LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Tietoturvallisen laboratorioverkon suunnittelu ja rakentaminen – Case KPMG Oy Ab

Lehmonen Emil

2018 Laurea

LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Tietoturvallisen laboratorioverkon suunnittelu ja rakentaminen - Case KPMG Oy Ab

Lehmonen Emil
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kesäkuu, 2018

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Tradenomi

Lehmonen Emil

**Tietoturvallisen laboratorioverkon suunnittelu ja rakentaminen – Case KPMG Oy Ab**

Vuosi 2018 Sivumäärä 20

Opinnäytetyön tavoitteena oli suunnitella laboratorioverkoksi kutsutun lähiverkkoympäristön uudistus ja aloittaa sen toteutus. Toimeksiantajana oli KPMG Oy Ab, jonka tietoturvapalveluiden kokonaisuus käyttää laboratorioverkkoa asiakastoimeksiantojen toteuttamiseen. Tarkoituksena on kehittää ympäristöä paremmaksi ja helpommin hallittavaksi palvelualustaksi.

Työn tietoperustana toimivat tietoturvan keskeiset käsitteet, kuten CIA-malli ja Paul Silfverbergin hankesuunnittelun menetelmät sekä toimeksiantajan määrittelemät tietoturvallisuuden vaatimukset. Tiedonkeruumenetelmänä käytettiin haastatteluja laboratorioverkon käyttäjäryhmien jäsenille. Haastattelujen tulokset selvensivät keskeiset uudistuksen kohteet ja vaatimukset ympäristön kehitykselle.

Tuotoksena syntyi projektin toteutussuunnitelma, joka kuvaa uudistuksen vaatimat toimet. Tavoitteena oli myös aloittaa uudistuksen vaatima ympäristön uudelleenrakennus. Uudistuksen ensimmäinen vaihe alkoi aikataulun mukaisesti, mutta se ei valmistunut aikataulussaan. Opinnäytetyön tulokset nostavat projektisuunnittelun tärkeyden esille erityisesti ajallisten resurssien sekä työntekijäresurssien osalta.

Asiasanat: tietoturva, lähiverkko, projektisuunnittelu

**Laurea University of Applied Sciences** **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Lehmonen Emil

**Designing and Building of a Secure Laboratory Network – A Case Study of KPMG Oy Ab**

Year 2018 Pages 20

The purpose of this bachelor's thesis was to plan a redesign of a local area network called laboratory network and start rebuilding it. The commissioner is KPMG Oy Ab whose cybersecurity services use the laboratory network to carry out client assignments. The purpose of the redesign project is to develop the environment to be better and easier to administer as a service platform.

The essential cyber security concept CIA triad, project planning methods of Paul Silfverberg and standards for the environment defined by the commissioner work as a knowledge base for the thesis. Interviews, conducted on the user groups that use the laboratory network, were used as a method of data collection. The findings from the interviews clarified the central redesigning targets and requirements for the development of the environment.

As a result, an implementation plan for the project was produced, which describes the tasks for the project. It was also the intention of this thesis to start the rebuilding process for the local area network. The first part of rebuilding started according to plan but it was not finished on time. The results of the thesis highlight time and employee resources as an important part of project planning.

Keywords: cyber security, local area network, project planning

Sisällys

# 1 Johdanto

Tämän opinnäytetyön tarkoituksena oli tuottaa toteutussuunnitelma yrityksen sisäisen verkko-osion uudistamista varten ja toteuttaa uudistuksen ensimmäinen vaihe käytännössä. KPMG Oy Ab:llä teknisen tietoturvatiimin työtä tukeva laboratorioverkko tarvitsi päivitystä ja tähän tarpeeseen tarvittiin työntekijä, joka ottaisi uudistuksen suunnittelun ja käytäntöönpanon vastuulleen. Laboratorioverkko käsitteenä ei ole yleisesti vakiintunut, vaan kyse on toimeksiantajan työyhteisössä muodostuneesta nimityksestä. Ympäristön pääasiallinen tarkoitus on toimia asiakastoimeksiantojen toteuttamisen apuna sisältäen erilaisia palvelinkoneita ja niillä ylläpidettäviä palveluita.

Konsultti Paul Silfverbergin mukaan hankesuunnittelussa voi pitää tärkeänä neljää vaatimusta: selkeät ja realistiset tavoitteet, aikataulu, selkeä johtamismalli ja organisaatio sekä selkeästi määritellyt panokset eli resurssit (Silfverberg 2006). Vaikka Silfverbergin projektisuunnittelun menetelmät onkin ensisijaisesti suunniteltu laajoihin kansainvälisiin hankkeisiin, käytän tähän työhön soveltuvia ohjeita vertailuaineistona. Aion tämän raportin johtopäätöksissä analysoida sitä, miten hyvin edellä mainitut vaatimukset täytettiin.

Tässä raportissa avataan työn lähtökohtia, prosessia ja analysoidaan, miten ympäristölle asetetut tietoturvavaatimukset vaikuttavat siihen. Aluksi esitellään toimeksiantaja ja miten työ toteutettiin. Projektimallin avaaminen alustaa projektin kulkua. Tämän jälkeen kuvataan projektin lähtökohtia ja päämäärää. Laboratorion fyysisen tilan vaatimusten avaaminen taustoittaa projektin toimintaympäristöä.

Tämän jälkeen kerrotaan projektiin liittyvistä keskeisistä teoreettisista käsitteistä. Mukana on arviointia, kuinka tietoturvan peruskäsitteistöön kuuluva CIA-malli näkyy uudistettavassa ympäristössä. Seuraavaksi käsitellään työssä käytettyä menetelmää. Haastattelu osoittautui arvokkaaksi menetelmäksi, sillä sen avulla saatiin tietoa koskien ympäristön vaatimuksia, varsinaista käyttöä sekä toiveita uudistusta varten. Suunnittelussa otettiin huomioon tietoturvallisuuden peruskäsitteistön sekä toimeksiantajan tietoturvavastaavan tuomia vaatimuksia. Viimeiseksi kuvataan projektiprosessi.

# 2 Case KPMG Oy Ab

KPMG Oy Ab on KPMG Internationalin jäsenyritys, joka on yksi niin sanotuista Big Four -yrityksistä. Nämä yritykset tarjoavat maailmanlaajuisella skaalalla yrityksille tilintarkastuspalveluita, liikkeenjohdon konsultointia, veroneuvonnan palveluita ja erilaisia auditointipalveluita. KPMG:n henkilöstömäärä Suomessa on noin 1100 henkeä ja liikevaihto tilikaudella 2016-2017 126,3 miljoonaa euroa (KPMG 2018). Suurin yksittäinen yrityksen toimistotila on Helsingin pääkonttori.

Teknisen tietoturvan tiimi toimii KPMG Oy Ab:n Cyber-yksikön alaisuudessa. Yksikössä on omat tiiminsä myös hallinnolliselle tietoturvalle, tietosuojalle, kokonaisarkkitehtuurille sekä turvallisuus- sekä tietoturvallisuusauditointeja ja sertifiointeja tarjoava tiimi (KPMG IT Sertifiointi Oy:n alainen). Cyber-yksikön rinnalla toimii myös identiteetin- ja pääsynhallinnan (IAM) tiimi. Tekninen tiimi toimii asiakastoimeksiannoissa runsaasti yhteistyössä hallinnollisen tietoturvatiimin kanssa.

Opinnäytetyö on toteutustavaltaan projektimuotoinen, mutta mukana on myös laadullisen tutkimuksen analyysiä. Projektin runkona toimii työssä toteutettu toteutussuunnitelma, joka määrittelee esimerkiksi toteutuksen rajauksen sekä millainen on projektin rakenne ja aikataulu. Kyseessä on siis toiminnallinen opinnäytetyö, jossa tuloksena on varsinainen työ, produkti sekä raportti. (Airaksinen 2009)

Kari Salonen (2013, 12) määrittelee projektin työksi, ”jota nimetyt projektityöntekijät tekevät organisaatiossa, joka on asettanut projektin määräajan sekä sen tavoitteet, projektiresurssin ja aikataulun”. Projektityöntekijäksi asetettiin minun lisäkseni kaksi muuta työntekijää, joista toinen toimii laboratorioympäristön vastuuhenkilönä. Tavoitteet ja arvioitu aikataulu päätettiin projektin työntekijöiden kesken ja asetettiin teknisestä tiimistä vastuullisen esimiehen toimesta. Projektin rahalliset resurssit oli päätetty jo aiemmin.

Projekti noudatti rakenteeltaan spiraalimallia, vaikka alun perin suunniteltiin melko lineaarista mallia. Lineaarisessa mallissa projektin vaiheet etenevät suoraviivaisesti määrittelystä suunnitteluun, toteutukseen ja päättämiseen. Spiraalimallissa on kyse syklistä, jossa suunnittelua seuraa toiminta, havainnointi ja reflektointi, jonka jälkeen edetään jälleen suunnitteluun. (Salonen, 2013) Projektin toteutusvaiheen vaiheistuksesta seurasi, että suunnitteluun palataan myös myöhemmässä vaiheessa projektia.

# 3 Projektin kuvaus

Teknisen tiimin käytössä oleva laboratorioverkko sijaitsee fyysisesti laboratoriotilassa, jonne on rajoitettu pääsy sillä perusteella, missä asiakastoimeksiannoissa työntekijä työskentelee. Vaikka työ olikin rajattu laboratorioverkon uudistamiseen, on sen tarkoituksen ja aseman ymmärtämisen vuoksi syytä selittää myös fyysisen laboratoriotilan käyttötarkoitus.

## 3.1 Uudistettava laboratorioverkko

Laboratoriotila sijaitsee KPMG:n Helsingin toimistorakennuksessa. Se on rakennettu turvatilaksi, joka noudattaa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) sekä Katakri-auditointityökalun fyysisen tilan vaatimuksia korkean turvallisuustason aineistojen käsittelyä varten. Katakri määrittelee fyysisten turvatoimien tarkoitukseksi ”estää tunkeutuminen salaa tai väkisin, ehkäistä, estää ja havaita luvattomat toimet ja mahdollistaa henkilöstön luokitus ja pääsy salassa pidettäviin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on” (Katakri, 2015). Fyysistä turvallisuutta koskeva osa-alue F Katakri-ohjeistuksessa määrittelee tiloja ja laitteita koskevia vaatimuksia, luvattoman pääsyn estämiseen tähtääviä vaatimuksia, suojaamiseen salakatselulta ja -kuuntelulta tähtääviä vaatimuksia sekä toiminnan jatkuvuuden hallintaan liittyviä vaatimuksia.

Laboratorioverkko koostuu laitteistoltaan palvelinkoneista sekä kytkimistä ja palomuurista. Palvelinkoneilla ylläpidetään palveluita, joista osa toimii pelkästään laboratorioverkossa ja osa ulkoverkossa. Tämä vaatimus aiheuttaa sen, että verkkoa rajataan fyysisesti erillisillä kytkimillä sekä vielä erillisiin virtuaalisiin lähiverkkoihin (VLAN), jotta vain tarvittavat palvelimet altistuvat avoimen internetin liikenteelle. Laboratorion tekniikkaa sekä sen käyttötapoja ei tässä ympäristössä määrittele Katakri-ohjeistuksen teknistä tietoturvallisuutta koskeva osa-alue I, joten sitä ei otettu myöskään uudistuksen suunnittelussa huomioon. Aiemmin mainittu verkon rajaaminen noudattaa Katakrin vaatimuksia verkon rakenteellisesta turvallisuudesta sekä tietoliikenneverkon vyöhykkeistämisestä. Mikäli asiakastoimeksianto niin vaatii, sen sisältämiä tietoja ei käsitellä edes laboratorioverkossa, vaan ainoastaan samassa fyysisessä tilassa. Tähän voi olla syinä mm. datan luottamuksellisuus tai haittaohjelmien käsittely.

Joihinkin laboratorioverkon palveluihin pääsee käsiksi ulkoverkosta virtuaalisen erillisverkkoyhteyden (Virtual Private Network, VPN) kautta. Hallintayhteydet palvelinalustoille on kuitenkin reititetty niin, että niihin ei pääse käsiksi muuten kuin laboratorioverkon sisältä niille osoitetuilta työasemilta. Tämä noudattaa myös Katakri-ohjeistuksen vaatimuksia hallintayhteyksistä.

### 3.2 Projektin tulokset

Projektin tuloksena syntyy toteutussuunnitelma laboratorioverkon vaiheittain tehtävää uudistusta varten sekä ensimmäisen vaiheen toteutus. Toteutussuunnitelmaan kuuluvat seuraavat asiat:

- Toteutuksen kohteen kuvaus
- Projektin rajaus
- Aikataulu
- Vaiheet
- Työmäärä ja kustannusarvio
- Tavoiteltava lopputulos

## 4 Millainen on hyvä laboratorioverkko

Termiä laboratorioverkko ei ole tarkkaan määritelty, joten se voi eri toimijoille tarkoittaa eri asioita. Suomen kielitoimiston sanakirja määrittelee sanan laboratorio merkityksen ”laitokseksi tai osastoksi, jossa tehdään kokeellisia tutkimuksia” (Kotimaisten kielten keskus, 2018). Kuten aiemmin on kerrottu, tämän projektin kohteena olevan laboratorioverkon pääasiallinen merkitys ei kuitenkaan ole tutkimuksellinen. Siellä voidaan tehdä kokeellista työskentelyä kuten jonkun tietoverkkojen testauksessa käytettävän työkalun kehitystä tai testausta, mutta nämä toimet merkitys on sidottu yrityksen asiakastoimeksiantoihin. Välineenä ja tilana tämän projektin laboratorioverkko on siis ensisijaisesti työskentelyä ja sen tukemista varten.

Tietoturvan teoreettisiin perusteisiin kuuluu niin sanottu CIA-malli. Takana ovat termit confidentiality eli luottamuksellisuus, integrity eli eheys ja availability eli saatavuus. Seuraavaksi tarkastelen, miten nämä tekijät näkyvät juuri tämän projektin laboratorioverkossa.

### 4.1 Saatavuus, eheys ja luottamuksellisuus

Saatavuudella tarkoitetaan sitä, että tieto on saatavilla silloin, kun sen saamiseen oikeutetut sitä tarvitsevat (Jarva, 2009). Tähän osa-alueeseen liittyy niin sanottu vähimpien oikeuksien periaate (eng. least privilege). Sen mukaan järjestelmän käyttöoikeudet tulee rajata niin, että sovelluksilla ja käyttäjillä on pienin määrä oikeuksia, mitä ne vaativat toimiakseen niille annetuissa tehtävissä. Tällä pyritään rajoittamaan mahdollisesta virhetilanteesta syntyvää vahinkoa sekä vähentämään eri prosessien välisiä vuorovaikutustilanteita ja niiden aiheuttamia ongelmatilanteita. Tätä periaatetta on noudatettu laboratorioverkossa melko suoraviivaisesti: laboratorioverkkoon pääsee vain laboratoriotilasta tai sille omistetuilta paikoilta toimistosta,

vain laboratorioverkon vastaavalla on täydet ylläpitäjän oikeudet ja työntekijöille on annettu käyttäjätunnuksia eri palvelimille ja palveluille silloin, kun niitä on tarvittu. Eri palveluita on ajettu palvelimilla niille tehdyillä järjestelmätunnuksilla. Saatavuudesta muualla kuin toimistolla on huolehdittu virtuaalisen erillisverkkoyhteyden (VPN) avulla, joka vaatii omat käyttäjätunnuksensa sekä yhteysavaimensa. Laboratorioverkon käyttäjistä muut kuin laboratorioverkon vastaava eivät tarvitse käyttäjätunnuksia kaikille laboratorioverkon palvelimille. Tämän vuoksi laboratorioverkon historian aikana on mietitty keskitetyn käyttäjähallinnan toteuttamista, mutta sitä ei olla katsottu tarpeelliseksi käyttää vaan pikemminkin yhdeksi tarpeettomaksi hallittavaksi osaseksi.

Eheydellä tarkoitetaan tiedon sekä sen käsittelymenetelmien oikeellisuuden varmistamista (Jarva, 2009). Oleellista on tiedon sisällön muuttumattomuus. Esimerkiksi kun siirretään palvelimella ollutta dataa tarkastelua varten toiselle tietokoneelle, halutaan että alkuperäinen tieto on muuttumatonta, vaikka työskentely vaatiikin tiedon käsittelyä. Tiedonsiirron tulee olla salattua myös suljetuissa ympäristöissä, jotta sen muokkaaminen voidaan mahdollisen tunkeutumisen sattuessa estää. Yksi käytetyn tiedon eheyttä edistävä asia laboratorioverkossa on keskitetty versionhallinta. Sitä on käytetty esimerkiksi erilaisten teknisissä auditoinneissa käytettävien komentosarjojen eli skriptien päivitysten hallintaan.

Luottamuksellisuudella tarkoitetaan sen varmistamista, että vain tiedon käsittelyyn oikeutetut voivat sitä käsitellä (Jarva, 2009). Tämän toteutumista käsiteltiin jo aiemmissa kappaleissa: verkon palvelimille pääsyä on rajoitettu käyttäjätunnuksilla ja tietoliikennettä on salattu. Tässä osiossa piilee kuitenkin ainakin yksi riski. Käytännön syistä laboratorioverkkoon pääsy on mahdollistettu myös fyysisen laboratoriotilan ulkopuolelta, sille tarkoitetuilta työskentelypaikoilta. Teoriassa siis yrityksen tiloihin pääsevä tunkeutuja voi päästä laboratorioverkkoon helpommin kuin fyysiseen laboratoriotilaan. Tämä yhteys on kuitenkin reititetty niin, että vain osa palvelimista on saatavilla. Saatavuudesta huolehtimisen avulla voidaan siis tukea luottamuksellisuuden toteutumista.

## 4.2 Tietoturvavastaavan kommentteja

Projektin alkuvaiheessa sain myös KPMG:n NITSO:n (National IT Security Officer) kommentteja siitä, mitä uudistusprojektissa tulisi ottaa huomioon. Kommentit tehtiin teknisen tiimin jäsenille esitettyjen haastattelukysymysten pohjalta. NITSO:n tehtävänkuva on olla KPMG Suomen yhteyshenkilö ja vastaava yrityksen globaaleille IT-palveluille. Monet kommenteista koskivat käytänteitä ja laboratoriosta vastaavan henkilön toimia, mutta käsittelen tässä muita huomioita.

Ensimmäinen huomio oli laboratorioon ja laboratorioverkkoon tarvittavien laitteiden vaatimusmäärittely. Tällä on tarkoitus rajoittaa ylimääräisten ja tarpeettomien laitteiden oloa laboratoriossa. Tässä huomiossa on mukana fyysisen tietoturvan aspekti, mutta koskee myös projektin alkuvaiheessa tiedostettua huomiota siitä, että verkossa on mukana tarpeettomia laitteita. Ratkaisuna on ylläpitää muutoshallintaa ja vaatia uusilta laitteilta hyväksyjän kuittaus. Muutoshallintaa varten verkon ulkopuolella on pidetty GLPI-ohjelmistoa, mutta sen ylläpito oli osoittautunut haastavaksi resurssimuutosten myötä.

Toisena huomiona oli IDS- (Intrusion Detection System) tai IPS-ohjelmiston (Intrusion Prevention System) tuominen osaksi laboratorioverkkoa. IDS-ohjelmiston tarkoitus on seurata ja hälyttää mahdollisista poikkeamista sille määritellyn verkon liikenteessä. IPS-ohjelmiston on taas tarkoitus reagoida uhkiin yrittämällä estää sen toiminta. Yhdeksi tärkeäksi tavoitteeksi tulikin ottaa uudistuksessa käyttöön IDS-ohjelmisto.

Kolmantena huomiona oli keskitetty lokitiedostojen ylläpito niin IDS-ohjelmistosta kuin palomuuristakin. Lokitiedostot kirjaavat ylös ohjelmistojen ja laitteiden toimintoja, jotta mahdolliset vikatilanteet voidaan myöhemmin selvittää. Globaalina vaatimuksena on pitää lokitiedostoja vähintään 180 päivää. Tähän palvelimeen pääsyn pitäisi olla rajattu vain verkon vastaavalle. Heti, kun jotain ongelmaa verkossa tulee, siitä lähtee ilmoitus verkon vastaavalle ja tarpeelliset ohjelmistojen tiedot tallentuvat lokitiedostoihin. Nykyisessä verkossa lokitiedostoja ei kerätty niin laajasti kuin näiden vaatimusten alle kuuluu, joten tästäkin kokonaisuudesta tuli osa uudistusprojektia.

# 5 Käytetyn menetelmän esittely ja perustelu

Projektin alussa haastattelin teknisen tiimin työntekijöitä. Haastattelun tarkoituksena oli kartoittaa sitä, millaisia käyttötarkoituksia työntekijöillä on laboratorioverkolle, mitä sen odotetaan tekevän ja miten sen toivottaisiin muuttuvan. Kyseessä on siis tarvelähtöinen suunnittelu. Paul Silfverberg (2006) määrittelee tarvelähtöisen suunnittelun lähtökohdaksi, jossa otetaan huomioon sidosryhmien itsensä kokemat mahdollisuudet tai ongelmat.

Haastattelumuodoksi valitsin strukturoidun haastattelun, sillä se helpottaa tiedon käsittelyä ja haastattelun kohteet edustivat yhtenäistä ryhmää (HAMK Opinnäytetyöpankki). Käyttämällä samaa haastattelurunkoa useiden ihmisten kanssa saadaan vertailukelpoisia tuloksia, jotka helpottavat ratkaisujen tekemistä suunnittelutyössä. Haastattelut toteutettiin yksilöhaastatteluina toimiston työtiloissa.

Haastattelu koostui seuraavista kysymyksistä:

1. Mitä tekninen tiimi tarvitsee laboratorioverkolta?
2. Mitä työkaluja ja toiminnallisuuksia käytät nyt eniten laboratorioverkossa?
3. Mitä työkaluja ja toiminnallisuuksia haluaisit laboratorioverkkoon?
4. Mitä tarvittaisiin muuhun internetiin avoimena olevaan osuuteen?
5. Mitä voitaisiin tehdä laboratorioverkon ylläpidon parantamiseksi (teknisessä ja hallinnollisessa mielessä)?

Haastatteluiden jälkeen tein haastatteluista yhteenvedon ja esitin sen tiimille. Tämän tarkoituksena oli kuulla kommentteja sekä mahdollisia lisäyksiä, joita yksilöhaastatteluissa ei selvinnyt. Näin haastattelusta saatuja tuloksia voitiin reflektoida jo suunnittelun alkuvaiheessa, jotka esittelen seuraavassa luvussa.

# 6 Suunnittelu ja toteutus

## 6.1 Ensimmäiset vaiheet

Projekti alkoi aikataulun suunnittelulla helmikuussa. Suunnittelimme yhdessä työelämäohjaajani kanssa alustavan aikataulusuunnitelman, josta selvisi yksityiskohtaisesti projektin suunnitteluvaiheet sekä sen jälkeiset toimet. Samalla sanallistettiin myös projektin tavoitteet: toteutussuunnitelma laboratorioverkon uudistamiseksi, uudistettu palvelualusta sekä toteutuksen mallinnus ja testaus. Jo lyhyt tavoitteiden asettaminen rajasi projektista ulkopuolelle esimerkiksi monilta osin käytänteiden uudistamisen, vaikka itse käytännöistä esimerkiksi dokumentointi katsottiin kuuluvaksi tärkeäksi osaksi projektia. Ympäristölle asetetut Katakri-vaatimukset rajoittavat käytänteitä, joten kyseessä eivät olleet vain työskentelyä helpottavat rajat, vaan käytännön syyt.

Ensimmäisen vaiheen haastatteluista selvisi, että työntekijöiden toiveissa ympäristön uudistamiseksi oli paljon yhtäläisyyksiä. Samalla kyselyssä myös kartoitettiin nykyisten palveluiden käyttöä, jonka avulla löytyi myös selkeät käytetyimmässä asemassa olevat palvelut. Kysymykset toivat esille myös juuri ulos rajattuja hallinnollisiin käytänteisiin liittyviä asioita, joka ei kuulunut työn fokukseen, mutta joiden esille tuominen oli tärkeää teknisen tiimin työskentelyn kannalta. Pääasiassa vastaukset olivat käytännönläheisiä ja toivat konkreettisia ehdotuksia uudistusta varten.

## 6.2 Haastatteluiden tuloksia

Ensimmäinen kysymys ”Mitä tekninen tiimi tarvitsee laboratorioverkolta?” oli yleisluontoinen kysymys siitä, mikä on haastateltavien näkemys uudistettavan ympäristön merkityksestä teknisen tiimin kannalta. Vastaukset yleensä pohjustivat muita jatkokysymyksiä ja toivat esille sen, että ympäristön välineellinen arvo kytkeytyy juurikin asiakastoimeksiantoihin ja niiden toteuttamiseen. Seuraavat kysymykset ”Mitä työkaluja ja toiminnallisuuksia käytät nyt eniten laboratorioverkossa?” sekä ”Mitä työkaluja ja toiminnallisuuksia haluaisit laboratorioverkkoon?” toivat molemmat esille selkeitä kohteita mitkä uudistuksessa pitää säilyttää sekä sellaisia sovelluksia, jotka voisiva ympäristöä täydentää. Nykytilannetta koskeva kysymys auttoi vahvistamaan ennakko-olettaman, että erityisesti tietyt ulkoverkosta käsin käytettävät verkkosivujen auditointipalvelut olivat käytetyimpiä asiakastoimeksiannoissa ja niiden saatavuus nähtiin erityisen tärkeänä. Halutuissa uudistuksissa useimmin mainittuna nähtiin virtualisointialusta, johon kuka tahansa tiimin jäsenistä pystyisi tekemään oman helposti hallinnoitavan virtuaaliympäristön erilaisten ympäristöjen ja sovellusten testaamista varten. Lisäksi haluttiin joidenkin nykyisten toiminnallisuuksien kehittämistä sekä täydentämistä.

Johtuen ympäristön vaatimuksista ja luonteesta halusin nostaa vielä esiin ulkoverkkoon kuuluvien palveluiden merkitystä kysymyksellä ”Mitä tarvittaisiin muuhun internetiin avoimena olevaan osuuteen?”. Tähän haluttiin osittain samoja toimintoja kuin sisäiseen verkkoon, kuten itse ylläpidettävät virtuaalikoneet testausta varten, mutta pääasiassa nykyisin käytössä olevien palveluiden täydennyksiä, kuten palvelin jossa helposti saatavilla huomattava määrä erilaisia auditointitestausta helpottavia työkaluja. Viimeinen kysymys ”Mitä voitaisiin tehdä laboratorion ylläpidon parantamiseksi (teknisessä ja hallinnollisessa mielessä)?” toi esille hyvin vähän mahdollisia teknisiä ratkaisuja ylläpidon parantamiseksi, enimmäkseen ideoitiin mahdollisuutta erilaisesta tavasta hoitaa servereiden lokitiedostojen ylläpitoa. Sen sijaan korostettiin, että henkilöresursseja laboratorion ylläpitoon haluttiin lisätä.

Esitin koosteen haastatteluista saaduista tuloksista teknisen tiimin viikkopalaverissa. Haastattelujen purkaminen sen osallistujien kesken oli tärkeää, koska tässä yhteydessä sain joitain täsmentäviä kommentteja sekä näkemyksiä siitä, miten kyselyiden tuloksia voitaisiin soveltaa. Koosteessa ei tuotu esille yksittäisten henkilöiden haastattelujen vastauksia.

## 6.3 Suunnittelu

Kun haastattelut oli saatu tehtyä, oli mahdollista alkaa suunnittelemaan erilaisia uudistusprojektin valintoja. Kävin läpi laboratorioympäristöä tuntevan kollegan kanssa laboratorion nykytilanteen yksityiskohtaisemmin. Tässä yhteydessä selvitimme koko ympäristön laitteiston sekä verkon rakenteen pääpiirteittäin. Nykytilanteen kartoitus yhdessä aiempien haastatteluiden

kanssa auttoi ymmärtämään, mitkä ovat senhetkisen ympäristön ongelmakohdat. Suunnittelussa osallisena olivat koko tekninen tiimi.

Toinen osa suunnittelua oli laitteiston sekä ohjelmistojen ja palveluiden läpikäynti. Tärkeä kysymys oli, mitä laitteistoa voidaan hankkia vanhan tilalle. Tässä auttoi jo ennen projektia tehty kustannusarvio uudesta laitteistosta, joka toimi hyvänä pohjana resurssien arvioinnille. Kustannusarviota piti muuttaa toteutuksen ensimmäisen vaiheen laitteistovalintojen jälkeen, jonka seurauksena budjetti kasvoi hieman, mutta kasvun arvioitiin olevan tarpeeksi maltillinen. Esittelen seuraavaksi tärkeimmät uudistettavat laitteiston osat.

Koska ympäristö, jossa palvelimia ylläpidetään, on myös työskentelytila, nousi hiljaisuus yhdeksi tärkeäksi kriteeriksi hankittavan laitteiston valinnassa. Yksi suurimmista äänen tuottajista ovat vanhat kytkimet, joten uusien haluttiin olevan passiivijäähdytteisiä. Kuitenkin toisena vaatimuksena oli tarpeeksi monta Ethernet-lähiverkkoympäristöissä käytettävää RJ45-porttia ympäristön kasvuvaraa sekä väliaikaisia ratkaisuja varten. Nämä kaksi vaatimusta yhdessä rajoittivat mahdollisia vaihtoehtoja. Korvaavaksi löytynyt malli ei tarjonnut yhtä laajoja OSI-mallin tason kolme mallintamia toimintoja, mutta nähtiin kuitenkin riittäväksi toteutettavalle ympäristölle.

Toinen tärkeä hankinnan kohde oli uudet virtualisointipalvelimet. Virtualisoinnilla jaetaan laitteistoresursseja erillisiksi loogisiksi resursseiksi, eli esimerkiksi toisistaan erillisiä palvelinympäristöjä voidaan ajaa samalla fyysisellä laitteella (Aalto, 2017). Tämä on tehokasta sekä energian että palvelinkomponenttien käytön kannalta. Laboratorioverkon palveluiden resurssivaatimukset skaalautuvat hyvin virtualisointiympäristössä. Uusia fyysisiä palvelimia tarvittiin, koska edelliset olivat elinkaarensa päätepisteessä jo useita vuosia. Palvelimien hankinnan osalta vertailtiin erilaisia vaihtoehtoja ja lopulta päädyttiin hieman paranneltuun versioon alkuperäisessä kustannusarviossa ehdotetusta mallista, joka tuotiin esille toimittajan tarjouksessa.

Kolmas tärkeä komponentti uudessa ympäristössä oli uusi palomuuri. Fyysinen palomuuri on tärkeä, koska osan verkosta täytyy kohdata suora julkinen internetliikenne samalla, kun osa verkosta on reititetty sisäverkkoon. Syyt tämän verkon palasen uudistamiselle olivat samat kuin kytkimien ja palvelimien kohdalla: äänekkyys ja elinkaaren loppupäässä oleminen. Lisäksi vaatimuksena oli ominaisuuksiltaan kaupalliseen yrityskäyttöön suunnattu laite, tarkoittaen esimerkiksi hallinnoinnin, konfiguroinnin ja valmistajan tarjoaman tuen osalta.

Ohjelmistojen saralla tärkein valinta liittyi käyttöön otettavaan virtualisointialustaan. Markkinoilla ei ole kovin montaa vaihtoehtoa, suurimpien ollessa VMwaren ESXi, Microsoftin HyperV

ja Citrixin XenServer. Nykyisin käytössä oleva XenServer on joitain hallinnointiin liittyviä ongelmia lukuun ottamatta nähty tässä ympäristössä hyväksi.

Palvelut pyörivät ympäristössä omilla virtualisoiduilla palvelimillaan. Niiden uudistamisen osalta nähtiin tarpeelliseksi, että samalla kun uudistetaan virtualisointialusta, asennetaan myös uudet virtualisoidut palvelimet. Vaihtoehtona oli myös virtuaalikoneiden siirto uudelle alustalle, mikä nähtiin tarpeettomana, koska useimmat palvelut yksittäisinä voidaan rakentaa uudelleen huolehtien tarpeellisten tietojen ja konfiguraatioiden tallennuksesta.

## 6.4 Toteutussuunnitelma

Työssäni toteutussuunnitelma oli dokumentti, jossa kuvataan, miten ympäristön uudistus toteutetaan ja mikä on tavoiteltu lopputulos. Toteutussuunnitelman kokoaminen alkoi kyselyn koosteen pohjalta. Toteutussuunnitelmalla varmistetaan, että toteutus tehdään hallitusti ja että tavoite on asetettu. Johtopäätöksissä selostan, miten toteutussuunnitelman noudattamisessa onnistuttiin.


Kuva 1: Projektin tulosketju

Suunnitelman alussa tuodaan esille projektin lähtökohdat ja tavoitteet. Tavoitteiden toteutumista havainnoidaan tulosketjulla, joka on nähtävissä kuvassa 1. Tulosketju kuvaa projektin tavoitteiden syy-seuraussuhdetta, jossa tavoitteet seuraavat toisiaan. Panos johtaa toimintoihin, toiminnot tuotoksiin ja tuotokset lopputulokseen, joka vielä avaa esille kehitystavoitteen (Tavoitteiden ja toimenpiteiden määrittely, Kepa). Tulosketju auttaa hahmottamaan, minkä vuoksi toiminnot tehdään ja mitä tulee tavoitteiden saavuttamisen jälkeen.

Toteutussuunnitelma kuvaa projektin sisällön kuvaamalla ensin vaiheet, jotka on käyty läpi suunnitteluvaiheessa. Tämän jälkeen kuvataan toteutusvaiheet. Ensimmäisessä vaiheessa otetaan käyttöön uusi palvelinympäristö ja kytkimet. Tässä kohtaa kerrotaan myös, mitkä ohjelmistot muodostavat virtualisoidun palvelinympäristön selkärangan sekä sen, mitkä ovat nykyiset virtuaalikoneet ja mitä niille tehdään: joko poistetaan tarpeettomana, asennetaan uusiksi ja muut toimenpiteet. Toisessa vaiheessa palomuuri ja kolmannessa vaiheessa tehdään viimeiset hankinnat sekä niiden asennus. Kaikki vaiheet osaltaan vaikuttavat verkon rakenteen uudistamiseen, mutta suurin työ tehdään ensimmäisessä vaiheessa.

### 6.5 Toteutuksen käynnistäminen ja jatko

Ensimmäisen vaiheen hankinnat olivat Dellin PowerEdge -palvelimet Intel Xeon -sarjan prosessoreilla sekä HP OfficeConnect -sarjan kytkimet. Vaiheen aloitus myöhästyi, sillä vastausta tarjouspyyntöön jouduttiin odottamaan oletettua pidempään, jonka myötä myös hankinnan hyväksyntä myöhästyi. Tämän jälkeen suunniteltiin sitä, missä järjestyksessä uudet hankitut laitteet tulisi ottaa käyttöön.

Tärkein huomioitava asia on ajankohta, sillä ympäristöä uudistettaessa palvelut ovat hetkellisesti alhaalla. Varsinaisesta siirrosta on tiedotettava hyvissä ajoin etukäteen, sillä jotkut palvelut voivat olla käytössä myös arkisten toimistotyöaikojen ulkopuolella. Uusille palvelimille sijoitetaan suurin osa palveluista. Tähän joukkoon kuuluvat esimerkiksi virtuaalinen erillisverkkopalvelin (VPN), versionhallinta ja asiakastoimeksiantojen auditointeihin käytetty ohjelmisto. IDS-ohjelmiston sisältämä palvelin sekä hallintaan käytettävä palvelin asennetaan kuitenkin erillisille fyysisille laitteistoille, koska mahdollisen vikatilanteen sattuessa (esimerkiksi haittaohjelma) ne on näin eriytetty vahvemmin muista. Kytkinten konfiguraatiossa otetaan huomioon vanhojen kytkimien konfiguraatiot, joka on helppoa niiden ollessa saman valmistajan tuotteita kuin uudet. Virtuaalisiin lähiverkkoihin jakaminen tehdään uusi laitekanta huomioiden.

Toteutuksen seuraavat vaiheet aiotaan toteuttaa kahden ja viiden kuukauden kuluttua ensimmäisen vaiheen jälkeen. Uuden palomuurin valinta ei ennen ensimmäisen vaiheen aloittamista ollut valmis. Sille asetetut vaatimukset eivät tule oleellisesti muuttumaan. Viimeisessä vaiheessa tullaan hankkimaan uutta laitteistoa runsaasti laskentatehoa vaativia toimia, kuten salasanojen murtamista varten. Tämän jälkeen uudistettu ympäristö on valmis jatkokehitystä varten.

# 7 Yhteenveto ja johtopäätökset

Tätä lukua kirjoittaessani projektin ensimmäistä toteutusvaihetta ei oltu vielä saatu päätökseen. Toteutussuunnitelmaa oli muokattu toteutusvaiheen aikana tarkentamaan ja lisäämään tavoitteita. Kaikkia projektin tavoitteita ei siis ole vielä saavutettu. Seuraavaksi vertailen johdannossa kerrottuja Paul Silfverbergin hyvän hankesuunnitelman vaatimuksia (2006) siihen, mitä tämän opinnäytetyön projektissa tapahtui ja miten toteutussuunnitelmaa noudatettiin.

Hankkeen aikataulusta tuli selkein kompastuskivi. Alun perin arvioidut ajankohdat siirtyivät useaan otteeseen. Yksi syy oli jo alkuvaiheessa riskiksi arvioidut henkilöresurssisyyt. Työhön tietoturvan konsultoinnin alalla kuuluvat yllättävät ja muuttuvat tilanteet, joten joskus voi olla vaikea arvioida, mikä on henkilöiden työtilanne kuukausien tai jopa parin viikon päästä. Mahdollisissa konfliktitilanteissa asiakastoimeksiannot vievät varman voiton verrattuna niin sanottuihin sisäisiin töihin. Tässä tapauksessa allekirjoittaneen sekä myös muiden projektissa mukana olleiden kevät oli paikoittain niin kiireinen, ettei projektiin päässyt keskittymään. Virheenä oli arvioida projektin aikataulua vain viikkotasolla. Ratkaisu tähän olisi ollut yksinkertainen: kokonaisten päivien varaaminen jo projektin alussa.

Edellinen kappale koskettaa myös toista Silfverbergin käsittelemää vaatimusta eli selkeästi määriteltyjä resursseja. Henkilötyön resurssit eivät siis olleet riittävän hyvin allokoituja tähän projektiin. Sen sijaan materiaaliset resurssit olivat hyvin arvioitu. Projektin saavutuksena voidaan pitää vanhan materiaalin eli vanhan laboratorioverkon laitteiston arviointia ja luokittelua. Rahallisten resurssien määrittelyssä auttoi runsaasti jo aiemmin tehty budjettiarvio, mutta sen uudelleen arviointi oli tärkeä osa projektia.

Projektin johtamismalli ja organisaatio olivat hyvin yksinkertaiset ja erityisesti tässä vaatimuksessa näkyy, kuinka Silfverbergin malli on suunnattu isommille, usean eri toimijan projekteille. Organisaatio eli muutama projektiin aktiivisesti osallistunutta henkilöä toimivat yhteistyössä ja vastuut olivat jakautuneet oikein, mutta kuten aiemmissa kappaleissa todettiin, yhteistyö olisi voinut olla täsmällisempää. Johtamismalli ei toteutunut selkeänä, johon olisin voinut vaikuttaa pysymällä aikataulussa.

Hankkeen tavoitteet olivat toteutussuunnitelma laboratorioverkon uudistamiseksi, uudistettu palvelualusta sekä toteutuksen mallinnus ja testaus. Toteutussuunnitelma toteutui, mutta sitä olisi voinut laajentaa vielä tarkemmilla aikatauluilla sekä tarkemmilla prosessikuvauksilla. Eri vaiheet ja rajaus olivat kuitenkin selkeitä. Täysin uudistettu palvelualusta on määritelty saavutettavaksi vasta kolmannen toteutuksen vaiheen kohdalla. Mallinnusta ja testausta ei vielä tätä kirjoittaessani oltu ehditty tekemään.

Vaikka projektin tuloksia ei vielä saavutettu, työn aikana saatiin selville ympäristö, millaisen toteuttaminen tukee toimeksiantajan liiketoimintaa sekä miten tietoturvallisuutta voidaan parantaa verrattuna nykytilanteeseen. Haastattelu ja sen tulokset antoivat pohjan verkon uudistukselle määrittelemällä tarvittavat uudistuksen kohteet. Jatkotoimenpiteisiin kuuluvat suunniteltujen toteutusvaiheiden toteutus, uuden ympäristön dokumentointi sekä jatkokehityskohteiden arviointi ja suunnittelu. Kuten projektityön spiraalimalliin kuuluu, eri vaiheiden jälkeen palataan aina uudelleenarvioimaan ja suunnittelemaan toimintaa, jonka ansiosta mahdollisista tuloksista voidaan saada entistä parempia. Laboratorioverkko vaatii toiminnaltaan luotettavuutta, mutta kuten toivottiin, se tulee myös kehittymään entistä joustavammaksi palvelualustaksi.

Lähteet

Aalto, Janne. 2017. Citrix XenDesktop 7.12 VDI -ympäristön käyttöönotto.
http://www.theseus.fi/bitstream/handle/10024/123563/Aalto_Janne.pdf

Haastattelu. Opinnäytetyöpakki, HAMK. Viitattu 5.5.2018.
https://www.kamk.fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Aineiston-keruumenetelmat/Haastattelu

Jarva, Olli. Pikaviestinnän tietoturva. Ongelmat, vaihtoehdot ja ratkaisut. Viitattu 26.5.2018.
https://olli.jarva.fi/kandidaatintyo_pikaviestinnan_tietoturva.pdf

Katakri – Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 14.4.2018.
https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Kielitoimiston sanakirja. Viitattu 24.5.2018.
https://www.kielitoimistonsanakirja.fi/laboratorio

Salonen, Kari. 2013. Näkökulmia tutkimukselliseen ja toiminnalliseen opinnäytetyöhön. Viitattu 19.5.2018.
http://julkaisut.turkuamk.fi/isbn9789522163738.pdf

Silfverberg, Paul. 2006. Ideasta projektiksi - Projektinvetäjän käsikirja. Viitattu 6.5.2018.
http://www.helsinki.fi/urapalvelut/materiaalit/liitetiedostot/ideasta_projektiksi.pdf

Tavoitteiden ja toimenpiteiden määrittely. Kepa itseopiskeluympäristö. Viitattu 10.5.2018.
https://itseopiskelu.kepa.fi/node/120

Tietoa KPMGstä. Viitattu 7.4.2018. https://home.kpmg.com/fi/fi/home/tietoa-kpmgsta/kpmg-yrityksena.html

Toiminnallinen opinnäytetyö tekstinä. Tiina Airaksinen. Viitattu 10.5.2018.
https://www.slideshare.net/TiinaMarjatta/toiminnallinen-opinnytety-tekstin

Kuviot