ollut käytössä enää. Palvelinta ei saanut vielä poistaa kokonaan, koska asiakas halusi varmistua, että he eivät sitä tarvitse enää tulevaisuudessa. Otin virtuaalikoneesta konfiguraation talteen ja asetin sen kopioitumaan sen asiakkaan levyjärjestelmään CIFS-jaolle. Tässä toimenpiteessä kesti reilu puoli tuntia, koska tiedoston koko oli yli kymmenen gigatavua.

Kopioinnin valmistuttua lähetin palvelimen valvonnan poistosta eteenpäin viestin vastaavalle taholle. Samoin tein nimipalvelumuutoksen kanssa, koska emme itse Service Deskissä hallitse asiakkaiden julkisia nimipalveluita. Lopuksi siirryin vielä tarkastamaan varmuuskopioinnit palvelimelle. Käytämme palvelimien varmuuskopiointiin Symantecin Netbackup-ohjelmistoa. Kirjauduin ohjelmiston hallintaan ja katsoin mitä kaikkea palvelimella oli määritetty varmuuskopioitavaksi. Sieltä löytyi muutama eri varmuuskopiointiluokka, jossa oli määritetty palvelimen koko kiintolevyn varmuuskopiointi menemään ajastetusti joka päivä. Poistin palvelimen kyseisistä määrityksistä.

Tässä vaiheessa ei ollut enempää tehtävissä työpyynnön osalta, joten kuittasin työn valmistumisesta asiakkaalle ja jäin odottamaan asiakkaan vahvistusta palvelimen lopullisesta poistamisesta.

Keskiviikko 1.10

Tänään oli taas vuorossa virtuaalipalvelimien kanssa työskentelyä. Eräs asiakas oli jälleen tilannut uuden virtuaalipalvelimen omaan ympäristöönsä. Tiketissä asiakas oli määrittänyt palvelimelle tulevat määrittely. Asiakas halusi, että heille tehdään Windows Server 2012 R2 käyttöjärjestelmällä oleva palvelin. Palvelimelle tuli myös laittaa kaksi virtuaaliydintä, kahdeksan gigatavua keskusmuistia sekä 60 gigatavua kovalevytilaa.

Aloitin homman tuttuun tapaan kirjautumalla VMWare ympäristöön. Suodatin näkymää hieman, jotta näin sieltä löytyvät virtuaalikoneiden templatet. Paikansin oikean templaten, joka oli siis mallia Windows Server 2012 R2. Laitoin templatesta kloonautumaan uuden palvelimen asiakkaan määritysten mukaan.

Kloonauksessa kesti noin kymmen minuuttia. Kun se oli valmis, asetin laitteelle asiakkaan kertomat määrittelyt laitteiston suhteen. Kytkin laitteen myös asiakkaan virtuaaliseen verkkoympäristöön, jossa muutkin palvelimet sijaitsivat. Muutosten jälkeen käynnistin virtuaalikoneen ja kirjauduin Windowsiin. Sisäänkirjautumisen jälkeen menin ensin asettamaan koneelle kiinteän IP-osoitteen asiakkaan määrittelyn mukaan. Tämän jälkeen siirryin tietokoneen asetuksiin ja muutin nimen asiakkaan haluamalla tavalla sekä liitin sen asiakkaan toimialueeseen käyttäen toimialueen admin-tunnuksia. Muutoksien jälkeen kone piti käynnistää uudelleen.

Näiden muutoksien valmistuttua lähdin hakemaan palvelimelle päivityksiä Windows Update-keskuksen kautta. Palvelimelle löytyi muutama tärkeä päivitys, jotka asensin koneelle. Lopuksi säädin palvelimelle vielä muutaman virrankäyttöön liittyvän asetuksen, jotta palvelin toimisi täydellä suorituskyvyllä.

Viimeisien muutoksien jälkeen kirjauduin ulos ja testasin toiselta palvelimelta, että yhteys sinne toimii normaalisti. Kun totesin kaiken olevan kunnossa, ilmoitin asiakkaalle palvelimen valmistumisesta sähköpostitse.

Torstai 2.10

Sain tehtäväkseni yhden tiketin, jossa erään asiakkaan kumppani pyysi meiltä palomuuriavauksia asiakkaan palveluun. Prosessin mukaisesti välitin pyynnön eteenpäin asiakkaan yhteyshenkilölle, koska vain hänellä on valtuudet pyytää muutoksia palveluun. Asiakkaan yhteyshenkilö vahvisti muutokset. Jouduin kuitenkin pyytämään asiakkaan yhteyshenkilöltä vielä lisätietoa keikkaan, koska muutospyynnössä oli mainittu melko niukasti miten kyseisen palomuuriavaus tulisi toteuttaa. Asiakkaan kumppani oli vain maininnut heidän käyttämänsä julkisen IP-osoitteensa, johon asiakkaan palvelimelta tulisi voida muodostaa HTTPS-yhteys.

Asiakkaan kumppani lähetti vastauksen tarvittavista avauksista, mutta viestistä jäi vielä-kin puuttumaan tarkka tieto mistä palvelimesta asiakkaan yhteys ulospäin muodoste-taan. Nyt kun minulla oli tiedossa julkinen IP-osoite mihin palvelimen ohjelmisto yritti ottaa yhteyttä säännöllisesti lähettääkseen dataa, rupesin tutkimaan palomuurin lokeja sekä monitoroimaan liikennettä palomuurilla. Asetin monitorointiin asiakkaan kump-panin antaman IP-osoitteen ja katsoin miten sinne meni liikennettä. Hetken aikaa mo-nitorissa ei näkynyt mitään liikennettä, mutta noin viiden minuutin odottelun jälkeen monitoriin alkoi näkymään yhteyden muodostuksia.

Näin monitorissa asiakkaan sisäverkon IP-osoitteen, joka yritti muodostaa HTTPS-yhteyden asiakkaan kumppanin mainitsemaan osoitteeseen. Tämän tiedon perusteella tein palomuurisäännön, joka sallii yhteyden kyseisten osoitteiden välillä ja pyysin asia-kasta tarkastamaan yhteyden toimivuuden. Asiakkaan kumppani ilmoitti, että vielä ei näkynyt kaikkea tarvittavaa dataa ja mainitsi samalla muutaman uuden julkisen IP-osoitteen, johon asiakkaan palvelimelta tulisi voida muodostaa yhteys. Lisäsin nämäkin osoitteet aiemmin tekemääni palomuurisääntöön kohdeosoitteiksi. Tämän jälkeen pyy-sin asiakasta taas testaamaan yhteyttä. Vastausta ei kuitenkaan kuulunut enää samana päivänä, joten tiketti jäi odottamaan asiakkaan vastausta siltä osin.

Viikkoanalyysi

Tällä viikolla oli mukavaa vaihtelua työtehtävissä, kun pääsin pitkästä aikaa tekemän työtehtäviä, jotka liittyivät Hosting-palveluihin. Nämä tehtävät ovat minulle aina mie-lenkiintoisia ja väitänkin osaavani niistä eniten. Työtehtävät viikon aikana sisälsivät muutamia keikkoja, joissa tehtiin uusia virtuaalipalvelimia asiakkaille heidän määritys-tensä mukaisesti. Viikon aikana pääsin myös tekemään muutamia uusia levyjakoja mei-dän SAN pohjaiseen levyjärjestelmään sekä suorittamaan virtuaalipalvelimien poista-mista eri järjestelmistä.

Nämä työtehtävät eivät suorastaan tuottaneet minulle vaikeuksia, sillä olen tehnyt niitä useamman kerran. Tehtävät vaativat silti aina huolellisuutta, koska kaikkia yksityiskohtia ei voi aina muistaa tarkalleen. Yleensä kaikki tarvittavat asiat kuitenkin muistuvat hiljalleen mieleen.

Aloitin viime analyysissä tarkastelemaan alan hyviä käytäntöjä palomuurien operointiin liittyen. Tässä suuressa osassa ovat Fortinetin tuotteet, joilla tuotamme valtaosan yrityksen tarjoamista tietoturvaratkaisuista. Tästä johtuen tiedon lähteenä on luonnollista käyttää valmistajan omaa dokumentaatiota. Joihinkin yleisempiin teknologioihin liittyviin seikkoihin on hyvä hakea myös ulkopuolista näkemystä.

Seuraavaksi on tarkoitus tarkastella hieman valmistajan suosituksia verkon rakentamiselle. Näistä oleellisimpina seikkoina voidaan pitää erilaisia reititysprotokollia. Verkkoa suunnitellessa ja rakentaessa on hyvä muistaa, ettei suojattuihin verkkoihin jää mitään takaovia, joiden mukana verkon tietoturva voi olla vaarassa. Tämän vuoksi onkin hyvä aina ylläpitää dokumentaatiota omasta verkosta, laitteista ja kytkennöistä. VPN-tunnelien kanssa olisi hyvä käyttää ns. Blackhole-reittejä. Nämä eräänlaiset staattiset reitit estävät sen, että liikenne ei reitity väärään paikaan salaamattomana, kun VPN-tunneli menee alas syystä tai toisesta. (Fortinet 2014.)

Sääntöpohjaisen reitityksen avulla voidaan liikennettä reitittää monipuolisemmin keinoin verrattuna perinteiseen kohdepohjaiseen reititykseen. Tämä kuitenkin vaatii palomuurilta enemmän suorituskykyä ja tämän vuoksi sen käyttöä tulisi pitää mahdollisemman pienellä. Sääntöpohjaisen reitityksen ajaminen voi myös aiheuttaa ylimääräistä päänvaivaa erilaisia vikatilanteita selvittäessä. (Fortinet 2014.)

Dynaamista reititystä käytettäessä on palomuurin reititystä ajavalle portille määritettävä Router ID arvo, jonka avulla muut reitittimet tunnistavat laitteen. Tässä tulisikin aina käyttää arvoa, joka vastaa palomuurin dynaamiseen reititykseen osallistuvan portin IP-osoitetta. Näin vältytään helposti tilanteilta, joissa kahdella eri laitteella on sama Router ID-arvo. Mikäli dynaamista reititystä ajetaan VPN-tunnelin ylitse, on tällöin tunnelin käyttämälle virtuaaliselle portille hyvä määritellä oma IP-osoite. Tämä selkeyttää reitityksen määrittelyä huomattavasti.(Fortinet 2014.)

Yrityksemme Service Deskissä olemme usein tekemisissä erilaisten VPN-tunneleiden kanssa. Monilla asiakkailla on Site-to-Site tyylisiä VPN-ratkaisuja ja nämä kannattaakin yleensä rakentaa mahdollisimman tietoturvallisesti. Loppupeleissä asiakkaalla on kuitenkin päätösvalta, kuinka tunnelin määrittelyt tehdään. Seuraavaksi käydään hieman suosituksia ja huomioita liittyen VPN-tunnelien luontiin.

IPsec tunnelien kanssa tapanamme on tehdä liikenteen rajaukset mahdollisimman tarkasti. Tunnelin suojattuihin verkkoihin pyritään laittamaan vaan tarpeelliset aliverkot molemmilta puolilta. Palomuurisäännöillä pyritään rajaamaan osoite -ja porttikohtaisesti kukin yhteys tarpeen mukaan. Esijaettu avain pyritään tekemään tarpeeksi pitkäksi ja se jaetaan vastapuolelle turvallisella menetelmällä, esim. sms-viestillä. Tunnelin salauksessa pyritään välttämään heikompia salausmenetelmiä, mikäli se ei rajoita tunnelin suorituskykyä. Blackhole-reititystä pyritään myös käyttämään tilanteen mukaisesti.

SSL-VPN pohjaisissa ratkaisuissa on myös omat seikat, jotka kannattaa ottaa huomioon niitä rakentaessa. VPN-yhteyspisteen tulisi sijaita verkon DMZ-vyöhykkeellä, jotta liikennöinti yrityksen sisäverkkoon voidaan rajata tehokkaasti. Split Tunneling reitityksen käyttöä on myös syytä välttää, koska se mahdollistaa liikennöinnin haitallisiin kohteisiin VPN-yhteyden ollessa päällä. Tällöin on hyvä käyttää erilaisia Antivirus ohjelmistoja käyttäjien päätelaitteiden valvontaan ja hallinnointiin. (Infosec 2014.)

Monilla asiakkaistamme SSL-VPN tekniikkaa käytetään antamaan erilaisille partnereille turvalliset yhteydet yrityksen sisäverkkoon. Tällöin on erityisen hyvä käyttää vahvaa autentikointia kirjautumiseen. Meillä yleisimpänä ratkaisuna on kaksivaiheinen autentikointi SSL-VPN yhteyksien kanssa. Pääsyä yrityksen resursseihin kannattaa rajoittaa käyttäjäkohtaisesti tarpeen mukaan. Oletusksena käyttäjille ei kannata antaa näkyvyyttä mihinkään ylimääräiseen resurssiin. (Infosec 2014.)

Tässä tuli käytyä läpi monenlaisia tärkeitä huomioita liittyen palomuureihin ja siihen miten niillä voidaan parantaa yrityksen tietoturvaa. Meillä Service Deskissä pyritään aina tekemään kaikki asiat noudattaen alan parhaita käytäntöjä huomioiden erityisesti tietoturvan. Asiakastoteutuksien kanssa pyrimme usein ohjaamaan asiakasta tietoturvan

näkökulmasta oikeaan suuntaan, ottaen huomioon ympäristön asettamat rajoitteet ja vaatimukset. Koen silti edellä mainitut ohjeistukset ja huomiot erittäin tärkeäksi. Näitä käytäntöjä onkin hyvä käydä läpi säännöllisin väliajoin, jotta oma tekeminen pysyy ajan hengessä ja ammattimaisena.

3.8 Työviikko 41

Maanantai 6.10

Asiakas teki meille pikaisen työpyynnön, jossa haluttiin tehdä lisäyksiä heidän etäkäyttöpalveluunsa. Otin tiketin itselleni työn alle. Tiketissä asiakas mainitsi, että tarvitsi uuden käyttäjäroolin heidän etäkäyttöpalveluunsa eräälle kumppanille. Muutostyö piti tehdä mahdollisimman nopeasti, jotta asiakas pystyi testaamaan toimivuuden ja pyytää tarvittaessa lisäyksiä rooliin.

Aloitin homman kirjautumalla asiakkaan Juniper SA laitteelle, johon etäyhteydet muodostetaan. Ensimmäiseksi tein uuden roolin, jossa määriteltiin sille nimi sekä käytettävät palvelut. Palveluiksi asiakas halusi määrittää Network Connect ominaisuuden, joka käytännössä muodostaa VPN-tunnelin käyttäjän ja laitteen välille. Tuohon VPN-yhteydelle piti sallia kaikki portit muutamaan asiakkaan sisäverkon palvelimeen. Rooliin määritettiin reitittämään kaikki clientin liikenne tunneliin kohti. Seuraavaksi siirryttiin tekemään autentikointisääntö roolille. Asiakkaan AD-palvelimella oli tehty käyttäjätunnus kyseiselle tunnukselle, jonka laitoimme laitteen autentikointisääntöön. Käytännössä autentikointi toimii niin, että kun kyseisellä käyttäjätunnuksella kirjaudutaan laitteelle, etsitään käyttäjätunnus asiakkaan AD-palvelimelta ja rooli määritellään sen mukaisesti. Tässä kohtaa on vielä mahdollista määritellä käytettäväksi vahva autentikointi, mutta tässä tapauksessa kyseistä asetusta ei otettu käyttöön.

Viimeisimpänä toimenpiteenä piti roolille tehdä vielä IP-osoitteen mappaus. Laitteelle oli määritelty yksi isompi verkkoavaruus, josta jaellaan IP-osoitteita VPN-käyttäjille, kun he muodostavat tunnelin. Lisäsin juuri tekemäni uuden roolin tähän kyseiseen sääntöön, jotta sekin saa kirjauduttaessa IP-osoitteen.

Muutoksien jälkeen lähetin asiakkaalle sähköpostin muutoksien valmistumisesta ja pyysin testaamaan toimivuutta. Hieman myöhemmin päivällä asiakas vastasi sähköpostilla ja kertoi uuden roolin toimivan halutun mukaisesti. Näillä tiedoilla pistin keikan ratkaistuksi.

Tiistai 7.10

Sain selvitettäväkseni erään asiakkaan tiketin liittyen heidän toimipisteensä palomuurin, jonka kanssa oli yhteysongelmia. Asiakkaan toimipisteellä oli ollut jo kauan aikaa toiminnassa oleva palomuuri. Edellisellä viikolla heiltä oli loppunut sopimus operaattorin kanssa ja heidän Internet-linjansa loppui. Tilalle asiakas oli hommannut mobiililaajakaistan, jossa ei ilmeisesti käytetty kiinteää julkista IP-osoitetta.

Uuden liittymän kanssa yhteydet ulospäin eivät enää jostain syystä toimineet. Asiakkaan erän paikallinen kontakti oli järjestänyt meille etäyhteyden palomuurille TeamViewer-ohjelman avulla, jotta pääsisimme tutkimaan ongelmaa. Pääsin kirjautumaan palomuurille ja aloin tutkia sen asetuksia. Palomuuri näytti saavan sisäverkon IP-osoitteen DHCP:llä sen ulospäin suunnattuun porttiin. Tämä ilmeisesti oli toiminut aiemmin vanhalla linjalla. Seuraavaksi rupesin tarkastamaan VPN-tunnelia, joka näytti olevan ylhäällä, mutta jostain syystä liikenne palomuurille ei kuitenkaan mennyt. Tarkastin myös VPN-tunnelin asetukset ja palomuurisäännöt, joissa ei näyttänyt olevan mitään ihmeellistä. Ainut mikä kiinnitti huomioni, oli VPN-asetus NAT-Traversal-parametrille, joka oli pois päältä. Tätä parametria tarvitaan yleensä, kun yhteyden varrella on osoitteenmuunnosta tekeviä laitteita ja tässä tapauksessa se oli mobiilireititin. Tunneli kuitenkin neuvotteli itsensä ylös vaikka varsinainen liikenne ei toiminut. Asiakkaan ympäristöstä johtuen tuota asetusta ei ilmeisesti voitu ottaa käyttöön. Monitoroin liikennettä palomuurilla ja näin, että asiakkaan pääpalomuurilta tulleet paketit eivät koskaan päässeet perille asti.

Asiakkaan kontakti antoi meille tunnukset reitittimen hallinta, jotta voisimme myös tarkastaa sen tilanteen. Katsoin reititintä, ettei siellä ole mitään estetty ja kaikki normaalit määrittelyt ovat kunnossa. Sieltäkään ei mitään selkeää löytynyt. Pyysin käyttäjää kysymään operaattorilta, että blokkaako se VPN-liikennöintiä liittymään. Yhteyshenkilö

tiedusteli asiaa operaattorilta ja sai vastauksen, että ei pitäisi estää. Tässä vaiheessa oma työvuoroni alkoi lähestyä loppuaan ja ongelman selvittämistä piti jatkaa jollain tavoin. Päätin eskaloida tiketin meidän toisen tason asiantuntijoille selvitettäväksi.

Keskiviikko 8.10

Otin meidän Service Deskin jonosta palvelupyynnön tehtäväkseni. Kyseessä oli tavanomaisia palomuuripyyntöjä eräälle asiakkaalle heidän palomuuriinsa. Hieman haastetta tähän normaaliin muutospyyntöön teki oikean palomuurin löytäminen ja muutosten tekeminen oikeaan paikkaan. Asiakkaan organisaatiossa oli tapahtunut muutoksia, mistä johtuen heidän ympäristönsäkin oli eriytetty kahteen eri virtuaaliseen palomuuri-instanssiin. Nämä kyseiset instanssit sijaitsivat molemmat meidän keskitetyllä palomuurialustalla.

Pyynnössä asiakas ilmoitti missä oletti palomuurisääntöjen sijaitsevan, mutta todellisuudessa ne näyttivät kuitenkin sijaitsevat juurikin toisella palomuurilla. Asiakkaan palomuurille oli tehty VPN-tunneli eräälle toimipisteelle ja täällä oli käytössä oma aliverkko. Täältä aliverkosta piti saada pääsy yrityksen VOIP-järjestelmään. Tämän vuoksi asiakas oli pyytänyt palomuurisääntöihin lisäyksiä. Nuo kyseiset lisäykset eivät menneet kuitenkaan ihan asiakkaan ilmaisemalla tavalla. Yhteys VOIP-palveluihin näytti menevän molempien asiakkaan palomuurien läpi. Tarkistin toisen palomuurin konfiguraatiota ja huomasin, että uusi aliverkko puuttui reititystaulusta. Lisäsin kyseisen aliverkon palomuurin staattisiin reitteihin sekä muutamiin kohtiin palomuurisäännöissä, jotta liikenne asiakkaan kahden palomuurin välillä toimisi oikein. Muutoksien jälkeen ilmoitin asiakkaalle ja pyysin heitä testaamaan, että toimiiko yhteys halutulla tavalla. Jäin odottamaan testituloksia.

Torstai 9.10

Saimme Service Deskiin melko kiireisen työpyynnön eräältä Hosting-palveluiden asiakkaalta. Kyseessä oli tiedoston palautukseen liittyvä palvelupyyntö. Asiakkaalla on käytössään virtuaaliympäristö, joka käyttää levyjärjestelmää hyväkseen. Asiakkaan palveluun kuuluu myös varmistuspalvelu, jossa levyjärjestelmästä otetaan talteen kopioita

päivittäin. Tiedostojen palautus levyjärjestelmästä onnistuu kolmenkymmenen päivän taakse. Tämä palautuspyyntö koski asiakkaalle tehtyä CIFS-jakoa, jota he käyttävät keskitettynä tallennuspaikkana kaikelle tärkeälle datalle.

Asiakkaalla oli ilmeisesti jokin tiedosto sotkeutunut ja he halusivat, että kyseinen tiedosto palautettaisiin tilanteeseen viikon takaa. Kirjauduin meidän omalle virtuaalityöpöydälle, jota käytämme asiakkaiden palvelinympäristöjen hallinnointiin. Työpöytä toimii Citrixin XenDesktop teknologialla. Virtuaalityöpöydältä otin taas RDP-yhteyden asiakkaan Vcenter-hallinnointikoneeseen. Kun olin kirjautunut asiakkaan koneelle mappasin sieltä CIFS-jaon näkyviin käyttäen Windowsin resurssienhallintaa. Hain esille kansion, josta kyseinen tiedosto löytyi ja valitsin näytettäväksi kansion edelliset versiot Windowsin omalla ohjelmalla. Tuosta näkymästä navigoin ajassa viikon taaksepäin ja löysin asiakkaan haluaman tiedoston. Kopioin tiedon tuosta näkymästä ja liitin sen ensiksi palvelimen järjestelmälevylle. Tämän jälkeen muutin kopioidun tiedon nimen niin, että sen tunnisti palautetuksi. Viimeiseksi liitin tiedoston asiakkaan verkkolevylle alkuperäiseen paikkaansa. Ilmoitin asiakkaalle, että tiedosto oli palautettu halutun mukaisesti sekä kerroin tiedoston tarkan nimen.

Viikkoanalyysi

Tämä viikko sujui lähes samoissa merkeissä kuin pari edellistä viikkoakin. Työtä riitti edelleenkin paljon. Työtehtävieni osalta tämä viikko erosi siten, että se sisälsi paljon enemmän tekemistä palvelimien ja niihin liittyvien järjestelmien kanssa.

Viikko toi mukanaan hieman uusia haasteita, mutta myös vanhojen asioiden kertaamista. Erityisiä haasteita aiheuttivat levyjärjestelmiin liittyvät muutamat kysymykset, joita viikon aikana tuli erään tiketin ohella. Haasteesta selvisin konsultoimalla vanhempaa kollegaa, jolla oli vahva kokemus asiaan liittyen. Sain kollegalta alustavan perehdytyksen aiheeseen ja alustavan ohjeistuksen, jonka pohjalta pystyin suoriutumaan tehtävän suorittamisesta itsenäisesti. Muutoin viikon aikana ei erityisempiä haastavia työtehtäviä esiintynyt ja niistä suoriuduttiin omalla työkokemuksella.

Tämän viikon analyysiin en vielä keksinyt uutta aihealuetta tutkittavaksi, joten päätin vielä jatkaa hieman edellisellä teemalla, jota olen käynyt läpi kahdessa edellisessä analyysissäni. Yritän löytää aihealueeseen vielä jotain yleisempiä mielipiteitä, jotka tukevat aiemmin kerrottua tietoa.

Aluksi voitaisiin hieman käsitellä yleisiä toimintatapoja palomuurien hallinnointiin liittyen. Näissäkin hommissa asioita voidaan tehdä oikein tai väärin. Valitettavan usein olen työtehtävissänikin kohdannut tilanteita, joissa palomuurien järkevää ylläpitoa ja hallinnointia ei ole harjoitettu tarpeeksi.

Löysin erään artikkelin, jossa otetaan hyvin kantaa keinoihin, joilla voidaan pitää palomuurien hallinnointi järkevällä tasolla. Yleensä palomuurin elinkaaren aikana sen konfiguraatioon tehdään paljon erilaisia palomuurisääntöjä ja erilaisia määrityksiä. Monissa yrityksissä näistä muutoksista on yleensä vastuussa valittu henkilö, jonka tehtävänä on valvoa, että kaikki määritykset ovat kunnossa palomuurilla. Vastuuhenkilöllä ei välttämättä aina ole suoraa näkymää palomuurin sisältöön ja tästä syystä siellä voikin olla paljon ylimääräistä sisältöä, joka ei välttämättä enää aja mitään tarpeita liiketoiminnan suhteen ja voikin pahimmillaan aiheuttaa erilaisia tietoturvariskejä. Tämän vuoksi palomuurien sääntökantoja on hyvä tarkastella säännöllisin väliajoin ja poistaa kaikki ei tarvitut palomuurimääritykset. Syynä voi olla, että sääntöä ei enää tarvita tai vastaava järkevämmin tehty määritys löytyy jo. Palomuurisääntöjen säännöllinen siivoaminen selkeyttää kokonaiskuvaa verkon tietoturvasta ja voi parhaimmillaan tuoda lisää suorituskykyä palomuurin kokonaistoimintaan. (Musthaler 2014.)

Tämän lisäksi palomuurisäännöissä voi olla paljon päällekkäisyyksiä, jonka vuoksi uudet palomuurisäännöt voivat usein jäädä turhiksi tai jopa toimimattomiksi. Palomuurit toimivat yleensä periaatteella, jossa ensimmäinen sopiva palomuurisääntö valitaan käytettäväksi. Tämän vuoksi useat palomuurisäännöt voivat jäädä täysin tarpeettomiksi ajan kuluessa. Artikkelissa kehotetaankin dokumentoimaan kaikki muutokset palomuurin mahdollisimman tarkasti. Tämän lisäksi niiden implementoinnissa olisi hyvä aina käyttää jonkinlaista prosessia, jonka mukaan niitä tehdään. Uusien palomuurisääntöjen pitäisi aina perustua johonkin liiketoiminnan tarpeeseen. Näin toimimalla voidaan hel-

posti päätellä mitkä palomuurin sallimat palvelut ovat vielä ajankohtaisia. (Musthaler 2014.)

Viimeisimpänä artikkelissa käsitellään kommunikointia ohjelmisto -ja verkkopuolen ihmisien välillä. Tyypillisesti ohjelmistoista ja palveluista vastaavat ihmiset pyytävät usein muutoksia palomuurien sääntöihin, kun uusia palveluita tai ohjelmistoja otetaan käyttöön. Tämä ei automaattisesti tarkoita sitä, että kaikki palveluiden käyttämät yhteydet olisivat täydellisessä ymmärryksessä. Tämän vuoksi olisikin hyvä, että verkosta vastaavat henkilöt olisivat tiiviissä yhteistyössä ohjelmistopuolen henkilöstön kanssa, kun uusia palveluita sallitaan palomuureilla. Tällöin vältytään turhilta avauksilta ja muutosten suorittaminen nopeutuu. (Musthaler 2014.)

Erään toisen julkaisun mukaan palomuurisääntöjen yhdenmukaistaminen on hyvä tapa pitää sääntökanta selkeänä. Eri bisnesyksiköille voidaan määrittää pääsyt palveluihin samoissa palomuurisäännöissä esim. käyttämällä osoiteobjekteja tai objektiryhmiä. Näin vältytään luomasta ylimääräisiä palomuurisääntöjä samaa yhteyttä varten. Tämän lisäksi objektien kanssa on hyvä käyttää selkeitä nimeämiskäytäntöjä. Useat palomuurit antavat nimetä objekteja melko vapaasti, jolloin esim. tietyt IP-osoitteet voidaan helposti yhdistää erilaisiin palveluihin. (Algosec 2014.)

Julkaisussa otetaan myös kantaa verkkoarkkitehtuurin suunnitteluun tietoturvan ja suorituskyvyn näkökulmasta. Sen mukaan yrityksen verkot kannattaa aina loogisesti erottaa toisistaan niiden käytön ja kriittisyyden mukaisesti. Palomuurisäännöt kannattaa myös kustomoida näitä kriteerejä huomioiden. Yhdessä nämä seikat tuovat yrityksen verkkoon lisää tietoturvaa sekä selkeyttä. Julkaisussa mainitaan myös, että verkkolaitteiden hallinointiin tulisi rakentaa aina oma yhteys, jota käytetään vain tähän tarkoitukseen. Jos pääyhteys verkkoon ja sen laitteisiin katoaa, pystyvät verkon operoijat pääsemään niihin kiinni käyttäen hallintayhteyttä. (Algosec 2014.)

Tässä tuli käytyä erilaisia käytännön asioita eri näkökulmista katsottuna. Pidän monia näistä käydyistä asioista erittäin tärkeinä ja oleellisina asioina, kun työskennellään palomuurien ja niihin liittyvien ympäristöjen kanssa. Monet näistä käytännöistä ovatkin meidän tekemisessä erittäin näkyvästi esillä ja pyrimme noudattamaan niitä aina par-

haalla mahdollisella tavalla. Osa asiakkaistamme noudattaa tämän tyylisiä ohjeistuksia myöskin hyvin tiiviisti ja tämä yleensä helpottaakin päivittäistä yhteistyötä heidän kanssaan.

3.9 Työviikko 42

Maanantai 13.10

Olin työskentelemässä päivävuorossa ja sain eräältä asiakkaalta puhelimitse toimeksiannon. Asiakas halusi avata tiketin aiheesta tiedostojen palautus virtuaalipalvelimelle. Asiakkaalla oli ostettuna yksi virtuaalipalvelin meiltä sekä varmuuskopiointipalvelu siihen liittyen. Asiakas oli kadottanut joitakin tiedostoja heidän palvelimensa jakamasta levyjaosta ja halusi, että tiedostot palautettaisiin ennalleen viimeisimmästä varmuuskopioista.

Tein asiasta ensimmäiseksi tiketin meidän järjestelmään ja otin yhteyttä asiakkaan myyjään ja rupesin tiedustelemaan hinnoittelua toimenpiteelle. Palveluun kuuluu, että varmuuskopiointi menee kuukausimaksulla, mutta tiedostojen palautus maksaa asiakkaalle erikseen, mikäli se on asiakkaasta aiheutuvaa. Sain myyjältä hintatiedon ja välitin sen asiakkaalle hyväksyttäväksi. Asiakas antoi hyväksynnän laskutukselle ja jatkoin palautuksen tekemistä.

Ensimmäiseksi avasin meidän varmuuskopiointiohjelmiston hallinnan ja paikansin sieltä asiakkaan varmistusluokan. Kävi ilmi, että asiakkaalla oli perustason varmuuskopiointi, eli muuttuneet tiedostot varmistetaan päivittäin ja täysi varmuuskopiointi suoritetaan kerran viikossa. Tiedostojen säilytysaika oletuksena on noin pari viikkoa.

Aloin selaamaan asiakkaan varmuuskopioita ja paikansin asiakkaan haluamat tiedosto viimeisimmästä täyskopioista, joka oli muutaman päivän vanha. Tutkin asiakkaan ympäristöä ja huomasin, että tiedostoja ei voitu suoraan palauttaa asiakkaan virtuaalipalvelimelle, koska konesalissa asiakkaalle ei ollut rakennettu omaa verkkoa tätä varten.

Jouduin turvautumaan seuraavaan ratkaisuun. Meillä on käytössä yhteinen terminaalipalvelin, jota voidaan käyttää tiedostojen palauttamiseen. Tässä tapauksessa palautetta-

vaa dataa oli sen verran paljon, että terminaalipalvelimelle piti luoda uusi levyosio, jotta palautettavat tiedostot mahtuisivat sinne. Teimme yhdessä vanhemman kollegani kanssa palvelimelle uuden levyn ja palautimme halutun datan sinne. Seuraavaksi data piti saada siirrettyä jotenkin asiakkaan palvelimelle. Tämä onnistuisi image-pohjaisen tiedoston avulla, joten teimme asiakkaan datasta uuden imagen ja liitimme sen virtuaalikoneen hallinnalla asiakkaan palvelimelle, jolloin se ilmestyi Windowsin resurssienhallintaan.

Viimeisimpänä aloimme kopioimaan imagelta tiedostoja alkuperäiseen hakemistoon. Tämä oli hiukan hidasta, koska kopioitavaa dataa oli paljon ja koneen suorituskyky ei kyennyt käsittelemään kaikkea dataa kerralla. Tämä piti siis tehdä pienissä osissa. Viimein saatiin kaikki data palautettua takaisin asiakkaan levylle, joten ilmoitin asiakkaalle, että halutut tiedostot olivat taas levyllä. Ilmoitin myös asiakkaan myyjälle, että tehdyt toimenpiteet voidaan pistää laskutukseen.

Tiistai 14.10

Sain kollegaltani erään tiketin hoidettavakseni. Asia koski asiakkaan palomuuripalvelua ja siihen lisättävää uutta yhteyttä. Uuden yhteyden lisäämisen kanssa oli ollut erinäisiä haasteita asiakkaan kanssa ja oli sovittu, että asiaan liittyen pidetään puhelinpalaveri, johon kaikki osapuolet liittyvät. Tehtäväni tässä tiketissä oli liittyä tähän puhelinpalaveriin ja saada ratkottua asiakkaan yhteysongelma. Asiakkaan palomuurille oli siis tuotu toiselta operaattorilta yhteys, joka oli lisätty muurille uutena Vlanina. Lisäksi tähän yhteyteen oli tehty muutama palomuurisääntö ja reititys testausta varten.

Puhelinkokouksen aikana asiakas halusi testata liikenteen toimivuuden. Aikaisemmalla yrityksellä liikennettä ei ollut saatu kulkemaan palomuurille asti. Tämän kertaisilla yrityksellä liikenne kuitenkin kulki palomuurille asti, mutta yhteys ei vielä mennyt viimeiseen päämäärään. Tämä johtui siitä, että asiakas testasi yhteyttä eri verkosta, kuin oli aiemmin ilmoitettu ja tämän vuoksi reititys ja palomuurisäännöt estivät yhteyden. Tein hieman muutoksia palomuurille, jotta saisin liikenteen kulkemaan.

Muutoksien jälkeen pyysin asiakasta testaamaan tietoliikenteen toimivuutta pingillä kohdeosoitteeseen. Samalla tutkailin liikennettä palomuurilta ja se näytti menevän halutulla tavalla. Asiakas vahvisti yhteyden toimivuuden ja testasi vielä lisäksi HTTPS.-yhteyttä kohdepalvelimeen. Tämäkin näytti toimivan halutulla tavalla.

Asiakas oli tyytyväinen muutoksiin ja yhteyden toimivuuteen, joten päätimme lopettaa puhelinkokouksen ja sulkea tiketin siltä erää.

Keskiviikko 15.10

Sain puhelinsoiton erään asiakkaan IT-henkilöltä. Asia koski itselläni auki olevaa tikettiä, jossa olimme ilmoittaneet asiakkaalle heidän toimipisteensä palomuurin toimimattomuudesta. Tiketissä ilmoitimme, että etäyhteys palomuuriin oli kadonnut jostain syystä. Yhteydet olivat olleet alhaalla muutaman päivän ja nyt asiakkaan paikallinen IT-henkilö soitti meille ja halusi yrittää selvittää tilanteen.

Katsoin ensin meidän valvontasovelluksesta, että oliko hälytys laitteesta vielä aktiivinen. Valvontasovellus näytti, ettei laitteeseen saatu vieläkään yhteyttä. Asiakkaan kontakti ilmoitti, että toimipisteessä oli tehty jotain muuttotoimenpiteitä. Kysyin kontaktilta, että oliko heidän Internet-yhteyteensä tullut mitään muutoksia, jotka voisivat vaikutta yhteyden toimivuuteen. Kontakti ei osannut sanoa varmasti, mutta lupasi selvittää asian palveluntarjoajan kanssa. Noin puolen tunnin päästä asiakkaan kontakti soitti uudelleen ja ilmoitti millaisella kokoonpanolla yhteys mahdollisesti saataisiin toimimaan taas. Hän sanoi myös, että voisi järjestää meille etäyhteyden omalle koneelleen, joka taas kytketään palomuuriin Ethernet kaapelilla.

Asiakkaan kontakti järjesti etäyhteyden toimintaan ja aloimme yhdessä tutkia tilannetta. Kytkimme tietokoneen Ethernet kaapelilla palomuurin ulkoiseen porttiin ja vaihdoimme tietokoneen IP-asetukset vastaamaan palomuurin konfiguraatiota. Saimme selaimella auki palomuurin hallintaikkunan. Tarkastelin hetken aikaa konfiguraatiota ja totesin, että palomuurin näkökulmasta mikään ei ollut muuttunut. Asiakkaan kontakti ehdotti, että vaihtaisimme IP-osoitteita palomuurin ja reitittimen kanssa keskenään. Ilmeisesti

reitittimen toinen portti oli siltaavana ja toinen reitittävänä. Vaihdoimme IP-osoitteet keskenään ja samalla muutin myös palomuurin oletusreitin vastaamaan uutta IP-osoitetta. Asiakas teki myös kytkennät uudelleen palomuurilla. Muutoksen jälkeen katsoin palomuurilta, että linkki nousi ylös ja yhteys ulospäin muodostui.

Tämän jälkeen asiakas liitti koneensa palomuurin sisäiseen porttiin ja testasin DHCP palvelun toimivuuden. Asiakkaan koneelta yhteydet toimivat. Samalla vaihdoin myös VPN-tunnelin asetukset toisessa päässä vastaamaan uutta IP-osoitetta, jotta hallintayhteys palomuurille onnistui.

Asiakkaan yhteyshenkilöllä oli vielä jotain muita pyyntöjä koskien heidän toimipisteensä sisäverkkoa, mutta päätimme selvitellä asiaa hieman tarkemmin asiakkaan pääyhteyshenkilön kanssa ja siltä osalta keikka sai jäädä odottamaan vastausta.

Torstai 16.10

Eräs asiakas teki tilauksen uudesta virtuaalipalvelimesta. Pyynnössä asiakas määritteli myös koneelle määritettävät yksityiskohdat. Asiakas ilmoitti, että käyttöjärjestelmäksi tulisi Windows Server 2008 R2 ja palvelin liitettäisiin asiakkaan DMZ-vyöhykkeelle. Palvelimelle tulisi lisätä myös kolme erillistä kovalevyä, joista yksi olisi 50 gigatavua, toinen 10 gigatavuaja kolmas 80 gigatavua.

Loin uuden palvelimen valmiina olevasta Templatesta ja määrittelin siihen tarvittavat asetukset. Loin palvelimelle kiintolevyt asiakkaan määrityksen mukaan. Koska tämä palvelin tuli asiakkaan DMZ-vyöhykkeelle, oli sille tarkoitus määritellä julkinen IP-osoite, joka hommataan meidän toimesta. Aloin etsiä dokumentaatiostamme vapaita IP-osoitteita. Katsoin hieman mallia aiemmista asiakkaan vastaavista palvelimista ja pääsin asiasta eteenpäin asian selvittämisessä. Huomasin, että aiemmat palvelimet oli lisätty keskitettyyn Reverse DNS tietokantaan. Aloin tutkia tietokantaa kunnes löysin seuraavan vapaan IP-osoitteen. Varasin IP-osoitteen palvelimelle ja tein sinne PTR-tietueen DNS-palveluun.

Tämän jälkeen asetin palvelimelle oikeat virtuaaliset verkkokortit, jotta ne liikennöivät oikeissa verkoissa. Palvelimelle laitoin yhden verkkokortin julkiverkkoa varten ja toisen asiakkaan sisäverkon liikennöintiä varten. Testasin myös, että liikenne ulospäin ja asiakkaan sisäverkkoon toimi. Tämän jälkeen siirryin päivittämään palvelimelle Windows tietoturvapäivityksiä. Katsoin vielä lopuksi muutamat perusmäärittelyt kuntoon, joita tavallisesti laitetaan palvelimille. Lopuksi vaihdoin palvelimelle Administrator-tunnuksen salasanan asiakkaan käyttämään tunnukseen ja ilmoitin asiakkaalle palvelimen valmistumisesta.

Viikkoanalyysi

Tämä viikko sujui kiireisissä merkeissä ja erilaisia työtehtäviä oli hyvinkin paljon. Palvelimiin ja virtualisointiin liittyviä työtehtäviä on nyt muutaman viikon ajan tullut vastaan tavallista enemmän. Itse koin tämän pelkästään positiivisena asiana, koska nämä teknologiat ovat itselleni kaikkein mielenkiintoisimpia.

Suurempia haasteita ei viikon aikana tullut vastaan. Hosting-palveluiden kanssa on lähes poikkeuksetta aina konsultoitava kyseisistä palveluista vastaavia asiantuntijoita, koska kyseisiin palveluihin liittyy aina jotain pieniä yksityiskohtia, joita ei välttämättä itse tule otettua huomioon. Lisäksi joitakin prosesseja tiettyjen palvelupyyntöjen osalta ei ole tarpeeksi hyvin kuvattu, joten tämäkin jo osaltaan lisää tarvetta kääntyä asiantuntijoiden puoleen pienemmissäkin asioissa.

Tähän analyysiin olen päättänyt sisällyttää pohdintaa virtualisoinnista yleisesti sekä siihen liittyviä alan käytäntöjä. Käytävät asiat eivät kaikki suoranaisesti kosketa omia työtehtäviäni ja minulla ei ole tällä hetkellä mahdollisuuksia päästä vaikuttamaan palveluissa käytettäviin teknologioihin. Uskon silti, että näistä tiedoista voi olla hyötyä jatkossa esim. erilaisissa vikojenselvitystilanteissa tai kun asiakkaan kysyvät tietoa palveluihin liittyen. Lisäksi nämä tiedot vahvistavat itsenäistä työskentelyäni virtualisoinnin parissa.

Käytettäviin teknologioihin liittyen meidän käytössä on VMWaren ohjelmistot virtualisointia varten. Tämän vuoksi se näkyy ensisijaisena lähteenä analyysissä. Pyrin myös löytämään muiden tahojen yleisiä mielenpiteitä virtualisointiin liittyen.

Yleisesti ottaen virtualisointia on jo tehty kauan aikaa, mutta vasta viime vuosina se on oikeasti noussut pinnalle ICT-alalla. Virtualisointia voidaan toteuttaa monella eri tapaa, kuten ohjelmien virtualisointi tai käyttöjärjestelmien virtualisointi, jotka ovat varmasti käytetyimmät menetelmät.

Aluksi voitaisiin tarkastella lyhyesti virtualisoinnin tuomia hyötyjä. Ensimmäisenä hyötynä voidaan pitää resurssien konsolidointia. Virtualisoinnin avulla yhdellä loogiksella resurssilla voidaan pyörittää monia eri sovelluksia, jotka normaalisti vaatisivat kaikki oman raudan tätä tehtävää varten. Tämä ei myöskään merkittävästi vaikuta virtualisoitujen sovellusten resurssienkäyttöön. (Intel 2014.)

Ohjelmien ja ympäristöjen testaus virtualisoinnin avulla helpottuu huomattavasti, kun uusia koneita ja sovelluksia voidaan provisioida mutkattomasti ja nopeasti. Provisioidut resurssit voidaan myös tehokkaasti eristää muusta ympäristöstä, joten niiden suorittaminen ei tuo ylimääräisiä riskejä tietoturvan tai resurssienkäytön näkökulmasta. Varmasti yhtenä mielenkiintoisimpana ominaisuutena voidaan pitää virtualisoinnin tuomaa vikasietoisuutta ja kuormanjakoa. Monet virtualisointiteknologiat tarjoavat mahdollisuuden tämän tyyppiselle toiminnalle. Hostit, joiksi normaalisti kutsutaan virtualisointialustoja, jotka pyörittävät virtuaalikoneita, osaavat jakaa keskenään virtuaalikoneiden tuomaa resurssienkulutusta. Mikäli yksi Host-kone kärsii kovasta CPU-utilisaatiosta, voidaan sillä pyöriviä virtuaalikoneita siirtää automaattisesti pyörimään toisella Hostilla. Samaa toiminnallisuutta hyödynnetään myös vikasietoisuudessa. Jos yksi Host lakkaa toimiasta, siirtyvät kaikki sen alla olevat virtuaalikoneet pyörimään seuraavalla vapaalla Hostilla ja näin toiminta virtuaalikoneilla jatkuu keskeytymättä. (Intel 2014.)

Seuraavaksi tarkastellaan hieman hyvänä pidettyjä käytäntöjä virtuaaalisointia suunnitellessa ja hallinnoidessa. Nämä seikat keskittyvät olennaisesti serveriympäristöjen virtualisointiin.

Onnistuminen virtualisoinnin toteuttamisessa vaatii tarkkaa suunnittelua jo alkuvaiheessa. Tässä tulee erityisesti ottaa huomioon oman ympäristön tarpeet sekä käytettävissä olevat resurssit. Pahimmillaan huonosti suunniteltu toteutus voi aiheuttaa merkit-

täviä lisäkustannuksia ja vähentää tuotantoympäristön tehokkuutta. Suorituskyky on myös yksi olennainen seikka, joka tulee ottaa huomioon virtuaalikoneita luodessa. On hyvä varmistaa, että virtuaalikoneelle allokoidaan tarpeeksi resursseja, jotta sen toiminta pysyy tehokkaana. (Solarwinds 2014.)

Oikean virtualisointiteknologia valitseminen yrityksen tarpeisiin on myös olennainen tekijä suunnitteluvaiheessa. Nykyään on olemassa monia eri toimittajia, jotka tarjoavat omia toteutuksiaan virtualisoinnista. Kaikilla näistä on omat hyvät ja huonot puolensa ja näitä kannattaakin tarkastella huolella, kun yrittää löytää sopivaa teknologiaa tarpeisiinsa. (Solarwinds 2014.)

Virtuaalikoneiden ylläpitoon liittyen on hyvä luoda erilaisia malleja tarvitsemista palvelimistaan. Esim. tietokanta -tai webpalvelimista on hyvä perustaa ns. Base Image, johon asennetaan kaikki näiden tarvitsemat ohjelmistot. Tämän jälkeen image tallennetaan johonkin keskitettyyn tallennusjärjestelmään, josta sitä voidaan käyttää aina kun uusia palvelimia tarvitsee luoda. Tämä vähentää merkittävästi aikaa, joka kuluu uusien palvelimien provisiointiin. (Solarwinds 2014.)

Viimeisenä tarkastellaan yhden valmistajan näkemyksiä hyvistä käytännöistä liittyen suorituskykyyn ja tallennusjärjestelmiin. Ohjeistukset liittyvät Vmwaren Vsphere teknologiaan, joka on meillä laajassa käytössä.

Ensimmäisenä on hyvä tarkistaa, että käyttämä laitteisto tukee kaikkia valmistajan teknologioita, joita ollaan aikeissa käyttää. Erityisen tärkeään on tarkastella käytettävien suorittimien yhteensopivuutta VMware käyttämien teknologienoiden kanssa esim. VMware VMotion, joka tarjoaa erilaisia ominaisuuksia virtuaalikoneiden vikasietoisuuteen ja kuormanjakoon liittyen. Lisäksi suorittimelta pitäisi löytyä tuki suoritintason virtualisointituelle, jolla saavutetaan merkittäviä tuloksia suorituskykyyn liittyen. Näitä teknologioita ovat eri valmistajilla esim. Intelin käyttämä VT-X sekä AMD:n AMD-V. (VMware 2014.)

Palvelinympäristön verkkolaitteiden suorituskyky on myös tärkeä ottaa huomioon kokonaiskuvassa. Huonosti suunniteltu verkko voi aiheuttaa pullonkauloja koko ympäristön suorituskykyyn. Valmistajan mukaan on suositeltavaa käyttää palvelintason verkkokortteja, jotka kykenevät suuriin tiedonsiirtonopeuksiin. Verkossa olevien kytkimien ja kaapeleiden on myös kyettävä toimimaan näillä nopeuksilla, jotta suorituskyky ei hidastu. (VMware 2014.)

Valmistajalla on myös omia suosituksiansa virtualisointialustoiden BIOS-asetuksiin. Oikein asetetuilla koneilla saadaan niistä irti maksimaalinen teho. Ensimmäiseksi suositellaan aina päivittämään koneiden käyttämät BIOS-versiot viimeisimpään valmistajaan tarjoamaan versioon. Suorittimista tulee ottaa käyttöön kaikki niiden tarjoamat suoritinytimet. Lisäksi, jos suoritin sitä tukee, on hyvä ottaa käyttöön Intelin kehittämä Hyper-Threading, joka mahdollistaa yhden prossessoriytimen jakamisen kahdeksi loogiseksi ytimeksi. Viimeisenä kannattaa myös säätää BIOS:in virransäästöasetukset niin, jotta ne tukevat parhainta suorituskykyä. Vaihtoehtoisesti ne voidaan määrittää myös käyttämään käyttöjärjestelmän määrittämiä asetuksia. (VMware 2014.)

3.10 Työviikko 43

Maanantai 20.10

Asiakas otti yhteyttä Service Deskiin sähköpostin välityksellä ja teki palvelupyynnön. Asia koski heidän palvelinkeskuspalveluitaan. Asiakkaalta oli viikkoa aiemmin poistettu yksi virtuaalikone, jolla ei ollut enää tuotannollista käyttöä. Tämän pyynnön ohessa asikas oli pyytänyt ottamaan koneen konfiguraation talteen heidän levyjärjestelmäänsä.

Nyt uudessa palvelupyynnössä asiakas ilmoitti, että olikin löytänyt poistetulle palvelimelle vielä jotain käyttöä ja halusi, että palvelin palautettaisiin tuosta aiemmin tallennetusta konfiguraatiosta. Otin tiketin itselleni hoitaakseni, koska en ollut aiemmin päässyt kyseistä toimenpidettä suorittamaan. Aloitin homman kirjautumalla asiakkaan palvelinympäristöön ja sieltä käynnistin Vsphere-hallintaohjelmiston. Palvelimen konfiguraatio oli tallennettu OVF-tiedostomuotoon, joka yleinen avoin pakkausmenetelmä virtuaalikoneiden tallentamista ja luomista varten.

Valitsin Vpshere ohjelman tiedostovalikosta komennon, joka tekee uuden virtuaalikoneen OVF-templatesta. Tämä aukaisi eräänlaisen interaktiivisen asennusohjelman, jossa palvelimelle kysyttiin nimeä sekä muuta peruskonfiguraatiota. Päätin palauttaa palvelimen oletusasetuksilla, jotta se olisi täysin samanlainen kuin aiemmin. Pistin kopioitumisen käyntiin ja tässä kesti noin viisi minuuttia. Kopioitumisen valmistuttua tarkastin, että koneessa oli kaikki oikeat määrittelyt ja sen jälkeen käynnistin virtuaalikoneen virran. Kirjauduin palvelimeen sisään käyttäen asiakkaan admin tunnuksia. Tarkastin koneella, että yhteydet toimivat normaalisti. Tämän jälkeen ilmoitin asiakkaalle, että palvelin oli palautettu kopiosta määritetyn mukaisesti. Asiakas kuittasi, että kaikki toimii ja sanoi ilmoittavansa kun palvelimen saisi jälleen poistaa lopullisesti.

Tiistai 21.10

Olin iltavuorossa työskentelemässä. Illan mittaan huomasin, että kaikki omat tikettini olivat siinä tilassa, että pystyisin ottamaan uusia tikettejä ratkottavaksi meidän jonosta. Niinpä otin jonosta vanhimman tiketin ja aloin ratkaisemaan sitä.

Tiketissä eräs asiakas pyysi muutoksia heidän kolmelle pääpalomuurilleen, jotka sijaitsivat kaikki eri maanosissa. Asiakkaan ympäristössä nämä palomuurit toimivat eräänlaisena Hub toimipisteenä, johon etätoimipisteet terminoivat kaiken liikenteensä sijainnista riippuen. Tiketissä pyydetty muutos liittyi näiden palomuurien toiminnallisuuteen ja tarkemmin Antivirus skannaukseen. Antivirus skannaus palomuurilla aiheuttaa lisää muistinkäyttöä, koska tarkastettava liikenne siirtyy palomuurin erilliseen proxy osioon. Tämä osio skannaa liikenteen ja sitten päättää päästetäänkö liikenne eteenpäin vai estetäänkö se. Oletuksena palomuurissa on asetus, joka lopettaa Antivirus skannauksen käsittelyn, jos palomuurin muisti ylittää yli 80 prosenttia. Tällöin uusille yhteyksille ei tehdä skannausta ollenkaan. Tämä tila päättyy, kun muistia on taas vapaana noin 70 prosenttia. Asiakas ei kuitenkaan halunnut palomuurien käyttäytyvän noin kyseisessä tilanteessa vaan pyysi, että palomuurin asetukset säädetään niin, että tuossa tilassa palomuuri ei ota vastaan uusia yhteyksiä ollenkaan, kunnes muistia on taas riittävästi saatavilla.

Avasin kaikkien kolmen palomuurin hallintaikkunat selaimella ja tein muutokset niihin vuorotellen. Tämä muutos piti tehdä palomuurin globaaleissa asetuksissa komentorivin kautta. Löysin oikean asetukset ja katsoin nykyisen arvon joka oli Pass. Tämä siis tarkoitti, että uudet yhteydet menevät ilman skannausta. Asetin tälle asetukselle arvon OFF, jotta palomuurin säästötilassa uudet yhteydet estetään, kunnes muistinkäyttö laskee tarpeeksi. Tämän jälkeen tallensin tekemäni muutokset ja otin palomuureista varmuuskopiot meidän verkkolevylle. Viimeiseksi ilmoitin asiakkaalle, että pyydetyt muutokset oli tehty ja pistin tiketin ratkaistuksi.

Keskiviikko 22.10

Sain erään tiketin hoitaakseni. Tiketti koski erään asiakkaan etätoimipistettä Unkarissa. Siellä oli menossa Internet palveluntarjoajan vaihtoprosessi. Asiakas oli ilmeisesti irtisanonut nykyisen linjan, jotta se päättyisi muutaman päivän kuluessa. Ongelmana oli, että asiakkaan uusi linja ei ollut vielä valmiina, sillä heiltä puuttui reititin siihen. Tiketissä asiakas tiedusteli, että voisiko palomuurille tehdä konfiguraation uutta yhteyttä varten, jotta se toimisi suoraan, kun paikalliset kytkevät sen kiinni.

Asiakkaalla oli vielä hieman epäselvää, että miten IP-osoitteet uudelle linjalla menisi. Lopulta asiakas ilmoitti, että ilmeisesti uusi linja käyttäisi staattista IP-osoitetta. Ilmoitin asiakkaalle, että uusi linja voitaisiin määritellä palomuurin vapaaseen porttiin, joka tässä tapauksessa oli Internal portti numero 13. Palomuuri oli oletusasetuksilla, joten kaikki Internal portit olivat kytkinmoodissa, jolloin ne käyttävät samaa IP-osoitetta. Ilmoitin asiakkaalle, että palomuuri täytyi käynnistää uudelleen, jotta portit saatiin eristettyä toisistaan asetuksella. Asiakas antoi tälle toimenpiteelle luvan, joten ryhdyin toimiin. Ensiksi ensimmäisestä Internal portista piti poistaa kaikki viittaukset, jotta muutos voitiin tehdä. Tämä sisälsi kaikki palomuurisäännöt sekä portin IP-osoitteen. Poistin nämä kaikki sekä laitoin portin alas hallinnollisesti.

Tämän jälkeen tein muutokset, jotta portit muuttuivat yksittäisiksi porteiksi. Tein myös ensimmäiseen Internal porttiin uudestaan IP-konfiguraation ja kohdistin siihen aiemmin tehdyt palomuurisäännöt. Katsoin, että kaikki näytti olevan ennallaan. Sitten siirryin konfiguroimaan Internal portti 13:sta. Asetin kyseiselle portille asiakkaan toimitta-

mat IP-osoitteet ja tein uuden oletusreitin kohdistumaan tälle portille ja sen takana olevaan reitittimeen. Muutin oletusreitin prioriteettia niin, että se ei vielä yliajaisi nykyistä yhteyttä. Tein vielä palomuurisäännöt, jotka sallivat yhteydet sisäverkosta ulospäin uuteen yhteyteen.

Tässä vaiheessa kaikki tarvittavat muutokset oli tehty, joten ilmoitin asiasta asiakkaalle. Asiakas vastasi viestiin ja ilmoitti, että he kytkevät uuden yhteyden vasta kahden päivän päästä. Kuittasin asiakkaalle, että asia oli kunnossa ja pistin tiketin Pending-tilaan. Tämän jälkeen siirryin tekemään muita tehtäviä.

Torstai 23.10

Sain erään tiketin hoitaakseni, joka oli ollut Service Deskin jonossamme jo hiukan aikaa. Tiketissä asiakas kyseli heidän nykyistä DHCP-konfiguraatiotaan, mutta ei maininnut, että mihin palveluun se liittyy. Päätin lähettää asiakkaalle viestin, jossa tiedustelin, että mihin palveluun tai laitteeseen kysely voisi olla. Asiakas tässä vaiheessa asiakas osasi vastata vain verkkosegmentin, jolle nykyinen DHCP-palvelu jakelee osoitteita.

Päätin ruveta oma-aloitteisesti selvittämään asiaa asiakkaan laitteilta. Tarkastin ensin asiakkaan pääpalomuurin, jossa oli DHCP-palvelu konfiguroitu muutamalle eri verkolle. Nämä eivät kuitenkaan ollut ne mitä asiakas haki kyselyssään. Seuraavaksi siirryin tarkastelemaan verkkokuvia asiakkaan ympäristöstä. Paikansin kaaviosta, että asiakkaan pääkonttorilla oli meidän hallinnoimia kytkimiä. Katsoin kirjautumistiedot asiakkaan toimipisteen runkokytkimeen ja otin SSH-yhteyden siihen.

Katsoin kytkimen konfiguraation läpi ja löysin sieltä asiakkaan etsimän DHCP-konfiguraation. Kytkimellä oli konfiguroitu IP-Helper parametreillä kaksi eri DHCP-palvelinta. Kyseisillä asetuksilla kytkin välittää kaikki siihen kytkettyjen koneiden DHCP-pyynnöt konfiguraatioissa määritetyille palvelimille. Ilmoitin asiakkaalle nykyisen konfiguraation kytkimellä. Asiakas ilmoitti, että he ovat lähiaikoina vaihtamassa DHCP-palvelimia ja tämän vuoksi toinen kytkimellä määritetyistä DHPC-palvelimista voitaisiin vaihtaa uuteen osoitteeseen. Poistin kytkimeltä olemassa olevat DHCP-määrittelyt ja korvasin ne asiakkaan antamilla tiedoilla. Tämän jälkeen kuittaisin asiak-

kaalle, että muutokset oli tehty. Asiakas ilmoitti, että testaa uuden DHCP-palvelun toiminnan seuraavana päivänä ja ilmoittaa tuloksista meille. Näillä tiedoilla pistin tiketin odottamaan asiakkaan vastausta.

Viikkoanalyysi

Viikko on taas mennyt edellisestä analyysista. Viikon aikana on taas tullut vastaan lukuisia uusia työtehtäviä ja erilaisia haasteita. Työviikko piti sisällään monia erilaisia ja eritasoisia työtehtäviä moniin eri palveluihin liittyen. Suurin osa työtehtävistä oli helppoja ja nopeita työpyyntöjä, joiden suorittamiseksi ei tarvittu erityistä pohdintaa tai konsultointia.

Työpyyntöjen haasteellisuuteen yleisesti ottaen suhtaudutaan niin, että Service Desk koittaa ratkaista mahdollisimman monet palvelupyynnöt tiimin sisällä ja sovittujen palveluaikojen mukaisesti. Lähtökohtaisesti Service Deskin työpyynnöissä voidaan konsultoida vanhempia asiantuntijoita, mikäli työpyyntö tätä vaatii. Jos työpyynnön tai ongelmanselvitykseen menee normaalia kauemmin aikaa, voidaan se siirtää seuraavan tason tutkittavaksi. Tällöin Service Deskin resurssit vapautuvat muiden töiden suorittamiseen.

Viime analyysissä aloitin käsittelemään virtualisointia ja sitä miten se liittyy Service Deskin työskentelyyn. Analyysissä käytiin läpi yleisiä seikkoja virtualisoinnin implementointiin ja valmistajien suosituksia niiden ylläpitoon. Tässä analyysissä jatkan aiheen tutkimista. Aluksi voitaisiin käydä hieman läpi viime kerralla aloitettua aihetta virtualisoinnin suorituskykyyn liittyen.

VMwaren virtualisointiteknologia toimii valmistajan oman ESXi-käyttöjärjestelmäkerroksen päällä. Koneita, jotka pyörittävät ESXi:tä sanotaan Hostiksi. Ensisijaisen tärkeää Hosteilla on säätää BIOS:issa kaikki mahdolliset virransäätöasetukset tukemaan maksimaalista suorituskykyä. Tämän lisäksi ominaisuudet jota ei tarvita omassa ympäristössä on hyvä kytkeä pois päältä, jolloin saavutetaan paras suorituskyky. Sama koskee alustalla pyöriviä virtuaalikoneita. Virtuaalikoneista kannatta esim. kytkeä

pois päältä kaikki optiset asemat, koska nämä saattavat aiheuttaa käyttöjärjestelmästä riippuen ylimääräistä kuormaa prosessorille. (VMware 2014.)

Hostien prosessorien käyttökuormitusta olisi hyvä tarkkailla säännöllisin väliajoin. Yleisesti ottaen 80:nen prosentin kuormitusta voidaan pitää vielä siedettävä rajana, mutta 90 prosenttia ja sen ylittävien määrien kanssa kannattaa jo harkita resurssien organisoimista uudelleen. Yleensä klusterissa olevat Hostit osaavat jakaa automaattisesti kuormaa niin, että yksittäinen Host ei kuormitu liikaa. Mikäli koko klusterin laskentateho alkaa lähestyä maksimitasoa, tällöin olisi hyvä lisätä laskentatehoa klusteriin lisäämällä siihen uusia Hosteja. (VMware 2014.)

Aiemmassa analyysissä oli mainintaa mallipohjien käytöstä virtuaalikoneiden kanssa. Valmistajan suositusten mukaisesti niiden käyttäminen on erittäin suotavaa. Yksinkertaisesti oleellisin syy niiden käyttöön on tehokkuus. Mallipohjien kanssa uusien virtuaalikoneiden provisiointi on erittäin nopeaa ja helppoa, kun malli sisältää kaikki tarvittavat ohjelmistot, mitkä ovat oleellisia niiden hallinnassa. Malleja kannattaa tehdä yksi jokaiselle tarvitsemalleen käyttöjärjestelmälle ja niiden eri versioille. (VMware 2014.)

Yrityksemme päivittäisessä tekemisessä hyödynnetään tehokkaasti näitä käytäntöjä. Meillä käytetään aktiivisesti mallipohjia virtuaalikoneiden kanssa. Niitä löytyy kaikille tukemillemme käyttöjärjestelmille. Malleja myös päivitetään säännöllisesti, jotta niiden sisältämät ohjelmistot pysyvät ajan tasalla.

Toinen oleellinen seikka virtuaalikoneiden ylläpidossa on niiden varmistaminen ja suojaaminen. On tärkeää, että koneista saadaan eritasoisia varmuuskopioita ja niitä voidaan käyttää tarvittaessa. Helpoin ja nopein tapa varmuuskopioida virtuaalikoneiden konfiguraatiota ja tietoa on käyttää snapshotteja. Nämä snapshotit tallentavat virtuaalikoneen sen hetkisen tilanteen ja luovat siitä imagepohjaisen tallenteen. Snapshotit ovat käteviä varmuuskopioita varsinkin, kun virtuaalikoneisiin tehdään kriittisiä muutoksia. Snapshottien avulla virheen sattuessa kone pystytään palauttamaan nopeasti aikaisempaan tilanteeseen. Snapshottien käyttöä ei kuitenkaan suositella varsinaisen varmuuskopioinnin menetelmänä, sillä ne voivat viedä äkillisesti paljon levytilaa, kun virtuaalikoneen koko kasvaa. Pidempiaikaista säilytystä varten koneesta kannattaa mieluummin

tehdä kloonaus, kun ottaa snapshotteja. Hyvänä käytäntönä pidetäänkin, että snapshotit otetaan ennen virtuaalikoneesen tehtäviä muutoksia ja poistetaan heti, kun virtuaalikoneen toiminta on todettu vakaaksi. (Davis 2014.)

Perinteinen toteutus, jota käytetään fyysisten palvelimienkin kanssa, on agenttipohjainen tiedostotason varmuuskopiointi. Tässä ratkaisussa ohjelmisto ottaa koneen sisällöstä tiedostotason varmuuskopioinnin ja tiedostot siirtyvät johonkin keskitettyyn järjestelmään. Tämän lisäksi on vielä hyvä käyttää varmuuskopiointimenetelmiä, jotka osaavat ottaa virtuaalikoneista levytason varmuuskopioita ja siirtää niitä etäisiin kohteisiin. Tämä nopeuttaa palautusprosessia jos paikallisessa ympäristössä tulee laajempia ongelmia. Parhaimpana käytäntönä onkin hyvä yhdistää näitä kaikkia varmuuskopioinnin menetelmiä ja saavuttaa parhaat puolet jokaisesta. (Davis 2014.)

Yrityksessämme on käytössä muutamia eri käytäntöjä varmuuskopiointiin liittyen. Näissäkin pyritään käyttämään alan hyviä käytäntöjä. Oletuksena kaikista virtuaalikoneista otetaan automaattisesti snapshotteja säännöllisin väliajoin. Nämä tallenteen poistuvat myös automaattisesti, jotta ne eivät vie ylimääräistä tilaa levyjärjestelmässä. Asiakkailla on myös mahdollisuus ostaa varmuuskopiontiin liittyvää varsinaista palvelua, jolloin koneista otetaan ennalta määritetyin väliajoin täysi tiedostopohjainen varmuuskopiointi. Tiedostojen palautus on asiakkaalle aina erikseen laskutettavaa työtä. Virtuaalikoneet käyttävät levyjärjestelmiä tallennukseen. Levyjärjestelmistä on myös mahdollista ottaa levytason varmuuskopioita palautusta varten. Asiakkaan on vielä mahdollista ostaa tähän lisäpalvelu, jolla levyjärjestelmät saadaan peilattua fyysisesti toiseen lokaatioon.

3.11 Työviikko 44

Maanantai 27.10

Aloitin työviikkoni, joka oli tällä kertaa yövuorossa. Olin saanut kollegaltani erään asiakkaan tiketin, joka soveltui parhaiten tehtäväksi yövuorossa sen laajuuden vuoksi. Tiketissä asiakas pyysi tarkastamaan useiden etätoimipisteiden monitorointipalveluiden

tilanteen. Monitorointipalveluilla mitataan asiakkaan palomuurien erilaisia statistiikkoja niiden suorituskyvystä ja muista mielenkiintoisista seikoista.

Tiketissä asiakas toimitti Excel-taulukon, joka sisälsi kaikki etätoimipisteet, joista piti tarkastaa, että monitorointi toimii oikein ja lisätä puuttuvat kohteet. Meillä on käytössä useampia sovelluksia valvontaa varten, mutta tässä tiketissä oleellisimmat olivat vapaaseen lähdekoodin perustuva Cacti sekä CA:n Performance Center ohjelmistot.

Siirryin ensin Cactiin tarkastelemaan valvottavia laitteita. Kävin asiakkaan antamaa listaa järjestyksessä läpi ja katsoin kaikki laitteet läpi. Muutamia laitteita näytti puuttuvan listasta, joten lisäsin ne manuaalisesti järjestelmään. Laitteen valvontaan laitoin vielä lisäksi muutamia valmiiksi määritettyjä graafeja, joita järjestelmä generoi laitteen valvontaa hyödyntämällä. Laitteiden valvontadataa kerätään SNMP-palvelun avulla, joka käyttää UDP-protokollan porttia 161. Laitteen lisäämisen jälkeen katsoin, että siitä alkoi generoitua dataa järjestelmään.

Tämän jälkeen siirryin seuraavaan valvontajärjestelmään ja aloin taas käydä läpi asiakkaan toimittamaa listaa. Katsoin järjestelmän hakutoiminnolla yksitellen läpi, että kaikki tarvittavat laitteet löytyivät listalta. Huomasin, että aika moni laitteista puuttui valvonnasta. Aloitin urakan näiden laitteiden lisäämiseksi. Järjestelmästä käsin laitteiden lisääminen ei ole kovin monimutkaista. Asiakkaalle on luotu oma säiliö järjestelmään, minne uudet laitteet lisätään niiden IP-osoitteen perusteella. Palomuureilla pitää olla reitityksset kunnossa sekä SNMP-asetukset tulee olla konfiguroitu niin, että ne hyväksyvät SNMP-kyselyt järjestelmästä.

Lisättäviä laitteita oli sen verran monta ja järjestelmiä kaksi johon niitä piti lisätä. Päätin, että jaan tämän urakan tuleville öille, jotta ehdin tekemään vuorojen aikana muitakin tikettejä.

Tiistai 28.10

Sain asiakkaalta tiketin ratkaistavaksi. Tiketissä asiakas viittasi aiemmin kesällä ilmenneeseen ongelmaan, johon ei ollut silloin saatu ratkaisua. Asiakkaalla oli sisäverkossaan käytössä eräs Citrix-palvelu johon ei enää pääsy toiminut muualta kuin samasta aliverkosta. Tämä oli lakannut toimimasta aiemmin, kun asiakkaan kuituyhteys kahden toimipisteen välillä oli katkennut ja yhteys oli siirtynyt varayhteydelle. Tällä hetkellä pääyhteys oli jo ollut käytössä jo jonkin aikaa. Pääsy palveluun ei silti näyttänyt toimivan.

Kirjauduin asiakkaan pääpalomuurille sisään ja koitin pingata kyseistä palvelun IP-osoitetta, mutta se ei vastannut. Tämän jälkeen rupesin paikantamaan missä tämä palvelu sijaitsi fyysisesti. Hetken aikaa tarkasteltuani asiakkaan dokumentaatiota kirjauduin asiakkaan runkokytkimelle. Tarkastelin kytkimen ARP-taulua ja näin kyseisen IP-osoitteen. Tämä ei ollut normaalissa tilassa, sillä MAC-osoitetta tuolle IP-osoitteelle ei näkynyt. Näin ollen tein olettamuksen, että kyseiseen osoitteeseen ei voitu kommunikoida.

Tiedustelin asiakkaalta palvelimen IP-konfiguraatiota. Asiakas toimitti tiedot palvelimesta ja sen MAC-osoitteesta. Kävi ilmi, että kyseessä oli kaksi eri palvelinta, joilla oli eri IP-osoitteet, mutta palvelimet käyttivät yhtä samaa IP-osoitetta kuormanjakoon liittyen. Tässä tilanteessa meidän hallinnoima asiakkaan kytkin kuitenkin näki kaksi eri IP-osoitetta samalla MAC-osoitteella. Tästä päättelin, että liikenne ei näin voisi toimia.

Palvelimilla oli myös käytössä omat yksilölliset IP-osoitteensa käytössä ja nämä näyttivät vastaavan kytkimelle normaalisti. Ohjeistin asiakkaalle, että yhteys toimisi käyttäen näitä osoitteita suoraan. Tässä vaiheessa jätin tiketin siihen tilanteeseen odottamaan ja päätin konsultoida vanhempia kollegoitani asiaan liittyen seuraavana päivänä.

Keskiviikko 29.10

Otin meidän Service Deskin jonostamme tiketin itselleni käsittelyyn. Tiketti oli vaihteeksi vähän suoraviivaisempi muutospyyntö asiakkaan palomuuripalveluun. Tiketissä asiakas oli käynyt keskustelua kolmannen osapuolen välillä ja viesteistä ilmeni, että asi-

akkaalle pitäisi rakentaa uusi Site-to-Site VPN-tunneli kolmannen osapuolen kanssa. Viesteistä kävi myös ilmi hieman tietoa yhteystarpeista. Ilmeisesti kolmannen osapuolen oli tarkoitus päästä käsiksi asikkaan Domain Controller palvelimiin VPN-yhteyden välityksellä.

Tikein aiemmissa viesteissä oli hieman teknisiä tietoja VPN-yhteyden määrittelyyn liittyen. Halusin kuitenkin hoitaa homman tarkasti, joten lähetin kolmannelle osapuolelle lomakkeen VPN.-yhteyden luomista varten ja sanoin, että tunnelin salausavaimen voisimme lähettää tekstiviestillä teknisen henkilön matkapuhelimeen. Tämä on meillä normaali käytäntö salausavaimien toimittamisen kanssa.

Jonkin ajan kuluttua asiakkaan kumppani lähetti sähköpostilla vastauksen, jossa oli VPN-yhteyden lomake täytettynä heidän haluamillaan parametreilla. Siirryin asiakkaan palomuurille tekemään konfiguraatiota. Syötin VPN-tunnelin määrittelyihin vastapuolen palomuurin julkisen IP-osoitteen. Lomakkeessa oli määritettynä, että IKE-neuvottelussa käytetään salaukseen AES265-protokollaa ja hashina SHA1-protokollaa. Diffie-Helman groupiksi määriteltiin viisi. Avaimen elinajaksi asetettiin 480 minuuttia.

Näiden määrittelyjen jälkeen siirryin tekemään phase2 konfiguraatioita tunneliin. Näihin tuli samat parametrit kuin ensimmäisen vaiheen neuvottelussa. Lisäksi määrittelin tunneliin suojatut verkot. Asiakkaan puolelta hosteiksi määriteltiin heidän kaksi Domain Controller-palvelintaan ja toisessa päässä määriteltiin yksi host heidän käyttämälleen palvelimelle. Viimeiseksi tein staattisen reitin osoittamaan vastapuolen verkkoon ja tein palomuurisäännöt, jotka sallivat liikenteen molempiin suuntiin. Tämän jälkeen laitoin viestiä, että tunneli oli määritelty meidän päässä ja samalla lähetin tunnelin salausavaimen kolmannen osapuolen tekniselle henkilölle. Jonkin ajan kuluttua asiakas vastasi viestiini ja ilmoitti, että tunneli toimi odotetulla tavalla.

Viikkoanalyysi

Viimeinen analysoitava työviikko on nyt vihdoin takana. Työviikkoni kului yövuorossa, joten työnteko meni melko rauhallisissa merkeissä. Kokonaisvaltaisesti tikettien määräkin näytti olevan laskussa verrattuna edellisiin viikkoihin. Työtehtävät koostuivat lähinnä tiketeistä, joita päivävuoro ei ollut ehtinyt tekemään. Lisäksi minulla oli muutama ennalta sovittu palomuuripäivitys asiakkaiden laitteisiin.

Mitään merkittäviä haasteita ei viikon aikana työtehtävissä tullut vastaan. Tästä huolimatta minulla oli muutamia hieman enemmän aikaa vieviä tikettejä jonossani, joita jouduin laittamaan kollegoiden suoritettavaksi päivävuoroon.

Viikon aikana kerkesin myös muutaman tunnin kuluttaa meidän sisäisen dokumentoinnin tarkasteluun liittyen uusiin tuleviin palveluihin, joita asiakkaille aletaan tarjoamaan. Näihin liittyen katselin erilaisia esityksiä ja videoita, joita oli päiväsaikaan esitelty muille kollegoille.

Tähän viimeiseen viikkoanalyysiin tuli mieleeni vielä käydä lyhyesti ja yleisellä tasolla asioita, joita Service Desk työskentelyssä tulisi ottaa huomioon. Tämä ei suoranaisesti liity aiempaan ITIL-aiheiseen analyysiini, vaan käsittelee enemmän tekemistä ja käytäntöjä päivittäisessä työskentelyssä. Analyysissä keskitytään myös asiakkaan kanssa käytävään kommunikointiin ja hyvään asiakaspalveluun. Nämä ovat seikkoja, joihin meidän yrityksessä erityisesti kiinnitetään huomiota, jotta saavutettaisiin paras mahdollinen asiakaskokemus.

Ensimmäiseksi käydään läpi hieman asioita, joihin Service Deskin piirin kuuluvilla henkilöillä on mahdollista vaikuttaa omalla tekemisellään. Näistä seikoista ensimmäinen ja ehkä tärkein osa-alue on työntekijän asenne. Kaikenlaisiin työtehtäviin Service Deskissä pitäisi aina lähteä asenteella, jossa haetaan ratkaisuja asiakkaan ongelmiin ja haasteisiin. Tässä auttaa, kun ymmärtää mitä asiakas tarvitsee ja toimii sen mukaan. Asiakkaalle voidaan myös tarjota ratkaisuja, joita he eivät itse ole tulleet ajatelleeksi. Asenne ratkaisee varsinkin silloin, kun viestitään asiakkaan kanssa puhelimitse. (Peter McGarahan 2012)

Omassa Service Deskissämme pyrimme aina ymmärtämään asiakkaan ongelmat ja tarjoamaan niihin järkevimmät ratkaisut. Mikäli asiakkaalla on palveluissaan kriittisiä ongelmia, suhtaudutaan niihin vakavasti ja pyritään ratkaisut niihin löytämään tehokkaasti. Lisäksi pyrimme antamaan asiakkaalle aina kuvan, että asiat kuin asiat saadaan hoidettua ammattimaisesti alusta loppuun.

Tiimityösketely Service Deskissä on yksi avain sen onnistuneeseen toteutukseen. Vastuun ja työtehtävien jakaminen tasaisesti tiimin kesken sekä alan parhaiden käytäntöjen soveltaminen päivittäisessä työskentelyssä takaavat Service Deskin onnistumisen nykypäivän vaativissa olosuhteissa. Työntekijöiden tulisi kaikkien tiedostaa koko tiimin yhteiset tavoitteet ja toteuttaa niitä parhaansa mukaan. Tämä saavutetaan parhaiten kommunikoimalla avoimesti kollegoiden kanssa ja auttaen aina, kun mahdollista. Myös huolellinen dokumentointi tikettien kanssa takaa sen, että kollegat pystyvät jatkamaan ongelmien selvittelyä ilman, että asiakkaalta täytyy tiedustella lähtötiedot tilanteeseen alusta alkaen.(McGarahan 2012.)

Proaktiivisuus on myös hyvä keino lisätä tiimin tehokkuutta ja luottamusta asiakkaan suuntaan. Tätä voidaan toteuttaa esim. seuraamalla aktiivisesti toistuvia ongelmia asiakkaiden palveluissa ja pyrkimällä löytämään ratkaisuja näihin. Näissä voidaan käyttää apuna erilaisia työkaluja kuten valvontasovelluksia, jotka generoivat arvokasta dataa asiakkaan palveluihin liittyen. (McGarahan 2012.)

Nämä edellä mainitut seikat ovat ensisijaisen tärkeitä yrityksessämme, sillä tuotamme asiakkaille palveluita, joilla pyritään tuottamaan lisäarvoa asiakkaan harjoittamaan liiketoimintaan.

Jatkuva kouluttautuminen on myös yksi ehto menestyvälle palveluntarjoajalle. Henkilöstön kouluttaminen tuo lisää kaivattua ammattitaitoa tiimiin ja lisää työntekijöiden motivaatiota työtehtäviin. Service Deskin tehokkuutta voidaan parantaa entisestään myös tarjoamalla parhaat käytettävissä olevat ohjelmistot henkilöstön käyttöön. (Gray 2012.)

Yrityksessäni on alusta asti panostettu henkilöstön koulutukseen. Tällä taataan, että eri teknologioihin löytyy osaajia ja työntekijöillä on mahdollisuus syventyä uusiin asioihin. Myös sisäistä koulutusta järjestetään aina, jos tarjoamiimme palveluihin tai käytäntöihin tulee merkittäviä muutoksia.

Viimeisimpänä seikkana voidaan mainita laadunmittaus. Tarjottavia palveluita kannattaa jatkuvasti mitata eri näkökulmista. Näin saadaan hyödyllistä tietoa Service Deskin onnistumisesta. Asiakkaille on myös hyvä antaa mahdollisuus palautteeseen. Palautteita tarkastelemalla voidaan parantaa omia palveluita vastaamaan paremmin asiakkaiden tarpeita. Näillä keinoilla saavutetaan lopuksi myös parempi asiakastyytyväisyys. (Gray 2012.)

Meillä laadunmittausta suoritetaan jatkuvasti käyttäen omaa Service Desk-järjestelmäämme, josta saamme statistiikka kaikista tehdyistä tiketeistä. Näiden perusteella tiimin suorituksia mitataan ja asetetaan tavoitteita tulevaisuudelle. Asiakkaiden tyytyväisyyttä mitataan säännöllisissä palavereissa, joissa asiakas arvioi palveluiden toimivuutta ja Service Deskin toimintaa. Palautteiden perusteilla tehdään muutoksia toimintatapoihin, mikäli tämä nähdään tarpeellisena.

4 Pohdinta ja päätelmät

Yhdentoista viikon pituinen seurantajakso on nyt viimein ohi. Päivittäiset päiväkirjamerkinnät ja viikoittaiset analyysit on nyt tehty. Näitä analyyseja tehdessä on opittu omasta tekemisestä erilaisia hyödyllisiä asioita. Seuraavaksi on tarkoitus käydä läpi kaikki mitä on tapahtunut kuluneen yhdentoista viikon aikana ja pohtia mitä tämän työn tekemisestä on jäänyt mieleen.

Ensimmäiseksi voitaisiin käydä hieman läpi omaa kehittymistä kuluneen syksyn ajalta. Seurantajakson aikana ehti tulla vastaan paljon erilaisia työhön liittyviä haasteita ja niistä selvittiin hyödyntämällä erilaisia resursseja sekä tekemällä yhteistyötä kollegoiden kanssa. Muutaman ensimmäisen viikon ajan keskityin analyyseissä käsittelemään langattoman verkon palveluihin liittyvää tietoa. Analyyseissä selvitin erilaisia näkökulmia langattoman verkon ongelmatilanteisiin liittyen. Ongelmatilanteita voi ilmetä langattoman verkon asiakaslaitteilla sekä verkkoja hallitsevilla laitteilla. Analyysissä tarkastelin, että miten näitä erilaisia ongelmatilanteita kannattaa lähteä selvittämään ja mitä asioita tulee ottaa huomioon ongelmien selvittelyssä. Tarkasteltujen asioiden avulla opin paremmin ymmärtämään vianselvityksessä tarvittavia tietoja ja soveltamaan tätä tietoa tositilanteissa.

Seuraavissa analyyseissä keskityttiin tarkastelemaan ITIL-viitekehystä ja sen näkyvyyttä omassa työskentelyssä. Analyyseissä käytiin läpi hyviä käytäntöjä, joita ITIL-viitekehys tarjoaa. Näitä käytäntöjä noudattamalla voidaan yrityksen IT-palveluiden toimintaa tehostaa entisestään ja siihen saadaan tietynlaista selkeyttä. ITIL-viitekehystä noudattamalla voidaan mahdollisesti saavuttaa myös taloudellisia hyötyjä erilaisten toimenpiteiden lopputuloksena. Analyysissä tarkasteltiin myös ITIL:in näkyvyyttä omassa päivittäisessä työskentelyssä sekä yrityksen prosesseissa. Analyysin aikana tarkentui, että ITIL on vahvasti mukana yritykseni Service Desk toiminnassa. Samalla opin myös ymmärtämään paremmin sisäisiä prosessejamme, jotka sisältävät vahvasti vaikutteita ITIL-viitekehyksestä. Yrityksen prosessien suunnittelussa on otettu huomioon alan hyvät käytännöt ja tämän tiedon pohjalta prosesseja on muokattu vielä sopimaan paremmin yrityksen omiin tarpeisiin.

Työn seuraavissa analyyseissä käytiin läpi asiaa liittyen yrityksemme tarjoamiin palveluihin. Näissä keskityttiin erityisesti palomuureihin ja virtualisointiin liittyviin asioihin. Analyyseissä käytiin läpi erilaisia hyviä käytäntöjä, joita voidaan ja kannattaakin hyödyntää työelämän ympäristöissä. Käsiteltyjä asioita olivat mm. tietoturvallisuuden lisääminen palomuurien hallinnoinnissa sekä virtualisointiympäristöjen optimointi ja parhaat käytännöt. Käytyjen asioiden avulla olen pystynyt kehittämään omaa tekemistä päivittäisissä työasioissa. Palomuurien hallinnoinnissa olen oppinut miten niiden sääntökantoja kannattaa rakentaa ja ylläpitää, jotta tietoturva voidaan maksimoida. Olen oppinut näkemään asiakkaiden ympäristöjä eri tavalla ja pystynyt tuomaan omia näkemyksiäni niihin liittyen. Erilaisissa palvelutilanteissa olen pystynyt ehdottamaan asiakkaalle parempia ratkaisuja, jotka ovat lähempänä alan hyviä käytäntöjä.

Työn tekemisen aikana olen myös löytänyt hieman erilaisia ratkaisumalleja omaan tekemiseeni. Olen oppinut myös hyödyntämään enemmän saatavilla olevia sisäisiä ja ulkoisia lähteitä. Ongelmien selvittelyissä olen oppinut noudattamaan enemmän johdonmukaisempia ratkaisutapoja. Ongelmien esiintyessä olen kerännyt enemmän lähtötietoja asiakkaalta ongelman selvittämiseksi. Tämän tiedon pohjalta olen saanut paremmat mahdollisuudet ongelman tehokkaaseen ratkaisemiseen.

Palvelupyyntöjen osalta olen saanut tehostettua omaa toimintaani tekemällä muutamia muutoksia toimintatapoihin. Isompien muutosten osalta olen oppinut tarkastelemaan koko tilannetta laajemmalta näkökulmalta. Tätä soveltaen olen pyrkinyt tehostamaan työskentelyä vähentämällä toistuvan manuaalisen työn määrää. Tämä onkin osoittautunut monissa tilanteissa erittäin hyödylliseksi toimintatavaksi. Olen myös havainnut, että oman työajan käyttö on tehostunut joissakin tilanteissa.

Opinnäytetyön kirjoittamisen aikana sisäisten prosessien ymmärtäminen on omalla osallani kehittynyt. Työympäristössäni on seurantajakson aikana tapahtunut muutamia muutoksia organisaatiotasolla sekä tekemisen määrä on kasvanut. Tästä johtuen olen havainnut, että joidenkin prosessien kohdalla löytyy selkeästi parannettavaa. Olen myös huomannut, että joihinkin asioihin ei selkeitä prosesseja löydy ollenkaan. Olen tuonut

omia näkemyksiäni esille ja oman tiimini kanssa olemme näitä yhdessä käyneet läpi. Joitakin ehdotuksia olemme saaneet vietyä eteenpäin korkeammalle tasolle käsiteltäväsi.

Työn tekemisen aikana olen oppinut paljon mielenkiintoisia asioita omasta työskentelystäni. Ennen opinnäytetyön tekemistä minulla oli herännyt kysymyksiä moniin asioihin, joita yrityksessäni tehdään. Kaikista asioista en aina ymmärtänyt, että miksi ne on tehty kyseisellä tavalla. Saatoin myös itse pohdiskella, että miten asioita saataisiin tehtyä paremmin. Opinnäytetyön tekemisen aikana nämä askarruttaneet asiat ovat selkiintyneet minulle paremmin. Olen oppinut ymmärtämään paremmin yrityksessä tehtyä ratkaisuja ja oppinut myös itsenäisesti pohtimaan parannuksia niihin.

Tällä hetkellä olen yleisesti tyytyväinen omaan tekemiseeni Service Deskissä. Aion jatkossakin pyrkiä kehittämään omaa tekemistäni ja osaamistani. Service Deskissä työskentely on tällä hetkellä itselleni mieluisaa ja pidän sitä erittäin opettavaisena työnä tulevaisuutta ajatellen. Tulevaisuudessa tarkoituksena on edistyä vaativampiin asiantuntijatehtäviin.

Lähteet

Algosec 2014. The big collection of firewall management tips. Luettavissa: http://www.algosec.com/resources/files/whitepapers/Tips-Book-Final.pdf. Luettu 13.10.2014

Ashford Global 2014. 5 Key Benefits of Implementing ITIL. Luettavissa: http://www.ashfordglobalit.com/training-blog/itil-tips-and-training/5-key-benefits-of-implementing-itil.html. Luettu 21.9.2014

Aruba Networks 2007. Aruba Troubleshooting Cheat Sheet. Luettavissa: http://community.arubanetworks.com/aruba/attachments/aruba/84/106/1/Troubleshooting+Cheat+Sheet-.pdf. Luettu 31.8.2014

Axelos 2014. What is ITIL?. Luettavissa: http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx. Luettu 14.9.2014

Davis, D. 2014. Top 10 best practices of Backup and Replication for VMware and Hyper-V. Luettavissa: http://www.championsg.com/includes/pdfs/Top-10-Best-Practices-of-Backup-for-VMware-and-Hyper-V.pdf. Luettu 26.10.2014

Fortinet 2014. FortiOS Handbook Best Practices. Luettavissa: http://docs.fortinet.com/uploaded/files/1954/Best_Practices_52.pdf. Luettu 27.9

Gray, G. 2012. Help desk best practices - Top 10 tips to improve end-user satisfaction and lower costs. Luettavissa: http://www.abc.net.au/technology/articles/2012/10/30/3621583.htm. Luettu 2.11.2014

HP 2014. Troubleshooting Wlan Connectivity. Luettavissa:
http://www.hp.com/rnd/pdfs/Troubleshooting_WLAN_Connectivity.pdf.
Luettu 5.11.2014

Infosec 2008. VPN Security. Luettavissa:
http://www.infosec.gov.hk/english/technical/files/vpn.pdf.
Luettu 5.10.2014

Intel 2014. The Advantages of using Virtualization Technology in the Enterprise. Luettavissa: https://software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise.
Luettu 20.10

ITIL Foundation 2008. Service Desk Objectives in ITIL Foundation. Luettavissa:
http://www.itilfoundation.org/Service-Desk-Objectives-in-ITIL-Foundation_43.html.
Luettu 15.9.2014

McGarahan, P. 2012. The top 10 Service and Support best practices. Luettavissa:
http://www.supportindustry.com/asktheexpert/toptenbestpractices.htm.
Luettu 1.11.2014

Musthaler, L. 2014. Best practices for firewall management. Luettavissa:
http://www.networkworld.com/article/2452587/network-security/best-practices-for-firewall-management.html.
Luettu 12.10.2014

Solarwinds 2010. Server Virtualization Best Practices. Luettavissa:
http://www.solarwinds.com/resources/whitepapers/server_virtualization_best_practices.pdf.
Luettu 21.10.2014

The Stationary Office 2010. Executive Briefing: The Benefits of ITIL. Luettavissa: http://www.best-management-practice.com/gempdf/ogc_executive_briefing_benefits_of_itil.pdf. Luettu 22.9.2014

Unique Micro Design, Aruba Networking Wireless- Access Points, Kuva. Luettavissa: http://www.umd.com.au/itd/products/aruba.html Luettu 7.9.2014

VMware 2014. Performance Best Practices for VMware vSphere® 5.5. Luettavissa: http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.5.pdf. Luettu 21.10.2014

VMware 2014. Virtual Center2; Templates Usage and Best Practices. Luettavissa: http://www.vmware.com/pdf/vc_2_templates_usage_best_practices_wp.pdf. Luettu 26.10.2014