Sami Kettunen

HERÄTEHALLINTA-, VALVONTA- JA TIETOTURVALLISUUSRATKAISUT IT-PALVELUTUOTANNOSSA

Organisaation kyberturvallisuusratkaisut

HERÄTEHALLINTA-, VALVONTA- JA TIETOTURVALLISUUSRATKAISUT IT-PALVELUTUOTANNOSSA

Organisaation kyberturvallisuusratkaisut

Sami Kettunen

Opinnäytetyö (Yamk)

Syksy 2016

Teknologialiiketoiminta

Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu

Teknologialiiketoiminta

Tekijä: Sami Kettunen

Opinnäytetyön nimi: Herätehallinta-, valvonta- ja tietoturvallisuusratkaisut IT-palvelutuotannossa

Työn ohjaaja: Juha Alakärppä

Työn valmistumislukukausi ja -vuosi: Syksy 2016 Sivumäärä: 83

Opinnäytetyö ja siihen liittyvä kehittämistehtävä tehtiin Oulun kaupungin liikelaitokselle, joka muun muassa vastaa kaupungin IT-infrastruktuurin toiminnasta ja sen palveluista. Työn tavoitteena oli kehittää organisaation kykyä toimittaa entistä parempaa ja häiriöttömämpää palvelua, vastata nykyajan kohonneisiin tietoturvavaatimuksiin sekä lyhentää tieto- ja viestintäteknologian palveluiden häiriötilanteiden kestoa, tai ennakoivasti estää niiden tapahtumista ollenkaan.

Yhä suurempi osa tiedosta tallennetaan erilaisiin tietojärjestelmiin ja on elintärkeää sekä turvata tiedon luottamuksellisuus, että myös sen saatavuus ja eheys kaikissa tilanteissa. Oulun Tietotekniikan tuottamat tieto- ja viestintätekniikan palvelut ovat verrattain lyhyessä ajassa muuttuneet Oulun kaupungin ydintoimintojen kannalta yhä kriittisemmiksi tukipalveluiksi, joiden toimintahäiriöillä on toiminnallisesti ja taloudellisesti merkittävät vaikutukset.

Opinnäytetyön lähtökohtana oli kehittää häiriöhallintaa ja tietoturvaa hankkimalla ulkopuoliselta toimijalta kokonaisratkaisu, jonka avulla mainittuihin kehityskohtiin voidaan vastata. Hankinta toteutetaan julkisen tarjouskilpailun avulla. Hankintaa varten tilaajalla täytyy olla riittävästi tietoa hankittavasta tuotteesta ja itse hankintaprosesista, joten tämän opinnäytetyön tuloksena esitellään tietoperusta ja tarpeelliset prosessit hankinnan toteuttamiseksi. Itse kilpailutus tapahtuu projektimuotoisena, josta tämä opinnäytetyö kuvaa tarvittavia toimia projektin alkuvaiheessa.

Asiasanat: tietotekniikka, IT-ala, palvelutuotanto, herätehallinta, häiriöhallinta, tietoturva, kyberturvallisuus, julkinen hankinta

ABSTARCT

Oulu University of Applied Sciences

Technology Business

Author: Sami Kettunen

Title of thesis: Event management, monitoring and security solutions on IT-production of services

Supervisor: Juha Alakärppä

Term and year when the thesis was submitted: Autumn 2016 Number of pages: 83

This thesis and its development project was made for Oulun Tietotekniikka liikelaitos, which is an internal business unit inside the City of Oulu. Oulun Tietotekniikka is responsible for the city IT-infrastructure and IT- services. The purpose of this project was to develop organization ability to provide better services with less technical problems and to prepare for the increase of the information security demands in the future.

Everyday more and more information is stored under different information systems and it's even more important to be able to secure the confidentiality and integrity of the stored information but also ensure availability to it in all times. The services provided by Oulun Tietotekniikka have in a relatively short period turned out to be even more critical service to the City of Oulu. Improvement of these services is important because every malfunction of the IT-infrastructure and systems provided by it cost money and reduces efficient work time of the city employees.

The base of this thesis was to develop process of the event management and information security by purchasing a solution for cybersecurity. The solution will be purchased from a third-party operator who can provide solutions in the field mentioned before. Obtaining desired results, the buyer should have enough information about the product purchased as well as the process of purchase itself. The result of this thesis is to introduce the knowledge and proper process for the acquisition. The purchase itself takes place as a project and this thesis describes the acts needed in the beginning of the purchase project.

keywords: information technology, IT-business, service operation, event management, error management, information security, cyber security, public procurement

SISÄLLYS

LYHENTEET

ICT	Information and communications technology, tieto- ja viestintäteknologia
KYBERTURVALLISUUS	Turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen
IT-INFRASTRUKTUURI	Perusrakenne, joka muodostuu järjestelmistä ja palveluista, jotka mahdollistavat tietojärjestelmien toiminnan
TIETOJÄRJESTELMÄ	Ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuva järjestelmä
SAATAVUUS	Ominaisuus, joka ilmentää kuinka varmasti jokin järjestelmä, laite, ohjelma tai palvelu on tarvittaessa käytettävissä
ITIL	Information Technology Infrastructure Library, kokoelma käytäntöjä IT- palveluiden hallintaan ja johtamiseen
SLA	Palvelusopimus, jolla määritellään palvelulle tietyt vaatimustasot
SIEM	Tuottaa operatiivisen tietoturvan tilannekuvaa, tehostaa lokienhallintaa ja yhdistää sekä raportoi tietoturvatapahtumien seurannasta yhtenäisesti
FALSE POSITIVE	Havainto, joka tulkitaan hälytykseksi, vaikka ei sitä ole
JIT2015	Julkisen hallinnon IT-hankintojen yleiset sopimusehdot
JYSE	Julkisten hankintojen yleiset sopimusehdot
24/7	24 tuntia vuorokaudessa, 7 päivää viikossa; aina käytettävissä
DDoS	Distributed Denial of Service, palvelunestohyökkäys, jonka avulla hyökkääjä pyrkii estämään oikeiden käyttäjien pääsyn palveluun. Tällöin hyökkääjä tukkii verkon turhalla datalla
CRYPTOLOCKER	Kiristyshaittaohjelma, joka salaa tiedostot ja pyytää lunnaita niiden avaamiseksi

IoT	Internet of Things, esineiden internet, yleiskuvaus kodin laitteista, jotka eivät ole tietokoneita, mutta joilla on internet-yhteys
SOC	Security Operations Center, tietoturvahallintakeskus
NOC	Network Operations Center, verkkohallintakeskus
IDS	Intrusion Detection System devices, järjestelmä, joka havaitsee haitallisen toiminnan verkossa
IPS	Intrusion Prevention System devices, järjestelmä, joka estää haitallisen toiminnan verkossa

1 JOHDANTO

Oulun Tietotekniikka (jatkossa OTT) on Oulun kaupungin liikelaitos, jonka tarkoituksena on tuottaa laadukkaita tietoteknisiä palveluita asiakkailleen ja luoda näin mahdollisuus asiakkaiden oman toiminnan kehittämiseen ja tehostamiseen. Asiakkaina ovat useat Oulun kaupungin organisaatiot sekä niiden henkilöstö. Toiminnan lähtökohta on asiakaslähtöisyys ja OTT toimii kaupungin ja sen muiden organisaatioiden tietojärjestelmien keskitettynä palvelutuottajana, palveluintegraattorina sekä kumppanina. OTT:n vastuualueella on muun muassa kaupungin kriittisen tietojärjestelmäinfrastruktuurin ylläpito ja kehittäminen. Infrastruktuuri kattaa tietoliikenneverkot ja -järjestelmät, kahdennetut ja katastrofisuojatut datakeskukset. Organisaatio vastaa myös yli 250 sovelluksen kokonaisuudesta ja sen integroinnista kokonaisinfraan. Vastuualueelle kuuluu myös päätelaitteiden kuten työasemien, puhelinten ja nykyaikaisten, liikkuvan työn mahdollistavien laitteiden ja järjestelmien hankinta, tuki ja palvelut. OTT vastaa myös ICT-omaisuuden ja -kustannusten hallinnasta, sekä kokonaisvaltaisesta asiakas- ja loppukäyttäjätuesta. (Oulun Tietotekniikka liikelaitos toimintakertomus 2015, 5.)

Teknologian nopean kehittymisen myötä ovat yhteiskunnan eri osa-alueet enemmän riippuvaisia tietojärjestelmien ja tietotekniikkainfrastruktuurin toimivuudesta ja saatavuudesta. IT-palvelutuottajilla on tarve varmistaa sekä palveluiden häiriötön saatavuus, että tiedon eheys ja luottamuksellisuus sekä turvallisuus. Häiriötilanteet IT-palveluissa aiheuttavat taloudellisia menetyksiä hukkaan menneenä työaikana, ja usein toistuvien häiriötilanteiden seurauksena voi olla asiakkaiden epäluottamus ja tyytymättömyys organisaation kykyyn tuottaa jatkuvasti saatavilla olevaa palvelua. Nykypäivänä melkein kaikki tieto tallennetaan tietojärjestelmiin, joten tietoverkkoon päässyt ulkopuolinen taho voi tietovarkauden kautta saada haltuunsa esimerkiksi organisaatiolle ja sen asiakkaille kuuluvaa kriititstä tietopääomaa. Samalla tietomurtautuja voi aiheuttaa luottamuspulan organisaation hallussa olevan tiedon eheyteen ja luottamuksellisuuteen, mikäli tiedon muuttumattomuutta ei voida teknisesti varmistaa.

Toimeksiantajana toimi OTT ja opinnäytetyön tekijä on OTT:n työntekijä, jonka päivittäinen työnkuva liittyy oleellisesti häiriötilanteiden hallintaan ja ennakoivan häiriöhallinnan kehittämiseen. Tällä hetkellä käytössä ei kuitenkaan ole riittäviä teknisiä välineitä johdonmukaiseen ja kattavaan teknisen terveydentilan yhdenmukaiseen valvontaan, eikä organisaatiolla ole myöskään sovittua toimintamallia tiedon eheyden ja luottamuksellisuuden varmistamiseksi. Opinnäytetyön kehittämistehtävänä oli löytää ratkaisu näiden puutteiden korjaamiseksi. Ratkaisu on osa OTT:n

pitkän aikavälin tavoitetta kehittää OTT:n varautumista tietoturvauhkiin ja kykyä vastata tämän päivän haasteisiin häiriövapaan ja tietoturvallisen toimintaympäristön luomisessa organisaation asiakkaille ja loppukäyttäjille.

Ratkaisun toteuttamiseksi haetaan kumppania, jolla on tarvittavat teknologiat, prosessit ja kyvykkyys toteuttaa kyberturvallisuuden ratkaisut, joiden avulla voidaan seurata IT-infrastruktuurin teknistä tilaa ja saatavuutta sekä mahdollistaa tallennetun tiedon eheys ja luottamuksellisuuden säilyminen. Koska Oulun Tietotekniikka on julkisen sektorin toimija, ratkaisun hankkiminen edellyttää julkista hankintamenettelyä. Tämä vaatii hankinnasta vastaavalta paitsi riittävää tietoutta hankittavasta kohteesta, myös osaamista suorittaa tarkoin säädelty julkinen kilpailutus.

2 KEHITTÄMISTEHTÄVÄ

2.1 Tutkimuksellinen kehittämistyö

Perinteisessä tieteellisessä tutkimuksessa noudatetaan mielellään traditioita, jolloin olennaisia asioita ovat tutkimusongelma, tutkimuskysymykset ja niihin vastaaminen yleisesti hyväksyttyjen menetelmien avulla. Ennen konkreettisten menetelmien valintaa pohditaan usein tieteenfilosofisia kysymyksiä kuten todellisuuden luonnetta (ontologiset kysymykset), tietämisen luonnetta (epistemologiset kysymykset) ja erilaisia välineitä tiedon saavuttamiseen (metodologiset kysymykset). Tieteellisessä tutkimuksessa osoitetaan teoreettisen viitekehyksen avulla, mihin tieteelliseen keskusteluun tutkimuksella osallistutaan ja mihin tutkimus luo uutta tietoa. Usein tulokset myös julkaistaan tieteelliselle yhteisölle suunnatuissa tutkimusjulkaisuissa. Tieteellinen tutkimus voidaan jakaa perustutkimukseen ja soveltavaan tutkimukseen, jolloin perustutkimuksessa pyritään löytämään uutta tietoa ja luomaan sitä tieteen itsensä vuoksi. Perustutkimuksella ei välttämättä ole kytköksiä käytännön sovellutuksiin. Soveltavalla tutkimuksella puolestaan voidaan tavoitella käytännössä sovellettavaa tietoa, esimerkiksi kaupallisia arvoja tavoittelevaa tutkimusta, jonka päämääränä on luoda uusia tai parempia tuotteita, tuotantovälineitä tai palveluita. (Ojasalo, Moilanen & Ritalahti 2014, 18–19.)

Tutkimuksellisella kehitystyöllä on usein erilaiset lähtökohdat, kuten tarve kehittää organisaatiota tai saada aikaan muutoksia toiminnassa. Tutkimuksellinen kehitystyö painottuu yleensä käytännön ongelmien ratkaisuun sekä uusien ideoiden, tuotteiden tai palveluiden toteuttamiseen ja tuottamiseen. Tyypillisesti tarkoituksena on luonnostella, kehitellä ja ottaa käyttöön uusia ratkaisuja. Erona perinteiseen tieteellisen tutkimukseen on, että asioita ei vain kuvailla ja selitetä, vaan niitä viedään myös käytännössä eteenpäin. Voidaan kysyä, halutaanko vain tuottaa ilmiöistä uutta teoriaa, vai saada aikaan myös käytännön parannuksia ja ratkaisuja. Vaikka tutkimuksellisen kehitystyön pääpaino on usein varsinaisen tehtävän saavuttamisessa, tavoitteena voi olla myös uuden tiedon tuottaminen käytännössä. Kun korostetaan tehdyn työn dokumentointia ja julkisuutta, on mahdollista luoda uudenlaista ammatillista tietoa. Tämä puolestaan voi toimia hyvin pohjana esimerkiksi tuleville kehittämishankkeille. (Ojasalo ym. 2014, 19–20.)

Aiheen osaamisen lisäksi tutkimuksellisessa kehittämistyössä on tarpeen osata myös projektityöskentelyä ja kehittämistyötä. Kehittämistyössä korostuvat usein suunnittelu ja suunnitelman mukainen etenemisen hallinta, jotka ovat olennainen osa myös projektityöskentelyä.

Kehittämistyöstä raportoidaan myös usein projektiraportin tapaisella kuvauksella, josta tulee käydä ilmi lähtökohdat, tavoitteet, työmuodot sekä prosessin eteneminen ja lopputulokset. Tutkimuksellinen kehittämistyö saattaa olla myös hyvin ennakoimatonta, kuten arkielämässä työ yleensäkin. Työ alkaa usein ideoinnista ja päättyy monien kehittelyvaiheiden kautta ratkaisuun, sen toteutukseen ja arviointiin. Tutkimuksellisessa kehittämistyössä korostuu vahvasti toiminnallisuus, parannusten hakeminen asiantiloihin ja ideoiden sekä ratkaisujen toteutettavuuden varmistaminen tutkimuksen keinoin. Kehitystyötä eivät siis ohjaa ensisijaisesti teoreettiset vaan käytännölliset tavoitteet, joihin haetaan tukea teoriasta. Tulosten hyödyllisyys riippuu niiden implementoinnista käytäntöön, eli kehitettyjen ideoiden toteutuksen onnistumisesta. Tutkimuksellinen kehitystyö on ihmisten välistä vuorovaikutusta, tiedon tuottamista, uusien yhteistyösuhteiden rakentamista, liikkumista tuntemattomalla alueella sekä erittäin usein epävarmuuden kohtaamista ja yllättävienkin haasteiden kohtaamista ja käsittelyä. (Ojasalo ym. 2014, 20.)

Tutkimuksellisen kehittämishankkeen lähtökohdiksi voidaan ajatella kehittämiskohteen tunnistaminen ja siihen liittyvien tekijöiden ymmärtäminen. Yleensä hanke liittyy jollakin tavalla liiketoiminnan tai työelämän kehittämiseen ja tarkoituksena on saada aikaan jonkinlainen muutos. Kohteen tunnistamisen jälkeen kerätään siihen liittyvää tietoa, jota voidaan hakea sekä käytännöstä että perehtymällä olemassa olevaan teoreettiseen ja muuhun kirjoitettuun tietoon. Kootulle tiedolle annetaan merkitys suhteessa kehittämishankkeeseen. Samasta aiheesta saattaa löytyä paljon toisistaan poikkeavaa tietoa, jolloin vaaditaan kriittisyyttä luettua kohtaan ja kykyä valintojen tekemiseen ja asioiden yhdistelemiseen. (Ojasalo ym. 2014, 23–24.)

Ojasalo, Moilanen ja Ritalahti (2014, 25–26.) jatkavat, että kohteena olevan organisaation ja toimintaympäristön tausta- ja tutkimustiedon avulla määritellään tarkempi kehittämisen kohde. Tämän jälkeen on mahdollista kuvata kehittämistyöhön liittyvät prosessit, ja kyetään suunnittelemaan oma lähestymistapa ja tarvittavat menetelmät. Lähestymistapa tarkoittaa tässä laajempaa näkökulmaa, josta tutkittavaa ja kehitettävää ilmiötä lähestytään ja jossa voidaan käyttää erilaisia konkreettisia menetelmiä ja ratkaisuja. Työelämässä esimerkiksi toimintatutkimus ja konstruktiivinen tutkimus ovat tyypillisiä lähestymistapoja. Lisäksi tutkimuksellisen kehittämistyön prosessiin kuuluu keskeisenä osana tulosten jakaminen kirjallisena ja mahdollisesti myös tulosten kaupallistaminen. Raportointi on tärkeä osa työtä paitsi työn kuvaamisen kannalta, mutta se myös vie sitä eteenpäin. Raportin muodostaminen jäsentää ajatuksia ja mahdollistaa keskustelua ja palautteen saamista kehittämiseen liittyen Lopuksi on vielä hyvä arvioida tehty työ. Arviointi kohdistuu sekä kehittämisprosessiin että sen tuloksiin. Myös eettiset kysymykset ovat tärkeitä kaikissa kehittämistyön vaiheissa.

2.2 Kehittämistehtävän määrittäminen ja tavoitteet

Tämä opinnäytetyö ja siihen liittyvä kehittämistehtävä on IT-palvelutuotannon laadun ja toiminnan kehittäminen hankkimalla Oulun Tietotekniikalle ulkopuoliselta toimittajalta kyberturvallisuuden kokonaisratkaisu. Oulun Tietotekniikan ja toimittajan välille tullaan laatimaan puitesopimus, jonka avulla voidaan hankkia organisaation tarpeisiin soveltuvia palveluita, laitteita ja ohjelmistoja. Ensivaiheessa hankinta tulee sisältämään ratkaisun herätehallintaan ja IT-ympäristön teknisen terveydentilan valvontaan sekä keskitettyyn lokien hallintaan. Ratkaisu käsittää sekä kumppanin toimittamat tekniset järjestelmät että tarvittavat palvelut, jotka tukevat haluttua tavoitetta. Toinen osa hankintaa on keskitetty lokienhallintajärjestelmä, joka sisältää konsultointityönä lokipolitiikan luomisen, lokienhallinnan, tietoturvavarautumisen ja kehittämisen. Puitesopimuskumppanin tulisi kyetä rakentamaan vaaditut ratkaisut palveluineen. Mikäli kumppani tilaa osan ratkaisuista tai palveluista alihankintana, tulee hänen olla yksin vastuussa kokonaisuudesta.

Onnistuakseen tavoitteeksi asetetun puitesopimuksen luomisessa tulee opinnäytetyön tekijän saavuttaa riittävä tietoperusta toimenpiteistä ja käytännöistä, joita tarvitaan julkisten hankintojen hankintaprosesseissa. Hankintaprosessien luonteen takia täytyy hankintayksikön omata myös riittävä tietoperusta hankittavan kohteen teknisistä vaatimuksista ja esimerkiksi palveluihin liittyvistä tarpeista. Hankintaa varten täytyy sekä tunnistaa nykytilanne ja sen aiheuttamat vaatimukset tahdotulle ratkaisulle, mutta myös määritellä tarkasti mitä ollaan hankkimassa ja millä tavalla se tahdotaan toteuttaa. Vaarana on virhehankinta, joka voi luoda turhia kustannuksia ja pahimmassa tapauksessa ei tuo lainkaan toivottua arvoa organisaation toimintaan.

Kehittämistyön tavoitteet voidaan jakaa kahteen osaan:

1. opinnäytetyön tekijän kyvykkyyden ja tiedon lisääminen palveluhankinnasta ja hankintakohteesta
2. kyberturvallisuusratkaisujen hankintaprojektin aloittaminen.

2.3 Kehittämistehtävän rajaus

Kokonaisuutena kehittämistehtävä on laaja ja sisältää paljon tiedon omaksumista useista eri asiakokonaisuuksista. Tietoperusta rajataan käsittämään vain oleelliset asiat, joita hankinnan toteutuminen vaatii. Eri aiheita joudutaan näin käsittelemään jopa pinnallisesti, mutta kuitenkin riittävällä tasolla niin, että opinnäytetyön lukija saa kuvan siitä, mitä ollaan hankkimassa, miksi se tarvitaan ja ennen kaikkea siitä, miten hankintoja voidaan toteuttaa kuntaorganisaatiossa.

Tavoitteen mukaisen hankintaprosessin läpivieminen on sen laajuuden takia hidasta ja vaatii paljon työtä sekä aiheeseen perehtymistä. Työn valmistelu ja tekeminen aloitettiin talvella 2016 ja varsinainen hankintaprosessin esivalmistelu voitiin käynnistää esitietopyynnöllä elokuussa 2016. Ennakoitu aikataulu hankinnan ja näin ollen myös projektin loppuun saattamiselle on vuoden 2017 loppuun mennessä. Opinnäytetyön tekijän opiskeluoikeus loppuu kuitenkin vuoden 2016 joulukuussa, joten tässä työssä tullaan esittelemään teoriaperustan lisäksi marraskuuhun 2016 mennessä saavutetut tulokset ja opitut asiat. Loppuprojektin osalta esitetään suunnitelma, miten työ jatkuu opinnäytetyön valmistumisen jälkeen. Koska projektia tarkennetaan jatkuvasti suunnitelmien edetessä ja tämän tyylinen työ saattaa muuttua nopeastikin, on tarkkojen suunnitelmien esittäminen kuitenkin mahdotonta. Työn loppuosa ”Jatkotoimenpiteet” esitetään paras arvaus -metodiikalla.

Itse hankintaprojektista rajataan pois mahdolliset jatkokehitystoimenpiteet, ja esimerkiksi valvontapalvelun tuotteistaminen ja myyminen asiakkaille on oma projektinsa.

Opinnäytetyö tehdään Oulun Tietotekniikalle realistisen toimintaympäristön pohjalta konkreettiseen käyttöön ja työhön liittyy myös kolmansien osapuolien salaiseksi luokiteltuja tietoja. Osa tiedoista saattaisi vaarantaa Oulun Tietotekniikan tietoturvan, ja kolmansia osapuolia koskevat tiedot on ilmoitettu toimijoiden taholta salassa pidettäviksi. Tämän vuoksi kaikki tietoturvallisuuden vaarantavat tai salassapitoilmoitusta rikkovat tekniset tiedot sekä yrityksiin selkeästi kohdistettavissa olevat tiedot jätetään tässä opinnäytetyössä julkaisematta. Asian ymmärrettävyyden ja luettavuuden vuoksi asiat esitellään sellaisesta tulokulmasta, että itse työ on mahdollista dokumentoida mahdollisimman selkeästi.

2.4 Tapaustutkimus

Tapaustutkimus soveltuu hyvin kehittämistyön lähestymistavaksi, kun tehtävänä on tuottaa kehittämisehdotuksia ja ideoita, tai kun halutaan syvällisesti ymmärtää kehittämisen kohdetta. Tutkimustavalla voidaan tuottaa tietoa nykyajassa tapahtuvasta ilmiöstä sen todellisessa tilanteessa ja toimintaympäristössä, ja sillä on pyrkimys tuottaa syvällistä ja yksityiskohtaista tietoa tutkittavasta tapauksesta. Näin ollen tapaustutkimuksen avulla on mahdollista ymmärtää yritystä tai kehittämisen kohdetta kokonaisvaltaisesti realistisessa toimintaympäristössä. Tapaustutkimuksessa ei tutkita sitä, miten yleistä jokin on, vaan sitä, kuinka jokin on mahdollista tai kuinka jokin tapahtuu, usein tutkimustapa vastaa kysymyksiin ”miten” ja ”miksi”. Tutkimustavalla ei pyritä tilastolliseen yleistämiseen, eikä se ole otos jostakin isommasta joukosta. Tapausta tutkimalla pyritään huomioimaan paikalliset, ajalliset ja sosiaaliset tilanteet ja yhteydet. Kehittämistyössä on myös tarkoitus tuottaa uutta tietoa kehittämisen tueksi. (Ojasalo, Moilanen & Ritalahti 2014, 52–53.)

Useimmiten tutkimuksen kohteita on vähän, usein vain yksi. Oleellista on kuitenkin, että kohde ymmärretään kokonaisuutena eli tapauksena. Tapaustutkimus on myös mahdollista toteuttaa kahden tai useamman tapauksen vertailuna ja sitä voidaan käyttää yleisesti kaikessa tutkimuksessa ja kehityksessä, jossa itse kohde voidaan rajata esimerkiksi kategorisesti, eli erotetaan fyysinen yksikkö tai yksikköjen joukko tutkimuskohteeksi. Vaihtoehtona on myös funktionaalinen rajaaminen, eli erotetaan jokin toiminnallinen kokonaisuus, prosessi, tapahtuma tai tapahtumasarja kokonaisuudeksi. (Ojasalo ym. 2014, 53.)

Parhaimmillaan muutokseen suuntautuvat kehittämishankkeet sisältävät aina arvioinnin ajatuksen. Jotta hanke pääsisi tulokseen, tarvitaan arviointi- eli evaluointitietoa. Jatkuva muutos tarvitsee avukseen jatkuvasti käynnissä olevan kehittämisprosessin, joka hyödyntää paitsi hankkeen toimintaympäristön materiaalia, myös sisäistä toimintaa arvioivaa tietoa. Evaluoivan kehittämisen lähtökohtana on luoda seurannan ja arvioinnin systeemi, josta saadaan tietoa kehitystyön eteenpäin viemiseksi. Jotta tiedosta saadaan kaikki hyöty irti, kannattaa se kytkeä mukaan hankkeen työprosesseihin. Hyvin järjestetyssä kehittämishankkeessa käytetään arvioivaa työtapaa, jolloin omaan työhön suhtaudutaan tutkivasti ja muuttavasti. Keskeistä tällöin on työn sisäisen logiikan ja työprosessien avaaminen. Realistisen evaluaation mallissa mukaan otetaan alusta alkaen kehityshankkeen prosessiluonne, eli sen prosessuaalisuus. Se tarkoittaa rakenteiden ja kontekstien käsittämistä dynaamisiksi, toiminnallisiksi, ajassa ylläpidettäviksi ja muuttuviksi. Todellisuus näyttäytyy jatkuvassa tuotannossaan ja keskeytymättömässä tulemisessaan. (Anttila 2007, 83.)

Yhden tai muutaman tapauksen tulkitsevaa ja ymmärtävää, tapauksen ainutlaatuisuudesta kiinnostunutta tutkimusta kutsutaan intensiiviseksi tapaustutkimukseksi. Tälle tutkimustavalle on tyypillistä, että tutkija tarkastelee tapausta tutkimukseen osallistuvien näkökulmasta ja heidän omilla käsitteillään ja kielellään. Kun tutkitaan useita tapauksia, joissa tehdään vertailua ja etsitään selityksiä, kutsutaan sitä ekstensiiviseksi tapatustutkimukseksi. Tällöin tutkimukselle on tyypillistä muihin tapauksiin yleistettävien teoreettisten ideoiden, käsitteiden ja selitysmallien kehittäminen ja testaus sekä tapausten käyttäminen välineinä työssä. (Eriksson ja Koistinen 2005, 15).

Eriksson ja Koistinen (2005, 17.) jatkavat, että ekstensiivisessä tapaustutkimuksessa pyritään löytämään ilmiöitä tai prosesseja koskevia yhteisiä ominaisuuksia ja yleisiä malleja sekä kehittämään uusia teoreettisia ideoita ja käsitteitä monen tapauksen järjestelmällisen vertailun eli replikoinnin avulla. Pyrkimyksenä on selittää ilmiöitä tai kehittää uutta teoriaa käyttämällä empiirisenä materiaalina useita tapauksia ja niiden vertailua. Tavoitteena on joko aiempien teoreettisten käsitteiden testaus ja täydentäminen uudessa ympäristössä, uusien teoreettisten ideoiden tai käsitteiden kehittäminen, kokeilu tai uuden teoreettisen selitysmallin luominen. Ekstensiivisessä tapaustutkimuksessa tutkittavia tapauksia vertaillaan toisiinsa jollakin tavalla. Tällöin on kyse vertailevasta tutkimusasetelmasta ja oleellista on se, miten vertailua tehdään.

Tässä opinnäytetyössä on tarkoitus hankkia organisaation käyttöön tekninen järjestelmä ja palvelukokonaisuus ulkopuoliselta toimittajalta. Jotta sopivin toimittaja ja ratkaisu tulisi valituksi, täytyy hankintayksiköllä olla riittävä tietoperusta ja ymmärrys hankinnan kohteesta. Tavoitteena on konkreettisesti saada aikaan hankintasopimus toimijan kanssa, joka täyttää asetetut kelpoisuusehdot ja vastaa kokonaistaloudellisesti edullisimmin tarjouspyynnössä esitettyihin vaatimuksiin.

Toimintaa dokumentoidaan projektisuunnitelman avulla ja samalla siitä tallennetaan tietoa muun organisaation hyödynnettäväksi muissa hankinnoissa ja luomaan ymmärrys tästä opinnäytetyöstä ja siihen liittyvän projektin sisällöstä ja tuloksista.

Tapaustutkimuksen periaatteet ja metodit sopivat tällaiseen työhön hyvin, koska tarkoituksena on kehittää uutta samalla dokumentoiden sitä. Markkinakartoitusvaiheessa tehdään tutkimusta, jonka avulla pyritään selvittämään millaisia toimittajia ja ratkaisuja markkinoilta löytyy ja millaisia vaatimuksia tarjouspyynnössä haetulle ratkaisulle asetetaan.

3 ITIL – PARHAAT KÄYTÄNNÖT

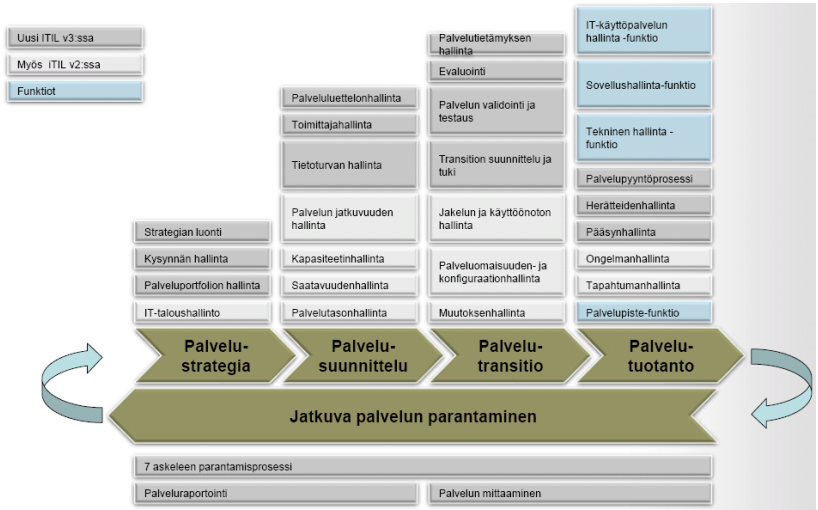
ITIL (Information Technology Infrastructure Library) on prosessikehys, jonka avulla voidaan johtaa tehokkaasti IT-palveluja ja niiden tuottamiseen käytettäviä prosesseja. Prosessien lisäksi se on kokoelma parhaita käytäntöjä IT-palveluhallintaan, suunnitteluun ja johtamiseen. Se on globaalisti tunnettu viitekehys, jota on käytetty ja kehitetty jo yli 20 vuotta. (itSMF Finland ry 2016, viitattu 19.10.2016.)

ITIL-mallia ei ole tarkoitettu käytettäväksi suoraan sellaisenaan, vaan se on kokoelma parhaita käytäntöjä (Best Practices), joista organisaatio voi ottaa käyttöönsä itselleen parhaat osat ja soveltaa niitä omaan toimintaansa sopivalla tavalla. ITIL ei pakota mihinkään tiettyyn toimintamalliin, vaan tarjoaa testattuja ja käytäntöön sopivia toimintamalleja palvelutuotannon eri osa-alueille.

ITIL-versiossa 2 otettiin käyttöön prosessinäkökulma ja jaettiin prosessit Service Support- ja Service Delivery -prosesseihin. ITIL-versio 3 otti käyttöön selkeän palvelunäkökulman ja jaottelee prosessit palvelun elinkaarimallin mukaan. (itSMF Finland ry 2016, viitattu 19.10.2016.)

ITIL- mallissa palvelut jaetaan viiteen eri vaiheeseen:

1. palvelustrategia (Service Strategy)
2. palvelusuunnittelu (Service Design)
3. palvelutransitio (Service Transition)
4. palvelutuotanto (Service Operation)
5. jatkuva palvelun parantaminen (Continual Service Improvement).



KUVA 1. Millog 2015. Palvelujen elinkaaren prosessit ITIL:n mukaan. (viitattu 12.11.2016)

3.1 Palvelustrategia (Service Strategy)

Yksinkertaisimmillaan strategia on suunnitelma, joka viitoittaa tavat, joilla organisaatio pääsee asettamiinsa tavoitteisiin. Palvelustrategia-elinkaarivaiheessa määritellään, mitä palveluita tuotetaan ja miten palveluntuottaja voi ne toimittaa niin, että liiketoiminta tai asiakas saavuttaa omat määrätyt tavoitteensa. Tässä vaiheessa määritetään tarvittavat viitekehykset, joiden avulla voidaan luoda ja toteuttaa onnistunut ja toimiva palvelustrategia. (ITIL Service Strategy 2014, 35.)

Hyvä liiketoimintasuunnitelma sisältää kuvauksen organisaation keinoista saavuttaa asetetut tavoitteet. Palvelustrategian avulla voidaan määrittää organisaation kyky tuottaa ja toimittaa arvoa asiakkaalle ja asiakkaan liiketoiminnalle. Ilman selkeästi määritettyä palveluastrategiaa on vaikea perustella asiakkaalle oman organisaation kyvykkyyttä toimia ja tehdä asioita paremmin kuin kilpailijat. (ITIL Service Strategy 2014, 36.)

3.2 Palvelusuunnittelu (Service Design)

Palvelusuunnittelun tarkoitus on suunnitella uusia ja muuttuvia palveluita, jotta ne voidaan viedä transition kautta tuotantoon. Poistuvien palveluiden poisto täytyy myös suunnitella ja toteuttaa hallitusti. Palvelusuunnittelun avulla on mahdollista suunnitella parempi ajan, kustannusten ja resurssien hallinta. Sen avulla onnistuvat myös paremmin muutokset, palveluihin käytetty uudelleensuunnitteluaika ja uusien tai muuttuvien palveluiden käytettävyys ja kustannustehokkuus (ITIL Service Design 2014, 35.)

Kaikki palvelusuunnitelmat ja palvelusuunnitelmien toteuttamiseksi tarvittavat toimenpiteet tulee viedä käytäntöön liiketoimintalähtöisesti ja organisaation tarpeet huomioiden. Hyvä lähtökohta palvelusuunnittelulle on analysoida ja ottaa huomioon organisaation liiketoiminan tarpeet ja rakentaa palvelusuunnittelupaketti, joka puolestaan viedään eteenpäin palvelutransitiolle. (ITIL Service Design 2014, 35.)

3.3 Palvelutransitio (Service Transition)

Palvelutransition tarkoitus on varmistaa, että sen elinkaaren aikana tuotetut uudet, muutetut tai lopetetut palvelut vastaavat liiketoiminnan tarkoitusta, kuten palvelustrategia- ja

palvelusuunnitteluvaiheissa on suunniteltu ja dokumentoitu. Palvelutransitiovaiheessa käydään läpi muun muassa muutoksenhallintaa ja riskienhallintaa sekä varmistetaan, että muutokset tuottavat toivotun lopputuloksen (ITIL Service Transition 2014, 4.)

Transitiovaiheessa pyritään muun muassa hallitsemaan muutoksia onnistuneesti, hallitsemaan uusien tai poistuvien palveluiden riskejä ja varmistamaan että palvelumuutokset tuottavat toivottua arvoa liiketoiminnalle. Jotta näihin tavoitteisiin päästään, täytyy transitiovaiheessa suunnitella ja hallita tuotantokapasiteettiä ja resursseja. Lisäksi on varmistettava toimivat ja toistuvat mekanismit palveluiden julkaisulle ja varmistaa että palveluita voidaan hallita, operoida ja tukea kuten palvelusunnitteluvaiheessa on määritety. (ITIL Service Transition 2014, 4.)

3.4 Palvelutuotanto (Service Operation)

Palvelutuotanto on ITIL:n elinkaarivaihe, jossa liiketoiminta saa näkyvää arvoa investoinneistaan. Palvelutuotantovaiheessa toteutetaan käytännössä palvelusuunnittelun ja -transition suunnitelmat. Palvelutuotanto on myös se ITIL-elinkaaren vaihe, joka näkyy konkreettisimmin asiakkaalle. Tämän prosessin vastuulla on tehokas tuotanto, hyväksytyt kustannukset, käyttäjätyytyväisyyden seuraaminen sekä palveluiden tuottaminen sovitulla palvelutasolla. (ITIL Service Operation 2014, 35.)

Palvelutuotanto sisältää herätteiden hallinnan, joka on läheisesti kytköksissä häiriö- ja ongelmahallintaan. Järjestelmäksi suositellaan yksinkertaista ja helposti muunneltavissa olevaa standardoitua järjestelmää, joka mahdollistaa herätetietojen takaisinsyötön palvelusuunnittelu- ja transitiovaiheisiin. Teknologian suositellaan myös mahdollistavan asiakkaan näkymän sekä suoran kytköksen organisaation häiriöhallintaprosesseihin. (ITIL Service Operation 2014, 219.)

Tämä on myös ITIL:n vaihe, jossa otetaan kantaa läheisesti tämän opinnäytetyön kehittämistehtävään. Herätehallintaprosessi ja sen kehittämisen idea ovat lähtöisin ITIL:n ajatuksista ja muun muassa niiden peruskuvausten perusteella organisaation toimintaa on lähdetty kehittämään eteenpäin.

3.5 Jatkuva palvelun parantaminen (Continual Service Improvement)

Tämä elinkaarivaihe määritellään tapahtumaan jokaisessa ITIL:n kuvaamassa elinkaarivaiheessa. Se on jatkuva prosessi, jonka tarkoitus on lisätä palveluiden tehokkuutta, optimoida palveluiden kustannukset ja prosessit sekä maksimoida palveluiden vaikuttavuus. (ITIL Continual Service Improvement 2014, 35.)

Jatkuvan palvelun parantamisen vaiheen tarkoitus on tiivistää yrityksen liiketoiminnan tavoitteet ja visio. Nykytilan arvioinnilla määritellään, mikä tilanne on tällä hetkellä ja mihin halutaan päästä. Tällä saadaan suunta siihen, mitä on tarpeen tehdä. Palveluiden parantaminen määritetään, arvotetaan ja suunnitellaan huolellisesti, ja lopuksi määritellään mittarit, joiden perusteella muutokset ja tulokset arvioidaan. (ITIL Continual Service Improvement 2014, 35.)

4 KYBERTURVALLISUUDEN MÄÄRITELMÄ

Tietoturvallisuus keskittyy tietojen luottamuksellisuuden, eheyden ja saatavuuden takaamiseen, kun taas kyberturvallisuus kattaa huomattavasti laajemman kokonaisuuden. Kyberturvallisuudella on tarkoitus varmistaa, että kybertoimintaympäristöön voi luottaa ja sen tarkoituksenmukaisesta toiminnasta huolehditaan. Kybertoimintaympäristöllä tarkoitetaan sähköisessä muodossa olevaa tietojenkäsittelyn ympäristöä, joka taas koostuu tietojärjestelmistä. (Rousku 2014, 33.)

Nykyaikainen teknistynyt yhteiskunta on yhä enenevissä määrin riippuvainen tietotekniikan avulla tuotettavista palveluista, ja tietojärjestelmien avulla ohjataan useiden yhteiskunnalle välttämättömien perustarpeiden saatavuutta. Sähkön saantia pidetään itsestäänselvyytenä, mutta entäpä jos sähkönsiirtoverkko lamaantuu vaikkapa luonnonkatastrofin tai terroriteon seurauksena. Lyhyt katkos ei vielä näy ihmisten normaalissa arkielämässä, mutta pitempään jatkunut keskeytyminen voi olla vaarallista. Erityisesti näin voi käydä talviaikaan, kun sähkölämmitteiset talot kylmenevät, vesijohtoverkosto lakkaa toimimasta, pankkiautomaateista ei saa rahaa ja kaupat eivät voi myydä hyödykkeitä. Sähköriippuvuuden lisäksi on havaittavissa, että ihmisten kriisinsietokyky on selvästi heikentynyt, ja emme osaa varautua taikka toimia erilaisissa häiriötilanteissa. Olemme oppineet luottamaan siihen, että yhteiskunnassa kaikki toimii luotettavasti ja hyvin. (Limnéll, Majewski & Salminen 2014, 49.)

Kyberturvallisuus on käsitteenä ja sisällöltään verrattain laaja, ja se on myös kohtuullisen uusi käsite, joka usein sivuutetaan, koska ei välttämättä ymmärretä sen tärkeyttä tai varsinaista ydinasiaa. Kyberturvallisuus-sanalla voidaan tarkoittaa monia eri asioita riippuen henkilöstä tai asiayhteydestä. On siis syytä käydä tätä ydinajatusta ja termistöä tarkemmin lävitse.

Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry määrittelee, että kyberturvallisuus on tavoitetila, jossa kyberympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus pitää sisällään kaikki sellaiset toimenpiteet, joiden avulla voidaan ennakoitavasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Tavoitetilana on myös, että kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriöitä sähköisen tiedon käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. (FiCom ry 2016. Kyberympäristö ja kyberturvallisuus, viitattu 23.10.2016.)

Kyberympäristö voi muodostua yhdestä tai useasta tietojärjestelmästä. Tietojärjestelmät puolestaan koostuvat atk- ja tiedonsiirtolaitteista, ohjelmista sekä ihmisistä. Näitä voidaan ajatella tiedon infrastruktuurina, ja koska tietoyhteiskunnan tieto on sähköisessä muodossa, jolloin

kyberympäristö on kokonaisuus, jossa sähköisessä muodossa olevaa tietoa käsitellään tietotekniikan avulla. Edelleen tätä tietoa käsitellään tietojärjestelmissä, joista kyberympäristö muodostuu. (FiCom ry 2016. Kyberympäristö ja kyberturvallisuus, viitattu 23.10.2016.)

Kyberturvallisuus on kuitenkin myös muuta kuin pelkkää teknologista varautumista ja tiedon suojaamista. Limnéll, Majewski ja Salminen (2014, 47–48.) toteavat kirjassaan Kyberturvallisuus, että on hyvä muistaa kyberturvallisuuden olevan vähintään 2/3 muuta kuin teknologiaa tai teknologisia ratkaisuja. Kybertoimintaympäristössä asioita voi tapahtua myös ilman, että havaitsemme tai tiedostamme niitä. Vakoiluohjelmat eivät haittaa toimintaa, eivätkä kaapatun internetsivuston väärään osoitteeseen ohjautuvat käyttäjät välttämättä näy sivujen ylläpitäjälle. Kyseisessä kirjassa jatketaan, että mikäli kybermaailman ja sen turvallisuuden vaikutuksia omassa organisaatiossa ei tunneta, saattavat turvallisuuteen liittyvät päätökset johtaa yllättäviin seuraamuksiin. Toisaalta myös kybermaailman ja fyysisen maailman yhteen kietoutuminen on usein niin monimutkaista, että yllättäviä seurauksia syntyy, vaikka päätösten vaikutukset omaan organisaatioon tunnettaisiin. Toisaalta ei kannata myöskään mieltää kybermaailman mahdollisuuksia ja uhkia liian monimutkaisiksi ja tämän varjolla sivuuttaa niitä.

Tietoturva- ja kyberturvallisuus-käsitteet saattavat helposti sekoittua toisiinsa, ja onkin hyvä selventää näiden eroja. FiCom ry:n määrittelyn mukaan tietoturva suojaa tietojärjestelmässä käsiteltäviä tietoja. Jos tietoturva pettää, seurauksena voi kyberympäristö toimia toisin kuin oli tarkoitus. Esimerkiksi vaikutus metroon voisi olla sellainen, että junat lähtisivät väärään aikaan tai väärään suuntaan. Kyberturvallisuuden tavoitteena taas on varmistaa, että kyberympäristöstä ei aiheudu haittaa, vaaraa tai häiriötä tästä ympäristöstä riippuvaiselle toiminnalle. Kyberturvallisuus on toimivan kyberympäristön tuotos ympäröivään yhteiskuntaan. (FiCom ry 2016. Kyberympäristö ja kyberturvallisuus, viitattu 23.10.2016.)

Suomen kyberturvallisuusstrategiassa tiivistetään vielä olennaisilta osin kyberturvallisuuden luonnetta. Voimakkaasti lisääntynyt tietointensiivisyys, toimintojen ulkoistaminen, ulkomaisen omistuksen kasvu, erilaiset integraatiot tieto- ja viestintäjärjestelmien kesken, avoimet tietoverkot ja voimakkaasti lisääntynyt riippuvuus sähköstä ja sen varassa olevista toiminnoista ovat luoneet yhteiskunnalle uudenlaisia vaatimuksia sen elintärkeiden toimintojen turvaamiseksi. Kyberympäristöön kohdistuvat uhkat ovat muuttuneet aiempaa vaarallisemmiksi yritysten, yhteiskunnan ja jopa yksittäisten ihmisten kannalta. Nykyään uhkakuvia muodostavat toimijat ovat ammattimaisempia ja myös valtiolliset toimijat lasketaan nykypäivänä uhkakuviin. Toisaalta turvallinen kybertoimintaympäristö voidaan nähdä mahdollisuutena ja voimavarana mahdollistaen yksilöiden ja yritysten taloudellisuutta ja toimintaa. Hyvä ja turvallinen toimintaympäristö parantaa

myös Suomen kansainvälistä houkuttelevuutta investointikohteena. Myös kyberturvallisuus itsessään on voimakkaasti vahvistuva liiketoiminnan alue. (Yhteiskunnan turvallisuus 2013. Suomen kyberturvallisuusstrategia, viitattu 20.10.2016.)

5 TIETOTURVA

Muutama vuosikymmen sitten tietokoneita ja niihin liittyviä järjestelmiä oli hyvin vähän ja ne olivat erikoistuneet tarkoin määriteltyihin toimintoihin, joita suoritettiin usein manuaalisesti ihmisten toimesta tehtävä kerrallaan. Suuria keskusyksiköitä operoitiin tyhmien päätteiden kautta, jotka olivat yhteydessä vain suoraan keskusyksikköön. Keskuskoneiden suojaaminen oli helppoa, koska niitä oli vähän ja hyvin harva ihminen osasi käyttää niitä tai yleensä ymmärsi operoimiseen tarvittavaa tekniikkaa. Samat ihmiset pystyivät myös valvomaan mahdollisuutta päästä operoimaan näitä laitteita, joten tietoturvasta oli yksinkertaista ja helppoa huolehtia. Kun tietokoneiden käyttösovellukset lisääntyivät ja monipuolistuivat, yritykset tulivat entistä riippuvaisemmiksi niistä ja pian huomattiin, että ei ollut kannattavaa päästää työntekijöitä käyttämään keskuskoneiden kapasiteettia vain vähäksi aikaa kerrallaan. Kun työpöytäkoneet alkoivat yleistyä, keskuskoneiden laskentateho tuotiin lähemmäs työntekijää, jolloin pystyttiin tekemään pieniä ja helppoja ”ajoja” oman työpöydän äärestä. Suuret laskentatehoa vaativat operaatiot suoritettiin edelleen suoraan keskuskoneilla. Kehitys jatkoi kulkuaan ja työpöytäkoneiden kehitys mahdollisti keskuskoneista riippumattoman ja autonomisen toiminnan. Pian huomattiin, ettei ollut järkevää varastoida tietoa jokaiselle työpöytäkoneelle, jos samaa tietoa käytettiin myös muilla yksiköillä. Niinpä tietoa alettiin varastoida erillisille palvelinkoneille, joista työpöytäkoneet hakivat sitä vain tarvittaessa. Koneiden ja käyttäjien lisääntyminen johti siihen, että pian oli tuhansia käyttäjiä, jotka osasivat käyttää ja hyödyntää koneita ja niiden mahdollisuuksia. Kohdattiin uusia ongelmia, joita ei ollut olemassa suurten keskuskoneiden alkukoina. (Harris 2005, 17–18.)

Suurten keskustietokoneiden ajoista on tultu pitkä matka ja kehitys näyttää jatkuvan koko ajan kiihtyvällä tahdilla. Suomen Internetoppaan mukaan tänä päivänä tietoturvalla pyritään suojaamaan yritysten tärkeät tiedot ulkopuolisilta tahoilta toimenpiteillä, jotka takaavat tietojen koskemattomuuden. Jotta tietoon voidaan luottaa, on sen oltava vain siihen oikeutettujen käytössä. (Suomen Internetopas 2016. Tietoturva, viitattu 27.10.2016.)

Tiedolla ja tietoaineistolla voidaan tarkoittaa mitä tahansa kuviteltavissa olevaa tietoa missä tahansa muodossa. Tällaista voi olla esimerkiksi asiakirja, joka on tehty käyttäen tekstinkäsittelyohjelmaa, musiikkikappaleet, videot tai jopa ihmisten esittämät ajatukset ja ideat. Perinteisessä tallennusmuodossa voidaan tiedon ajatella olevan paperilla tai jollakin fyysisellä tavalla tallennettuna, nykyään puhutaan tietojärjestelmistä ja sähköisesti käsiteltävästä muodosta. (Rousku 2014, 30.)

5.1 Tiedon luottamuksellisuus

Mikäli tiedon katsotaan olevan luokiteltua tai muuten salassa pidettävää, voidaan sen käyttöoikeus myöntää vain tahoille, joilla on siihen tiedonsaanti- ja käyttöoikeus. Tietojärjestelmien osalta luottamuksellisuus toteutetaan normaalisti käyttöoikeuksien hallinnalla. Tällöin käyttäjälle annetaan vain sellaiset oikeudet, jotka ovat tarpeen tehtävien hoitamisen kannalta. Käyttöoikeudet eli salasanat ja käyttäjätunnukset on syytä pitää huolellisesti salattuina muilta, koska jos ne joutuvat tietoverkkorikolliselle, hän voi käyttää niitä tietovuodon mahdollistamiseen tai vahingon aiheuttamiseen. Mitä kriittisempi tietojärjestelmä on, sen tärkeämpää on tietojen eheyden säilyttäminen ja organisaation kyky palauttaa hallitsemattomasti muuttuneet tiedot esimerkiksi varmuuskopioista. (Rousku 2014, 29.)

5.2 Tiedon eheys

Tiedon eheys tarkoittaa, että tieto ei saa muuttua hallitsemattomasti, eli tietoa saavat muuttaa vain sellaiset käyttäjät ja järjestelmät, joilla on siihen tarvittava käyttöoikeus ja vain sallituilla keinoilla. Tieto- ja kyberturvallisuuden näkökulmasta tällaisia ovat esimerkiksi kansalaisten terveydenhuoltoon liittyvät tiedot, julkishallinnon johtamisjärjestelmät, pankkijärjestelmät, verotus-, maanomistus- ja kiinteistötiedot sekä vakuutustiedot. Tiedot on oltava kaikissa olosuhteissa palautettavissa, mikäli hallitsematon muutos tapahtuu. Esimerkkinä vapaa-ajan käytöstä voidaan ajatella, että väärinkäyttäjä pääsee kirjautumaan toisen käyttäjän Facebook-profiiliin ja voi kirjoittaa sinne mitä tahansa tai muutella mitä tahansa tietoja haluamikseen. (Rousku 2014, 29.)

5.3 Tiedon saatavuus

Tiedon saatavuudella tarkoitetaan, että tietojen on oltava saatavilla niitä tarvitsevalle käyttäjälle IT-järjestelmien tai palveluiden toiminnoilta edellytettävällä vasteajalla (SLA). Yhteiskunnan digitalisoitumisen myötä kuitenkin tietoa tarvitaan jatkuvasti, eli tietojen ja palveluiden tulee olla saatavilla jatkuvasti. Käytännössä palvelut pyritään aina pitämään käytössä sadan prosentin vasteajalla, joskin pakolliset huoltokatkot jätetään saatavuudesta pois. (Rousku 2014, 30.)

5.4 Tietomurto

Finlex on oikeusministeriön omistama oikeudellisen aineiston julkinen ja maksuton internet-palvelu. Rikoslain luvussa 38 pykälässä 8 kuvataan tietomurto seuraavasti:

> ”Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta
>
> 1) teknisen erikoislaitteen avulla tai
>
> 2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin
>
> oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.
>
> Yritys on rangaistava.
>
> Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.”

(Suomen rikoslaki 2016. Asetus tietomurrosta 10.4.2015/368 38:8 §, viitattu 23.10.2016.)

On syytä huomata erityisesti kohta ”yritys on rangaistava”. Eli vaikka ei murtautuisi tai onnistuisi murtautumisessa, vaan ainoastaan kokeilee onneaan, tulkitaan teko lain mukaan tietomurroksi, eikä kokeilu ole lieventävä asianhaara. Tietomurtojen yleistyminen johtuu osittain entistä laajemmasta tietotekniikan hyödyntämisestä ja helppokäyttöisten murtautumisvälineiden ja ohjeiden helposta ja laajasta saatavuudesta internetissä. (Rousku 2014, 34.)

5.5 Haavoittuvuudet

Haavoittuvuus on teknisessä järjestelmässä oleva vika, jonka avulla järjestelmää on mahdollista käyttää sellaisella tavalla, jota varten sitä ei ole suunniteltu. Yleensä puhutaan tietoturvahaavoittuvuuksista, joiden avulla järjestelmää väärinkäyttämällä on mahdollista suorittaa esimerkiksi tietomurto. Tällöin murtautuja voi päästä haavoittuvuutta hyödyntäen esimerkiksi järjestelmän päätasolle ja muuttaa, vahingoittaa tai varastaa tietoja. Usein myös haavoittuvuuksia

hyödynnetään niin, että niiden kautta järjestelmään sijoitetaan vakoilu- tai haittaohjelmia. Pahimmillaan tällaiset ohjelmat voivat olla järjestelmässä pitkiäkin aikoja ilman, että käyttäjä tietää niiden olemassaolosta. Järjestelmätoimittajien vastuulla on korjata tunnistetut ja ilmoitetut haavoittuvuudet, sekä julkaista niitä korjaavia päivityksiä, joilla korjataan tunnetut haavoittuvuudet. Nollapäivähaavoittuvuudet ovat haavoittuvuuksia jotka ovat tiedossa, mutta joihin järjestelmän toimittajalla ei ole olemassa korjausta. Kun tieto tällaisesta haavoittuvuudesta pääsee julkisuuteen, järjestelmätoimittaja pyrkii tiedottamaan keinoista, joilla uhkaa voidaan pienentää ennen kuin korjaus on julkaistu. (Rousku 2014, 30.)

5.6 Organisaation varautuminen ja jatkuvuuden hallinta

Kun tietojärjestelmään tai palveluun tulee ongelma, joka voi olla tekninen häiriö tai esimerkiksi tietomurto, organisaatiolla on syytä olla selvillä suunnitelma, jonka avulla palaudutaan normaaliin toimintaan ja turvataan toiminnan jatkuvuus. Mitä kriittisemmästä toiminnosta on kyse, sitä laaja-alaisemmat ja kattavammat tulisi suunnitelmien olla. Näin pyritään varmistamaan, että häiriöstä tai tapahtumasta aiheutuvat vahingot pysyisivät mahdollisimman pieninä. Käytännössä suunnitelmat perustuvat organisaation liiketoiminnan jatkuvuuden takaamiseen, jolloin sellaiset toiminnot, joiden häiriöillä ei katsota olevan suurta merkitystä toimintaan, jäävät pienemmälle huomiolle. Eri toimintojen keskinäiset riippuvuudet tulisi osata arvioida ja kuvata niin, että tiedetään mahdollisimman tarkasti, miten mikäkin toiminta vaikuttaa kokonaisuuteen. Yksittäisillä tietojärjestelmillä tulisi olla omat toipumissuunnitelmat, joiden avulla huolehditaan häiriöiden korjaamisesta ja normaalitilan palauttamisesta. (Rousku 2014, 36.)

5.7 Oulun kaupungin tietoturvapolitiikka

Oulun kaupungilla on kirjattuna tietoturvapolitiikka, joka on kaupungin ylimmän johdon hyväksymä strateginen asiakirja ja se on myös samalla kannanotto tietoturvan kehittämiseen. Tietoturvapolitiikassa todetaan, että tavoitteena on luoda Oulun kaupungin konserniohjeen mukaisesti yhdenmukaiset toimintaperiaatteet ja käytännöt hyvän tietoturvatason toteuttamiseksi. Politiikan toteuttamisella luodaan edellytykset tietoturvallisen toiminnan pitkäjänteiseen

kehittämiseen ja työssä onnistuminen edellyttää kaupungin johdon sitoutumista tietoturvatyön tukemiseen. (Oulun kaupungin tietoturvapolitiikka 2013, 3.)

Tieto eri muodoissaan on tärkeä perusta kaikelle kaupungin toiminnalle, sillä tarkoitetaan tietojen suojaamista eri uhkatekijöiltä ja samalla varmistetaan palveluiden jatkuvuus minimoiden toimintaan tai asiakkaiden tietoihin liittyvät riskitekijät. Osa tietoturvaa on myös tietosuoja, jolla varmistetaan ihmisten yksityisyyden kunnioittaminen ja suojeleminen oikeudellisia säännöksiä noudattavin periaattein ja käytännöin. Tietoturvapolitiikassa määritellään tietoturva kolmen peruskäsitteen kautta. Tietojen luottamuksellisuus, tietojen eheys, sekä palveluiden ja tietojen saatavuus. (Oulun kaupungin tietoturvapolitiikka 2013, 3.)

Tiedon turvaaminen on merkittävä osa kaupungin toiminnan sekä sen tuottamien palveluiden laatua, ICT- riskienhallintaa ja kokonaisturvallisuutta. Keskeisenä tavoitteena riskienhallinnassa on tunnistaa toimintaan kohdentuvat riskitekijät sekä arvioida niitä ja ryhtyä tarvittaviin toimenpiteisiin. (Oulun kaupungin tietoturvapolitiikka 2013, 4.)

Oulun kaupungin tietoturvapolitiikassa otetaan kantaa oleellisiin tietoturvan kehittämisalueisiin ja pyritään varautumaan tulevaisuuden haasteisiin. Yhdeksi näkökohdaksi on otettu tietoturvan visio, jonka mukaan monikanavaiset palvelut tuotetaan luotettavalla ja tietoturvallisella ICT-infrastruktuurilla. Tietoturva on kiinteä osa johtamista, riskienhallintaa, palvelutoimintaa ja esimiestyötä. Lisäksi tietoturvan hallinta on hyvällä tasolla ja toimintaan vaikuttavia tietoturvan häiriötilanteita esiintyy mahdollisimman vähän, Oulun kaupunki toimii aktiivisena tietoturvan kehittämistoimijana ja verkostoituneena edelläkävijänä ICT-varautumisessa.

Oulun kaupungin tietoturvapolitiikan visio 2020:

> ”Oulun kaupungilla on käytössään kokonaisvaltainen tietoturvan hallintajärjestelmä ja työntekijät ovat tietoturvatietoisia, motivoituneita ja sitoutuneet yhteisesti asetettuihin tietoturvatoiminnan tavoitteisiin.”

Oulun kaupungin tietoturvapolitiikassa on määritelty, että häiriötilanteisiin varautumiseksi ja nopean reagoinnin varmistamiseksi kaupungille perustetaan ICT-turvallisuusjohtamisen tiimi. Sen tehtävänä on päättää, miten uhkatilanteeseen reagoidaan ja mitä toimenpiteitä käynnistetään mahdollisimman nopeasti samalla minimoiden uhkatekijöistä aiheutuvia vakavia haittatekijöitä. Tiimiin kuuluvat henkilöt ovat tavoitettavissa hälytysringin muodossa 24/7 eri viestintävälineillä. (Oulun kaupungin tietoturvapolitiikka 2013, 14.)

6 HERÄTTEIDEN HALLINTA

Herätteeksi voidaan määritellä mikä tahansa muutos, jolla on vaikutusta IT-järjestelmään tai palveluun. Herätteet tunnistetaan tyypillisesti joko erilaisista automaattisista ilmoituksista tai monitorointityökalun avulla. Automaattiset ilmoitukset voivat tulla esimerkiksi ohjelmiston, palvelimen tai tietoliikenteen normaalista poikkeavista tapahtumista. Tehokas palvelutuotanto on tietoinen palveluiden ja järjestelmien tilasta, sekä niiden normaaleista tai ennakoimattomista muutoksista. (ITIL Service Operation, 58.)

Herätteitä saadaan tyypillisesti kahdella eri tavalla:

- Aktiiviset valvontatyökalut, jotka kyselevät eli pollaavat koko ajan aktiivisesti järjestelmien tilaa ja saatavuutta. Poikkeama normaalista tilasta muodostaa hälytyksen, johon täytyy reagoida joko automaattisen järjestelmän tai ihmisen toimesta.

- Passiivinen valvontatyökalu, joka vastaanottaa hälytyksiä ja ilmoituksia poikkeamatilanteista ja lähettää ennalta sovitulla tavalla ilmoituksen sovittuun paikkaan, joka voi olla esimerkiksi sähköpostilaatikko tai valvontajärjestelmä.

Herätteiden hallinta ja valvontajärjestelmät ovat hyvin lähellä toisiaan toiminnollisesti, mutta on hyvä tiedostaa niiden välillä olevat eroavaisuudet. Herätehallinta keskittyy tyypillisesti seuraamaan ja tuottamaan häiriö- ja ilmoitusviestejä IT-infrastruktuurista ja palveluista. Tämä vaatii yleisesti vuorovaikutteisuutta seurattavien järjestelmien ja seurantatavan välillä. Valvonnan voidaan käsittää olevan suurempi kokonaisuus, johon voidaan paitsi tuoda herätteitä, mutta samalla myös seurata palveluiden tai laitteiden tilaa. Esimerkiksi tietoliikennedata, palvelinten kuormitus tai vaikkapa palomuurin statustila voidaan asettaa valvontaan ja niiden tilaa seurataan, vaikka ne eivät muodostaisi herätteitä. Yksinkertaistaen herätehallinnassa jokin asia laitetaan spesifisesti seurantaan, mutta valvonta paitsi seuraa näitä herätteitä, myös tapahtumia yleisesti ilman varsinaista ilmoitusta. (ITIL Service Operation, 59.)

Vaikka herätehallinta on ITIL:n prosesseissa kuvattu tarkkaan kytköksineen muihin prosesseihin, on myös tässä tapauksessa hyvä nimenomaan poimia parhaat käytänteet ja sovittaa ne oman organisaation toimintoihin. Mikäli herätteitä lähdetään tulkitsemaan ja viemään liian orjallisesti valmiiden säännösten mukaan, voidaan joutua tilanteeseen, jolloin prosessista on enemmän haittaa kuin hyötyä. Esimerkiksi levyjärjestelmässä tapahtuu levyrikko, josta muodostuu heräte, joka ohjataan sitten palveluhallinnan häiriöjonoon. Mikäli jonossa on jo muita häiriöitä, jotka ovat

vaikuttavuudeltaan pienempiä, mutta joiden SLA on umpeutumassa, voi käydä niin, että näitä pienempivaikutteisia häiriöitä ratkaistaessa levyn vaihto kestää liian kauan, joka taas aiheuttaa suuremman häiriötilanteen. Tai mikäli heräteilmoitusten ja asiakkailta tulleiden häiriöilmoitusten palvelunhallintaprosessi on samanlainen, voi iso määrä herätteitä tukkeuttaa asiakkaiden palvelemisen. Asiakkaiden hidas palveleminen taas aiheuttaa asiakastyytymättömyyttä ja huonoa palautetta organisaatiolle. Onkin mielekästä lähteä tavoittelemaan tilannetta, jossa herätteet voitaisiin mahdollisuuksien mukaan kuitata pitkälti automatiikan avulla ja ainoastaan ihmisten toimintaa vaativat ilmoitukset tulisivat palvelunhallintajärjestelmään. Täältä järjestelmästä asiantuntijat poimivat aina relevanteimmat tapaukset kiireellisimmiksi.

Liiketoiminnan näkökulmasta katsottuna herätehallinta ja valvonta voivat tarjota epäsuoraa hyötyä. Vaikka niiden avulla ei voida välttämättä tuoda suoraa rahallista tuloa organisaatiolle, on niistä koituva arvo kuitenkin usein merkittävä. Mikäli tuotanto keskeytyy ennakoimattoman häiriön seurauksena, useiden toistuvien häiriötilanteiden takia asiakastyytyväisyys laskee tai pahimmassa tapauksessa asiakas vaihtaa kilpailijan palveluihin, on hyvin toimiva infrastruktuuri ensiarvoisen tärkeää. Mikäli häiriötilanteisiin ja odottamattomiin tapahtumiin voidaan vaikuttaa ennakoivasti, eli ratkaista häiriönaiheuttajat ennen niiden näkymistä katkoksina tuotannossa tai palveluissa, säästetään näin henkilötyövoimakustannuksia ja resursseja. Myös asiakastyytyväisyys paranee, kun tietoa häiriötilanteista ei tarvitse saada loppukäyttäjiltä.

7 TIETOTURVATIEDON JA TAPAHTUMIEN HALLINTA (SIEM)

SIEM (Security Information and Event Management) -järjestelmän tarkoitus on tuottaa operatiivisen tietoturvan tilannekuvaa, tehostaa lokienhallintaa ja yhdistää sekä raportoida tietoturvatapahtumien seurannasta yhtenäisesti. SIEM yhdistää tapahtumaketjuja, mutta myös lisää tietoturvatietoa esimerkiksi paikka- tai kriittisyystiedoilla. SIEM-järjestelmät osaavat automatisoida eri standardien vaatimat jatkuvat seurannat ja raportoinnit. Järjestelmät osaavat myös tuottaa hälytyksiä erilaisten lokitietojen, IDS-havaintojen ja haavoittuvuuslistauksien perusteella. SIEM-järjestelmiä on markkinoilla hyvin paljon ja ala on jatkuvassa kehityksessä. Omalle organisaatiolle sopivan ja oikean hintaisen tuotteen löytäminen voi olla vaikeaa. Myöskään pelkän järjestelmän ostaminen ei itsessään riitä. Sekä järjestelmä että lokilähteet täytyy määrittää, ja lokienhallintaprosessien tulee olla kunnossa, jotta asetetut vaatimukset täyttyvät ja järjestelmästä saadaan toivottu hyöty. (Nixu 2016. Tietoturvatiedon ja tapahtumien hallinta (SIEM), viitattu 7.11.2016.)

SIM (Security Information Management) kerää lokitietoja eri lähteistä ja luo niistä raportteja. SEM (Security Event Management) suorittaa korrelointia tälle kerätylle datalle ja helpottaa näin tietoturvatapahtumien analysointia. Security Information and Event Management (SIEM) on näiden kahden tuotteen yhdistelmä, jolloin molempien edut saadaan yhdistettyä saman järjestelmän alaisuuteen. Perinteiset lokienhallintatyökalut pelkästään keräävät ja raportoivat kerättyä dataa, eivätkä sisällä analysointi- tai korrelointitoimintoja. (TechRebublic 2011. How to choose a SIEM solution: An overview, viitattu 28.10.2016.)

SIEM ei sellaisenaan ole valmis järjestelmä, joka alkaa välittömästi tuottaa lisäarvoa olemassaololollaan, mullistaa yrityksen tietoturvan, tai muuttaa itsekseen raa'an lokidatan käsiteltäväksi informaatioksi. Organisaation täytyy olla valmis laittamaan resursseja ylläpitoon ja kehitykseen. Valmiit korrelointisäännöt tai tilannenäkymät eivät sellaisenaan välttämättä sovi yritykselle, joten asiantuntijoiden täytyy olla valmiita säätämään ja kehittämään raporttien ja sääntöjen toimintaa sekä tilannekuvien sisältöä. Jos järjestelmä jätetään ”olemaan” vain sellaisenaan, hukataan siitä saatava hyöty hyvin helposti. (TechRebublic 2011. How to choose a SIEM solution: An overview, viitattu 28.10.2016.)

7.1 Tiedon lokitus

Loki tarkoittaa yksinkertaisimmillaan aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tietojärjestelmien, sovellusten ja tietoverkkojen tapahtumia ja muutoksia kirjataan eli lokitetaan. Lokitus puolestaan tarkoittaa kerättyjen lokitietojen hyödyntämistä. Tätä tietoa tarvitaan silloin, kun pyritään selvittämään mitä, miksi tai milloin jotakin on tapahtunut. Näin saadaan selvitettyä häiriötilanteita tai varmistettua, että virheitä ei ole syntynyt esimerkiksi tiedonkäsittelyssä ja että käsitelty tieto on oikeaa. Mikäli lokitietoja ei ole saatavilla, on häiriöiden juurisyytä hyvin hankala, ellei mahdoton selvittää. Mikäli järjestelmiltä vaaditaan tiedon kiistämättömyyttä, luottamuksellisuutta ja eheyttä, tarvitaan monipuolista lokitusta sen varmistamiseksi. Lokitietoja tulee myös säilyttää riittävän pitkään, jotta niihin voidaan tarpeen vaatiessa palata. Tietoturvapoikkeamien tapauksessa lokeja voidaan analysoida reaaliaikaisesti tai jälkeenpäin. (Viestintävirasto 2016. Lokien keräys ja käyttö, 2, viitattu 28.10.2016.)

Ensin on tärkeää määritellä lokienhallintapolitiikka. Mitä ja miten lokitetaan ja ennen kaikkea mitä kerätyllä lokidatalla tehdään. Eräs keskeinen ongelma on tapahtumien valtava määrä, joka johtaa nopeasti tilanteeseen, jossa järjestelmän ylläpitäjät eivät enää kykene tehokkaasti etsimään tietoa lokimassasta. Järjestelmän rakentaminen kannattaa aloittaa kevyesti ja samalla tarkasti määritellä, miksi ja mihin jotakin tietoa tarvitaan tai joku toimenpide tehdään. Seurattavia lokilähteitä kannattaa lisätä asteittain samalla kehittäen omia toimintatapoja. Esimerkiksi palomuurin lokiin voi generoitua valtava määrä tietoa väärin määritellyistä palveluista. Väärin määritelty järjestelmä voi johtaa liian suureen määrään vääriä positiivisia (false positive) havaintoja, jolloin hälytysten lokitulvan takia hälytykset joudutaan kytkemään pois päältä. Jotta järjestelmästä saadaan paras hyöty, kannattaa monitoroitava osa IT-infrastruktuurista määritellä niin, että SIEM-järjestelmän korrelaatiosääntöjä voidaan tehokkaasti hyödyntää. (Viestintävirasto 2016. Lokien keräys ja käyttö, 9, viitattu 28.10.2016.)

Viestintäviraston lokien keräys- ja käyttöohjeessa luetellaan tyypillisimmät erilaiset lokitusmuodot:

Ylläpitoloki	Ylläpidetään tietoa järjestelmän toimintaan ja käyttöoikeuksiin tehdyistä muutoksista ja hallitaan virhetilanteita. Sopii versiohallintaan ja toimintaympäristön seurantaan.
Käyttö- eli tapahtumaloki	Tavallisin ja välttämättömin muoto. Rekisteröi käyttäjien sisään- ja uloskirjautumisia, sekä

	järjestelmien suorittamia prosesseja. Esimerkiksi tulostustapahtuma tai tietosisällön lukeminen tietokannasta kirjataan käyttölokiin.
Muutosloki	Kirjataan merkinnät tietojen lisäyksistä, poistoista ja muutoksista. Tarvittaessa muuttuneen tiedon alkuperä voidaan jäljittää ja varmistaa muutoslokista.
Virheloki	Käytetään ongelmatilanteiden selvittämisessä. Kun virheen syy kirjataan lokiin mahdollisimman tarkasti, on helpompi selvittää sen aiheuttaja.
Viestintäloki	Sisältää tietoja viestinnästä: viestin alkuperä, pääteosoite, ajankohta jne. Esimerkiksi teletunnistetiedot ovat tällaisia.
Haltijaloki	Kertoo kenelle jokin nettiosoite, puhelinnumero tai verkkodomain jne. on kuulunut tiettynä ajan hetkenä.
Pääsynvalvontaloki	Kertoo onnistuneista ja epäonnistuneista sisään- ja uloskirjautumisista. Lokia analysoimalla voidaan raportoida tietoturvapoikkeamista, eli esimerkiksi onko salasanoja yritetty murtaa tai kirjautua vanhentuneilla käyttäjätunnuksilla. Voidaan myös seurata organisaation käyttölupien ajantasaisuutta.

Hyvin toteutettu lokiympäristö on muusta järjestelmästä erillään oleva tietokanta, jonka eheys varmistetaan niin, ettei sitä voi jälkeenpäin muokata. On myös syytä lokittaa erikseen näiden lokitietojen katselu ja käsittely. Hyvä loki sisältää riittävästi tietoa sen mukaiseen käyttötarkoitukseen.

Käyttökelpoisen lokin pitäisi sisältää ainakin seuraavia tietoja:

- **aikaleima,** milloin tapahtuma oli

- **tapahtuma,** mitä tehtiin tai yritettiin tehdä
- **toimija,** kuka tai mikä teki
- **käyttöoikeus,** millä valtuuksilla tai oikeuksilla tapahtuma tehtiin
- **tapahtuman lähde,** mistä tehtiin, mistä muutostieto on peräisin
- **tapahtuman kohde,** mihin tietoon tai järjestelmään toiminta perustui
- **tapahtuman tila,** onistuiko tai epäonnistuiko ja epäonnistumisen syy.

(Viestintävirasto 2016. Lokien keräys ja käyttö, 4, viitattu 28.10.2016.)

7.2 Tiedon normalisointi ja korrelointi

Normalisoinnilla tarkoitetaan eri lähteistä saatavan raakatiedon yhdenmukaistamista, jonka jälkeen tietoa on helpompi analysoida ja käsitellä. Esimerkiksi jos halutaan muodostaa lista eri henkilöistä, jotka kirjautuvat eniten tai useimmin palvelimelle, voitaisiin lokidataa kerätä kirjautumisesta ja ohjata se tietokantaan, johon tallennetaan esimerkiksi aikaleima, lähdeosoite ja kohdeosoite sekä käyttäjänimi. Kun nämä perustiedot ohjataan tietokantaan, jossa jokaiselle tiedolle on oma kenttä, on tämän jälkeen helppo tehdä kerätyn datan avulla erilaisia analysointeja ja vertailuja keskenään. Ongelmana normalisoinnissa on se, että kaikki laitteet tai järjestelmät eivät ole välttämättä keskenään yhteensopivia. Mitä suuremmalta alueelta tapahtumien lähteitä kerätään, sen hankalampi on löytää yhteiset kentät, joista saadaan rakennettua normalisoitua dataa. Esimerkiksi jos halutaan yhdistää palomuurin ja puhelimen käytön tiedot, saattaa tämä vaatia todella paljon erilaisten kenttien muodostamista tietokantaan, jotta yhtenevät tiedot lopulta löydetään. Tämä puolestaan kasvattaa tietokannan kokoa ja vaatii enemmän prosessointitehoa. On myös mahdollista, että eri laitteiden tai järjestelmien päivitysten myötä myös niiden tuottaman datan sisältö muuttuu niin, että aiemmin normalisointia varten säädetty järjestelmä ei enää toimikaan oikein, vaan säätötoimenpiteet täytyy tehdä uudelleen, tai pahimmassa tapauksessa ne eivät ole enää yhteensopivat. (Marty, R. 2007. Event Processing – Normalization, viitattu 28.10.2016.)

Tiedon korreloinnilla tarkoitetaan tiedon keräämistä ja yhdistämistä useista eri lähteistä, jotta niistä voidaan löytää poikkeamia, jotka jäisivät muuten huomaamatta. Tieto voi olla toisistaan erillään olevista lähteistä, mutta liittyä samaan tapahtumaan, jolloin tämä tietomassa yhdistämällä voidaan luoda tapahtumalle konteksti, johon yksittäinen tietolähde ei kykene. (Securosis 2010. Understanding and Selecting a SIEM/LM: Correlation and Alerting, viitattu 28.10.2016.)

Esimerkkinä voidaan ajatella tilannetta, jolloin verkkorikollinen koettaa murtautua yrityksen tietoverkkoon. Ensin hyökkääjä etsii verkkoskannerilla julkisia palvelimia ja löytää web-palvelimen, jolla on useita tiedossa olevia haavoittuvuuksia. Kun hyökkääjä pääsee haavoittuvuutta hyödyntäen sisälle palvelimeen, hän luo itselleen uuden käyttäjätunnuksen ja pääsee näin organisaation sisäverkkoon, jossa voi etsiä lisää kohteita tietomurrolle. Järjestelmän ylläpitäjillä on olemassa kaikki tieto hyökkääjän huomaamiseen, mutta se on hajautettuna eri paikkoihin. Palomuuri huomaa porttiskannauksen, IDS- ja IPS-laitteet havaitsevat haavoittuvuudet ja palvelimella voidaan havaita uusi käyttäjätunnus. Korrelaation tarkoitus on yhdistää kaikki näiden yksittäisten tapahtumien tieto yhteen ja tunnistaa, että palvelimelle on murtauduttu ja että tilanne vaatii välittömiä toimenpiteitä. Tämä on erittäin helppo toteuttaa ajatuksen tasolla, mutta erittäin vaikea hallita käytännössä. Sääntöjen luominen vaatii aikaa ja henkilöiden osaamista, samoin kuin järjestelmän ylläpitäminen ja kehittäminen. Vaikka järjestelmätoimittaja todennäköisesti voi tarjota muutamia perussääntöjä ja asetuksia, vaatii ympäristön ja uusien sääntöjen kehittäminen paljon resursseja, varsinkin kun ympäristö on dynaaminen ja muuttuu jatkuvasti. Myös isot sääntökannat ja tapahtumalähteet lisäävät ympäristön raskautta ja vaativat paljon laskentatehoa. Ympäristön balanssissa pitäminen on jatkuvaa hienosäätöä sääntöjen, tulosten tarkkuuden ja järjestelmän raskauden sekä sen monimutkaisuuden kesken. (Securosis 2010. Understanding and Selecting a SIEM/LM: Correlation and Alerting, viitattu 28.10.2016.)

7.3 Forensiikka

Sanalla forensiikka tarkoitetaan yleisesti rikosteknistä tutkimusta, mutta tietoturvan alueella kyse on sähköisen todistusaineiston keräämisestä oikeudellisia toimenpiteitä varten. Forensiikka tulee yleensä kyseeseen, kun epäillään joko väärinkäytöstä tai tietomurtoa, tai kerätään tietojärjestelmistä sähköistä todistusaineistoa. Lokitettu tieto on tällaisessa tapauksessa ensiarvoisen tärkeää, koska muutoin ei välttämättä ole olemassa minkäänlaista todistusaineistoa tekijää vastaan, tai että rikosta olisi edes ylipäätään tapahtunut. Tiedon avulla voidaan myös sulkea pois aiheettomia epäilyksiä. (Secmeter 2016. Forensiikka, viitattu 28.10.2016.)

8 JULKISET HANKINNAT

Julkisilla hankinnoilla tarkoitetaan tavara-, palvelu- ja rakennusurakkahankintoja, joita julkisen sektorin hankintayksiköt, kuten valtio, kunnat ja kuntayhtymät tekevät julkisilla varoilla oman organisaationsa ulkopuolella. Julkisten hankintojen arvo on Suomessa lähes 30 miljardia euroa vuodessa, ja ne ovat näin ollen kansantalouden kannalta erittäin merkittäviä. Suomen kansallinen hankintasääntely tulee lähes suoraan EU-sääntelystä, joka on melkein yksinomaan menettelysääntelyä, eli siinä määrätään, millaisen menettelyn kautta julkiset hankinnat tulee suorittaa. (Elinkeinoelämän keskusliitto 2016. Julkiset hankinnat, viitattu 24.10.2016.)

Lähdettäessä tekemään hankintoja kunta-alalla, on syytä ottaa huomioon hyvinkin tarkat menettelyt, jotka ohjaavat hankintaprosessia kautta linjan, alun markkinakartoituksesta hankintasopimuksen allekirjoitukseen saakka. Oulun kaupunki onkin määritellyt hankintoja varten ohjeistuksen kaupungin organisaatioiden käyttöön. Yhteiskuntavastuu (ympäristö- ja sosiaaliset näkökohdat sekä elinkeinoelämän elinvoimaisuus) korostuu tuottavan ja taloudellisen toiminnan sekä avoimuuden että syrjimättömyyden rinnalla. Hankintatoimen on oltava läpinäkyvää Oulun kaupungissa ja sen täytyy voida nauttia julkista luottamusta. Kaupungin toimintaan ja sen periaatteisiin täytyy voida luottaa eri yhteyksissä, jotta sen uskottavuus ostajana, luotettavana kumppanina sekä imago merkittävänä toimijana säilyvät. Hankintalainsäädäntöä noudattamalla varmistetaan lainmukainen menettely ja hyvällä hankintaosaamisella päästään haluttuun lopputulokseen. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 7.)

Samaisessa kaupunginhallituksen ohjeistuksessa todetaan myös, että suunnitteluvaihe ja hankinnan valmistelu ratkaisevat sekä hankinnassa onnistumisen että mahdollistavat toimivan sopimussuhteen. Kuntakonserniin kuuluvien hankintayksiköiden sekä Oulun kaupungin täytyy toimia tehokkaasti sopimusten toteutuksen seurannassa, ettei kilpailutusvaiheessa hankintoihin käytetty panostus mene hukkaan. (2013, 7–8.)

8.1 Julkisen hankinnan periaatteet

Julkisyhteisöjen (valtio, kunnat, kuntayhtymät, valtion ja kunnan omistamat osakeyhtiöt jne.) tulee lain mukaan (Laki julkisista hankinnoista, 2007/348) julkisesti kilpailuttaa hankintansa, joiden arvo ylittää hankintalaissa määritellyt kynnysarvot, jotka tarkistetaan vuosittain. Hankintaa suorittavaa

julkisyhteisöä kutsutaan hankintayksiköksi ja puolestaan hankintayksikköä, joka tekee hankintoja muiden puolesta, kutsutaan yhteishankintayksiköksi. Mikäli hankinnan arvo ylittää kansallisen kynnysarvon, sovelletaan hankintalakia, tai mikäli arvo ylittää EU-kynnysarvon, on hankinta tehtävä EU:n laajuisena. Hankintalakia ei sovelleta silloin, jos hankinnan arvo jää alle kynnysarvon. Kilpailuttamisvelvoite on vahva, mutta hankintalaki ei kuitenkaan määrää, mitä tai millaisin ehdoin hankintaa ja sopimuskautta täytyy valmistella. Se säätää vain ja ainoastaan, miten kilpailutusprosessi tehdään. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 15.)

KANSALLISET KYNNYSARVOT (HANKINTALAIN 15 §)

Hankintalaji	Kynnysarvo (euroa)
Tavara- ja palveluhankinnat	30 000
Käyttöoikeussopimukset	30 000
Liitteen B (ryhmä 25) terveydenhoito- ja sosiaalipalvelut ja koulutuspalvelut yhteishankintana	100 000
Rakennusurakat	150 000
Käyttöoikeusurakat	150 000
Suunnittelukilpailut	30 000

EU-KYNNYSARVOT (HANKINTALAIN 16 §)

Hankintalaji	Kynnysarvo (euroa)	
	Valtion keskushallintoviranomainen	Muut hankintaviranomaiset
Tavarahankinnat ja palveluhankinnat	135 000	209 000
Rakennusurakat	5 225 000	5 225 000
Käyttöoikeusurakat	5 225 000	5 225 000
Suunnittelukilpailut	135 000	209 000

Ohjeellinen lista valtion keskushallintoviranomaisista

KUVA 2. Kansalliset ja EU-kynnysarvot (HILMA. 2016a. Kynnysarvot, viitattu 24.10.2016).

Hankintalain mukaan julkiset hankinnat tulee toteuttaa avoimesti ja toimittajia syrjimättömästi. Se tarkoittaa, että tarjoajia on kohdeltava samalla tavalla ja tasapuolisesti riippumatta sellaisista tekijöistä, jotka eivät liity hankinnan toteuttamiseen, esimerkiksi paikallisuuden suosiminen. Niin ikään avoimuudella tarkoitetaan, että hankintamenettelyä koskevia tietoja ei salata ja hankintaa koskevat asiakirjat ovat lähtökohtaisesti julkisia. On kuitenkin mahdollista, että toimittajat haluavat liikesalaisuuteen vedoten salata omaa teknologiaansa tai organisaationsa tietoja muilta toimittajilta. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 4.)

8.2 Julkiset hankinnat Oulun Tietotekniikassa

Oulun Tietotekniikan tekemiä julkisia hankintoja ohjaavat Oulun kaupungin hankintasäännöt ja -ohjeet. Kun uutta hankintaa suunnitellaan, tulee ensin tutkia voiko hankintayksikkö hyödyntää jotain jo olemassa olevaa puitesopimusta hankinnan toteuttamiseen. Joissakin tapauksissa voi olla järkevää hyödyntää myös KL-Kuntahankintojen kuntatoimijoille valmiiksi kilpailuttamia puitesopimuksia. Laskemalla hankinnan ennakoitu arvo, voidaan määritellä oikea menettelytapa, jolla hankinta suoritetaan. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 5.)

8.3 Ennakkoilmoitus ja markkinakartoitus

Ennen varsinaista kilpailutuksen aloittamista ja tarjouspyynnön julkaisua on monesti tarpeen kartoittaa markkinoita, jotta saadaan riittävästi perustietoa kohteena olevan hankinnan toimijoista, hintatasosta ja erilaisista ratkaisuvaihtoehdoista. Hankintayksiköllä on vapaus kartoittaa markkinoita, tehdä markkina-analyysiä sekä käydä teknistä vuoropuhelua mistä tahansa hankintaan liittyvästä seikasta, kunhan se tehdään läpinäkyvästi ja suosimatta yksittäistä toimijaa. Markkinakartoitusta voidaan tehdä julkaisemalla tietopyyntö tai ennakkoilmoitus hankintayksikön sähköisessä hankintajärjestelmässä. Ennakkokyselyllä voidaan kartoittaa yleisellä tasolla hankintaan liittyviä tekijöitä. Tämä ns. tekninen vuoropuhelu on turvallisinta toteuttaa kirjallisena. Tietopyynnöllä puolestaan pyritään kartoittamaan markkinoilla toimivia yrityksiä ja heidän ratkaisuvaihtoehtojaan sekä yleistä hintatasoa. Tietopyynnössä tulee ilmaista yksiselitteisesti, että kyseessä on tietopyyntö, eikä se (tietopyyntö) ole osa hankintamenettelyä. Sitä ei saa myöskään kohdentaa vain muutamalla yritykselle, tai muodostaa tarjouspyynnön kaltaiseksi. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 25.)

8.4 Hankintamenettelyt

Hankintaa voidaan lähteä tekemään erilaisilla tavoilla, joiden soveltuvuus kuhunkin hankintaan tulee arvioida tapauskohtaisesti. OTT:laisen hankintaoppaassa (2016, 9–10) kuvataan eri neuvottelumenettelyjä seuraavasti:

- Avoimessa hankintamenettelyssä kuka tahansa kelpoisuusehdot täyttävä toimittaja voi jättää hankintayksikön julkaisemaan tarjouspyyntöön sen pakolliset vaatimukset täyttävän

tarjouksen, jossa tarjottu ratkaisu esitellään ja laatuun vaikuttavat asiat on kuvattu hintatiedoista erillään.

- Rajoitettu hankintamenettely on kaksivaiheinen, joista ensimmäinen on osallistumisvaihe ja sitä seuraa tarjouspyyntövaihe. Ensimmäisessä vaiheessa toimittajia pyydetään ilmoittamaan halukkuudestaan osallistua tulevaan hankintaan. Hakemusten perusteella hankintayksikkö valitsee vähintään viisi kelpoisuusehdot täyttävää toimittajaa, joille varsinainen tarjouspyyntö lähetetään. Toimittajien valinta on perusteltava.

- Neuvottelumenettelyssä toimittajia pyydetään ilmoittamaan halukkuudestaan osallistua käsillä olevaan hankintaan. Tässä menettelymallissa ehdokkaita on kutsuttava neuvottelumenettelyyn vähintään kolme. On hyvä ottaa huomioon, että neuvottelumenettelyn käyttö edellyttää aina hankintalaissa olevaa perustetta sen käytölle ja hankinnan arvon tulee jäädä alle 50 000 euron tavara- ja palveluhankinnoissa.

- Kilpailullisessa neuvottelumenettelyssä toimittajia pyydetään ilmoittamaan halukkuudestaan osallistua tulevaan hankintaan. Myös tässä menettelytavassa ehdokkaita on kutsuttava mukaan vähintään kolme. Hankintayksikkö neuvottelee valittujen kelpoisuusehdot täyttäneiden toimittajien kanssa löytääkseen yhden tai useamman ratkaisun joka vastaa sen tarpeita, jonka perusteella toimittajia pyydetään tekemään tarjous. Neuvottelujen edetessä tarjouspyynnön sisältövaatimuksia voidaan muokata ja niihin voidaan pyytää toimittajien kannanottoja. Lopuksi valmis tarjouspyyntö julkaistaan neuvottelumenettelyyn valituille toimittajille ja he vastaavat jättämällä kirjallisen tarjouksen kuten avoimessa menettelyssä. Haasteena tässä menettelytavassa on toimittajien tasapuolinen ja syrjimätön kohtelu, minkä vuoksi neuvottelut kannattaa toteuttaa kirjallisena. Huomioitavaa on, että puitejärjestelyä ei voi hankkia kilpailullisella neuvottelumenettelyllä.

- Suorahankinnassa hankintayksikkö voi poiketa kilpailuttamisvelvoitteestaan. Sen käynnistäminen on todella harvinainen poikkeus ja sitä voidaan käyttää vain hyvin rajallisesti hankintalaissa määriteltyjen edellytysten täyttyessä, esimerkiksi jos avoimessa menettelyssä ei ole saatu lainkaan tarjouksia, tai hankinnalla on äärimmäinen kiire.

- Sähköisessä huutokaupassa halvimman hinnan tarjoaja voittaa kaupan. Huutokauppa on kaikille kelpoisuusehdot täyttäville toimittajille avoin ja kaikki näkevät voittavan tarjouksen. Huutokaupassa kohteelle voidaan määritellä pakolliset vaatimukset ja laatukriteerit, joiden tulee täyttyä. Tätä menettelyä käytetään yleensä helposti määritettävissä tuotteissa, kuten kopiopaperit, toimistotarvikkeet jne.

8.5 Tarjouspyyntö

Tarjouspyyntö on hankintaa koskevan kilpailutuksen tärkein vaihe, johon täytyy varata riittävästi aikaa. Yleinen virhe on laatia tarjouspyyntö liian hätäisesti, jolloin siinä ei ole otettu huomioon kaikkia sopimusehtoja. Koska hankintayksikkö on sidottu tarjouspyyntöön, rasittavat huonot ehdot hankintaa sen loppuun asti. Mikäli joku olennainen ehto puuttuu, tai sellainen on määritelty hankintayksikön kannalta epäedullisesti, on ainoa vaihtoehto hankinnan keskeyttäminen. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 51.)

Toimittajat tekevät tarjouksensa tarjouspyynnön vaatimusten perusteella, joten sen tulee olla mahdollisimman yksiselitteinen ja selkeä vertailukelpoisten tarjousten saamiseksi. Kun käytetään sähköistä hankintajärjestelmää, tulee hankinnan kohteen kuvauksesta helposti sekavan oloinen. Tämän vuoksi kannattaa liittää tarjouspyyntöön erilliset dokumentit, joissa hankintaan liittyvät sopimusehdot, vaadittu laatutaso ja palvelun tai ratkaisun sisältövaatimukset ovat tarkemmin kuvattuina. On myös mahdollista määritellä tarjouspyyntöön vain haluttu lopputulos, jolloin tekninen toteutus jää toimittajien mietittäväksi. Tällaisissa tapauksissa vaatimusmäärittelyssä kuvataan vain halutut käyttötapaukset ja tarvittavat rajapinnat. Hankintayksikkö voi myös vaatia yhteensopivuutta jo olemassa olevaan ratkaisuun tai ICT-käyttöympäristöön. Lisäksi tarjouspyynnössä on hyvä varata mahdollisuus keskeyttää hankinta. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 14.)

8.6 Toimittajien soveltuvuuden vaatimukset

Hankinnassa mukana olevien tarjoajien soveltuvuutta hankinnan toteuttamiseen selvitetään esittämällä hankintailmoituksessa toimittajien rekisteröitymistä, rahoituksellista ja taloudellista tilannetta, teknistä suorituskykyä ja ammatillista pätevyyttä sekä laatua koskevia vaatimuksia.

Näiden vaatimusten ja selvitysten tulee liittyä toimittajan edellytyksiin toteuttaa hankinta. Mikäli toimittaja ei täytä hankintayksikön asettamia vähimmäisvaatimuksia, on ehdokas suljettava pois tarjouskilpailusta. Tarvittaessa hankintayksikkö voi pyytää tarjoajia täydentämään tai täsmentämään selvityksiä ja muita asiakirjoja. Toimittajasta tulee myös tehdä tilaajavastuulain mukainen selvitys, tällä pyritään torjumaan ns. harmaita markkinoita. Tarjoaja voidaan sulkea pois kilpailusta tilaajavastuulaissa mainituin perustein, eli jos on syytä epäillä väärinkäytöksiä tai puutteita toimintaselvityksissä. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 53–55.)

8.7 Tarjousten valinta- ja vertailuperusteet

Hankintailmoituksessa on käytävä ilmi, millä perusteilla tarjousten valinta tullaan tekemään. Valintaperusteita ovat halvin hinta tai kokonaistaloudellinen edullisuus. Mikäli on valittu kokonaistaloudellinen edullisuus, on hankintayksikön ilmoitettava, millä perusteilla kokonaistaloudellista edullisuutta verrataan. Mikäli valintaperusteita tai kokonaistaloudellisen edullisuuden vertailuperustetta ei ole mainittu, valinta tehdään halvimman hinnan perusteella. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 70.)

Hankintayksikön täytyy miettiä ennen tarjouspyynnön julkaisua, millä perusteella tarjoukset tullaan vertailemaan keskenään. Vertausperusteiden tulee käydä ilmi tarjouspyynnössä ja hankintayksikön täytyy kuvata haluttu tavara tai palvelun sisältö mahdollisimman tarkasti sekä esittää siihen liittyvät pakolliset vaatimukset ja ilmoittaa, mistä asioista tarjousvertailussa toimittajat saavat laatupisteitä. Yleensä laadullisia asioita kannattaa vaatia pakollisina vaatimuksina, jolloin toimittajia ohjataan tarjoamaan määritellyn minimilaatutason ylittäviä ratkaisuja. Vertailussa voidaan käyttää ainoastaan niitä perusteita, joita tarjouspyynnössä on ilmoitettu ja niin ikään vertailussa huomioidaan vain ne tiedot, joita toimittaja tarjouksessaan esittää. Myös kaikkia tarjouspyynnössä ilmoitettuja vertailuperusteita tulee käyttää tarjouksia vertailtaessa. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 13.)

Tarjousten käsittelyssä on toteuduttava julkisten hankintojen vaatimus toimittajien tasapuolisesta ja syrjimättömästä kohtelusta ja hankintayksilöllä on velvollisuus hylätä tarjoukset, jotka eivät vastaa tarjouspyyntöä. Kun tarjoajien kelpoisuus on todettu, voidaan siirtyä tarjousten laadulliseen vertailtuun, jonka on puolestaan tapahduttava ennen hintavertailua. Tällä estetään hinnan vaikutus tarjousten laadulliseen arviointiin. Mikäli ei voida olla varmoja tarjoajien

tarjouksissa esittämistä lupauksista, voidaan järjestää tarjousvertailun voittaneen toimittajan ja sen ratkaisun auditointi ennen lopullista hankintapäätöstä. Tällöin tarjottua ratkaisua verrataan tarjouspyynnön vaatimuksiin. Auditointivaatimus tulee kirjata osaksi tarjouksen vaatimusmäärittelyä. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 22–23.)

8.8 Hankintapäätöksen tekeminen

Hankintamenettelyn päättävästä ratkaisusta täytyy aina tehdä kirjallinen hankintapäätös, joka on perusteltava, pelkkä tarjousten pisteytys ei ole riittävä perustelu hankintapäätöksen tekemiselle. Ennen päätöksen tekoa on varmistettava, että kaikki tarvittavat selvitykset on tehty ja hankinnassa vaaditut ominaisuudet on tarvittaessa auditoitu. Tämän jälkeen hankinnasta voidaan laatia kirjallinen esitys hankintapäätökseksi, joka esitellään hyväksyttäväksi henkilölle tai toimielimelle, jolla on asiaan riittävä päätösvalta. Vastuu tehdystä hankintapäätöksestä on päätöksentekijällä ja esittelijä puolestaan vastaa siitä, mitä hänen esittelystään on päätetty. Merkityksellisistä hankinnan vaiheista, joilla on vaikutusta ehdokkaiden ja tarjoajien asemaan, on tehtävä kirjallinen päätös, joka on myös perusteltava. Markkinaoikeudessa olleet hankintapäätökseen liittyvät virheet ovat selkeästi johtuneet siitä, ettei tarjousten saamia pistemääriä olla sanallisesti perusteltu. (Kaupunginhallitus 2013. Oulun kaupungin hankintakäsikirja, 82.)

Oulun kaupungin hankintakäsikirjassa kerrotaan myös, että puitesopimukseen perustuvassa tilauksessa hankintapäätöstä ei edellytetä, mikäli hankinnan ehdot on sitovasti vahvistettu jo puitejärjestelyä perustettaessa, eli käytännössä puitesopimusta solmittaessa. Hankintapäätöstä ei myöskään tarvitse tehdä, kun hankintayksikkö tekee uuden hankinnan alkuperäisen toimittajan kanssa lisätilauksena, tai uutena hankkeena, joka vastaa aiempaa hankintaa. (2013, 82.)

8.9 Hankintasopimus

Kun muutoksenhakuaika on päättynyt ja hankintapäätös tulee lainvoimaiseksi, hankintayksikön tulee laatia hankintasopimus. Hankintasopimuksen voi laatia automaattisesti tarjouspyynnön pohjalta hyödyntämällä sähköistä hankintajärjestelmää, mutta on suositeltavampaa laatia erillinen hankintayksikön oman mallin mukainen hankintasopimus. Mikäli hankinta on EU-laajuinen,

edellytetään siltä myös jälki-ilmoituksen tekemistä, jossa kerrotaan, kuka tuli valituksi ja mikä on sopimuksen kesto sekä arvo. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 25.)

Sopimusehdot, joita hankintoihin käytetään, tulee valita tapauskohtaisesti. Yleisiä kaikkiin hankintoihin sopivia ehtoja ei ole olemassa. Käytettäessä julkisen hallinnon sopimusehtoja kuten JIT2015 tai JYSE on syytä huomata, että ne eivät sellaisenaan välttämättä käy kaikkiin hankintoihin. Tällöin voidaan poiketa yleisistä ehdoista. Mikäli yleisistä ehdoista poiketaan, tulee hankintasopimuksessa tai sen liitteessä todeta, miltä osin yleisistä ehdoista poiketaan. On erityisesti syytä huomata, että niin kutsutut ankarat ja yllättävät ehdot eivät sido vastapuolta, ellei niitä ole erityisesti korostettu vastapuolelle. Sopimuksenlaatijalla on tällöin tässä asiassa todistustaakka. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 26.)

Hankintapäätös on lainvoimainen vasta, kun siihen liittyvä muutoksenhakuaika on kulunut loppuun. Sähköisen ilmoitusmenettelyn tapauksessa muutoksenhakuaika on 14 päivää. Mikäli tarjouskilpailun hävinnyt toimittaja on eri mieltä hankintayksikön tekemästä hankintapäätöksestä, voi toimittaja perusteltujen syiden avulla esittää hankintayksikölle vapaehtoista hankintaoikaisua tai vaihtoehtoisesti päätöksestä voi valittaa markkinaoikeuteen, mikäli hankinnan arvo ylittää kansallisen kynnysarvon. Hankintayksikkö voi omasta aloitteestaan tai hankintaoikaisuvaatimuksen saatuaan ratkaista asian uudelleen 60 päivän kuluessa hankintapäätöksen tiedoksisaannista, mikäli aiempi päätös perustuu hankintalain soveltamisessa tapahtuneeseen virheeseen. Tällöin hankintayksikön tulee ilmoittaa hankintaoikaisun vireille tulosta hankintaan osallistuneille tarjoajille. EU-laajuisissa hankinnoissa toimittajan tekemä markkinaoikeusvalitus johtaa hankinnan automaattiseen täytäntöönpanokieltoon. Tällöin hankintasopimusta ei voi allekirjoittaa tarjouspyynnön mukaisessa laajuudessa. Mikäli hankintaa ei voi lykätä, hankintayksikkö voi järjestää hankinnan väliaikaisin käytännöin muutoksenhaun ajaksi laatimalla tarjouskilpailun voittaneen tai aiemman toimittajan kanssa toistaiseksi voimassaolevan sopimuksen, jonka voimassaolo raukeaa, kun markkinaoikeus on tehnyt valitusasiasta päätöksen ja hankinta on lopulta saanut lainvoiman. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 29–30.)

8.10 Uudistuva kansallinen hankintalainsäädäntö

Työ- ja elinkeinoministeriön internetsivuilla todetaan, että Suomen julkisia hankintoja koskevaa lainsäädäntöä uudistetaan parhaillaan. Tavoitteena tällä on muun muassa yksinkertaistaa

hankintamenettelyä ja ottaa hankinnoissa paremmin huomioon työllisyyteen, terveyteen ja sosiaalisiin näkökohtiin liittyviä tekijöitä. Lisäksi pyritään parantamaan PK-yritysten osallistumista, luodaan hankinnoille valvontamekanismi ja tarkastellaan kansallisia kynnysarvoja tarkemmin. Taustalla ovat huhtikuussa 2014 annetut EU:n julkisia hankintoja koskevat direktiivit, jotka uudistavat lähes kokonaan nykyisen hankintoja koskevan EU-sääntelyn. (Työ- ja elinkeinoministeriö 2016a. Hankintalainsäädännön kokonaisuudistus, viitattu 25.10.2016.)

EU-jäsenmaiden tuli saada lainsäädäntönsä uusien direktiivien mukaisiksi 18.4.2016 mennessä, mutta näin ei ole tapahtunut. Uusi ennuste direktiivien voimaantulolle on vuoden 2017 alku. Hankintayksiköiden tulee kuitenkin soveltaa 18.4.2016 jälkeen osittain nykyistä voimassa olevaa lainsäädäntöä, sekä sen lisäksi uusia hankintadirektiivejä niiltä osin, kun direktiivit luovat välittömiä oikeusvaikutuksia. Käytännössä siis siirtymävaiheen aikana noudatetaan nykyisiä kansallisia kynnysarvoja ja määräyksiä, mutta mikäli uudet direktiivit ja määräykset on julkaistu, tulee hankintayksikön noudattaa niitä. (PTCServices 2016. Hankintadirektiivien uudistus, viitattu 25.10.2016.)

Välittömän oikeusvaikutuksen piirissä ovat kuitenkin vain ne määräykset listatuista lainkohdista, joissa on asetettu ehdoton velvoite hankintayksikölle tai hankintaviranomaiselle, tai vastaava oikeus tarjoajalle tai ehdokkaalle. (Työ- ja elinkeinoministeriö 2016b. Hankintalain kokonaisuudistus – Siirtymävaiheen toimenpiteet ja järjestelyt, viitattu 25.10.2016.)

9 NYKYTILAN ANALYYSI

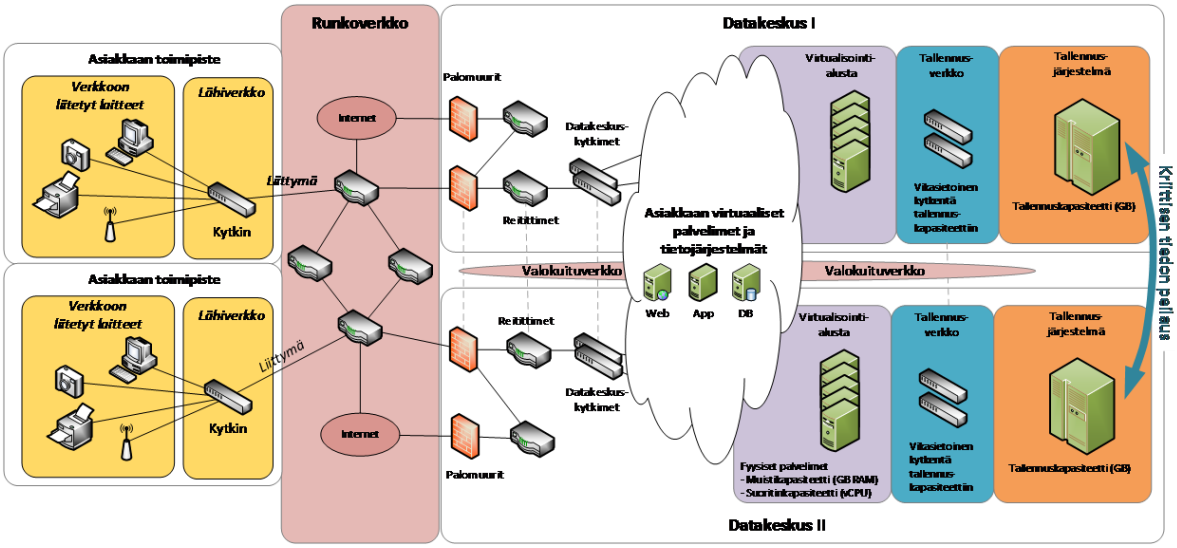
Nykytilan analyysillä kartoitetaan tämän hetkinen toimintaympäristö, johon kuuluvat tekniset järjestelmät ja erilaiset palvelut, joita teknisen alustan avulla tuotetaan. Näin saadaan selkeä kuva lähtökohdasta sekä ymmärys siitä millaisia valvontatarpeita ja kyberturvallisuuteen liittyviä vaatimuksia ympäristö hankittavalle ratkaisulle asettaa.

9.1 Toimintaympäristö

Oulu on Suomen viidenneksi suurin kaupunki, jonka asukasluku on noin 194 000. Oulu ”pohjoisen Skandinavian pääkaupunkina” on keskeinen palveluiden ja logistiikan solmupiste, sekä yksi Suomen johtavista ICT-osaamiskeskittymistä.

Oulun Tietotekniikka liikelaitos (myöhemmin OTT) tuottaa Oulun kaupungin konserniin kuuluvana kunnallisena liikelaitoksena laadukkaita tietoteknisiä palveluita. OTT toimii kaupungin sekä sen organisaatioiden strategisiin ydinprosesseihin liittyvien tietojärjestelmien keskitettynä palveluintegraattorina ja kumppanina mahdollistaen asiakkaiden oman toiminnan kehittämisen ja tehostamisen tietotekniikan avulla. Edellisten lisäksi OTT vastaa kaupungin kriittisen tietojärjestelmäinfrastruktuurin tuotannosta, asiakastuesta sekä tietoteknisten päätelaitteiden, järjestelmien ja sovellusten elinkaaren mukaisista hankinnoista ja palveluista.

IT-infrastruktuurin ydin koostuu kahdesta datakeskuksesta, joiden kautta tuotetaan IT-palvelut sekä hallinnon että opetuksen käyttöön. OTT:n ylläpitämät ja valvomat datakeskukset ovat kaupungin tietoliikenteen solmukohtia. Datakeskuksen palvelut on rakennettu vikasietoisiksi ja maantieteellisesti hajautetuiksi. Tällä tavoin on mahdollista suojata kriittiset tietojärjestelmät katastrofeilta. Katastrofisuojauksella tarkoitetaan palvelun kahdentamista kahteen eri datakeskustilaan siten, että palvelu voi toipua esimerkiksi datakeskustilan tuhoutumisesta verrattain lyhyessä ajassa. (Oulun Tietotekniikka 2016a. Palveluluettelo, 43.)



KUVA 3. Datakeskuspalvelun katastrofisuojauksen rakenne ja komponentit. (Oulun Tietotekniikka 2016a. Palveluluettelo.)

OTT ylläpitää noin 450 palvelinta, joista suurin osa on x86/x64 arkkitehtuurin Microsoft Windows Server -käyttöjärjestelmällä varustettuja. Loput palvelimista ovat Linux-käyttöjärjestelmällä toimivia tai Unix-variantteja. Pääosa palvelimista on virtuaalisia, vuonna 2015 virtualisointiaste oli 92 %.

Asiakkailla on mahdollisuus tilata käyttöönsä virtuaalinen työasema (virtuaalityöpöytä), joka toimii OTT:n pilvipalveluiden kautta. Virtuaalityöpöytä mahdollistaa tietoturvallisesti kaikkien OTT:n tuottamien palveluiden käyttämisen siellä, missä on internetyhteysmahdollisuus. Työpöydälle kirjaudutaan joko nettisivun tai erillisen asiakasohjelman avulla.

OTT:n tarjoamaan tallennuskapasiteettiin liittyy aina varmistuspalvelu. Tällöin asiakkaan tieto kopioidaan päivittäin erilliselle tallennusmedialle ja varsinaisesta datasta erilliseen datakeskustilaan, josta tieto voidaan tarvittaessa palauttaa. Tallennusjärjestelmän kriittinen tieto voidaan yhtäaikaisesti kopioida toisessa datakeskustilassa sijaitsevaan tallennusjärjestelmään. Tällöin datasta on olemassa kaksi identtistä kopiota maantieteellisesti kahdessa eri paikassa sekä lisäksi varmistusjärjestelmässä oleva kolmas kopio. Kaikista palvelimista ajetaan varmuuskopio päivittäin. Varmuuskopio mahdollistaa palvelun ja tietojen palautumisen erilaisissa häiriötilanteissa. Lisäksi virtuaalipalvelimista on mahdollista ottaa ns. ”snapshotteja” eli eräänlaisia pikakopioita esimerkiksi päivitystapahtumien yhteydessä, jolloin nopea palautuminen toimivaan tilaan on helppoa ja käytännöllistä.

Palvelinten toimintatilaa valvotaan jatkuvasti muutaman eri valmistajan valvontatuotteilla. Kriittisten palvelinten hälytykset ohjataan 24/7 päivystäjän matkapuhelimeen. Osalle palvelimista on myös määritelty erilaisia palvelinkohtaisia hälytyksiä. Palvelimen valvontaan voidaan asiakkaan pyynnöstä määritellä myös oletuksena valvottavien kohteiden ulkopuolisia asiakaskohtaisia asioita, kuten lokimerkintöjen valvontaa tai esimerkiksi palvelun saatavuuden valvontaa. On myös mahdollista määritellä automatisoidusti suoritettavia toimenpiteitä havaitun häiriötilanteen korjaamiseksi.

Osa palvelimista voidaan luokitella toimintojen kannalta kriittiseksi, jolloin niihin kuuluu automaattisesti Valvomo24-palvelu. Myös asiakkaat voivat tilata Valvomo24-palvelun palvelimilleen niin halutessaan. Tällä hetkellä tätä palvelua toimitetaan yhteensä 111 palvelimelle. Valvomo24-palveluun sisältyy automaattinen ympärivuorokautinen palvelinjärjestelmän valvonta, joka kattaa laitteet, käyttöjärjestelmän, tietokannat sekä verkkoyhteydet ja datakeskuksen käyttöympäristön. Kriittisimmistä häiriötilanteista lähetetään automaattisesti viesti päivystäjän puhelimeen, jotta korjaustyöt voidaan aloittaa välittömästi. Osa vähemmän kiireellisistä ilmoituksista menee myös päivystäjien yhteiseen postilaatikkoon.

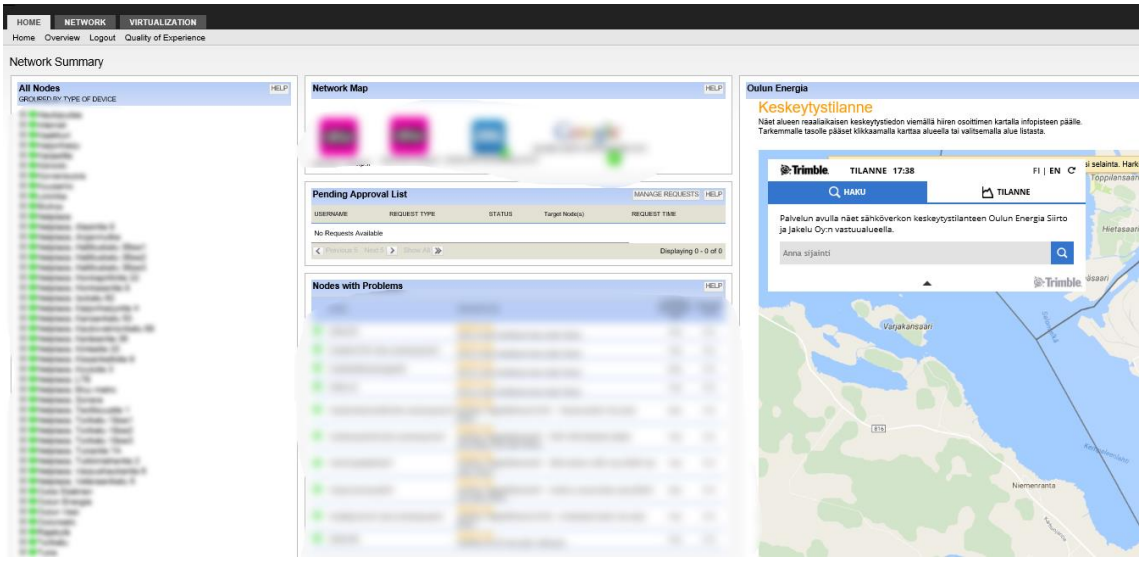
Keskitetyn ja tietoturvallisen tulostustyönkulkujen hallinnan eli turvatulostuksen avulla loppukäyttäjä voi vapauttaa tulostustyönsä miltä tahansa kaupungin tulostusjärjestelmältä ja säilyttää silti dokumenttien luottamuksellisuuden. Käyttäjä voi henkilötodennuksen jälkeen tulostaa kaikki työt kerralla tai valita vapautettavat työt. Turvatulostuspalvelut tulevat palveluna kolmannelta osapuolelta. Turvatulostuspalvelun lisäksi käytössä on edelleen perinteisiä ns. suoria tulostusjonoja, jolloin käyttäjä tulostaa työnsä suoraan valitsemalleen tulostimelle.

Käyttäjälle voi tulla tarve päästä Oulun Tietotekniikan tarjoamiin palveluihin esimerkiksi kotoa tai työmatkan aikana. Virtuaalityöpöydän lisäksi etäkäyttöratkaisuja tarjotaan kuormanjakolaitteiston kautta, jonka toimittaa palveluna kumppaniyritys. Tällöin asiakas voi henkilökohtaisen salasanan ja pääsyoikeuden omatessaan käynnistää tarvitsemiaan sovelluksia internetistä käsin. Tällaisia ovat esimerkiksi sähköposti, kaupungin intranetsivusto tai henkilöstöhallinnon itsepalvelu.

9.2 Valvonta

Tällä hetkellä organisaatiolla ei ole olemassa yhtenäistä valvontaratkaisua, vaan kokonaiskuvaa muodostetaan useiden erilaisten informaatiolähteiden perusteella. Vaikka useissa IT-

infrastruktuurin ylläpitoon liittyvissä palveluissa on toimittaja- tai valmistajakohtaisia valvontaratkaisuja ja mahdollisuus tehdä järjestelmäkohtainen valvontanäkymä, ei tätä ole yleensä hyödynnetty riittävästi. Tarvittavat määrittelyt on tehty hyvin pintapuolisesti tai ei ollenkaan, jolloin näkymän käyttöarvo on merkityksetön. Yksittäisistä näkymistä hyödynnetään tällä hetkellä eniten valvontatyökalua, jolla tarkkaillaan tietoliikenneyhteyksien ja tietoliikennelaitteiden statusta. Virtuaalialustan valvontaratkaisulla seurataan virtuaaliympäristön toiminnallisuutta. Sen kautta nähdään esimerkiksi palvelinten saatavuus ja riskianalyysi. Näkymään voidaan myös tuoda yksittäisiä palvelinten hälytyksiä, kuten levytilan, muistin tai prosessoritehon suorituskykyilmoituksia. Lisäksi jonkin verran on myös muita järjestelmäkohtaisia valvontanäkymiä, mutta koska niitä ei saada helposti tuotua yhteen yhteiseen näkymään, on niiden hyödyntäminen enemmän asiantuntijakohtaista.



KUVA 4. Näkymä tietoliikenneyhteyksien ja tietoliikennelaitteiden tilasta.

Käytössä olevia järjestelmäkohtaisia valvontanäkymiä on muun muassa seuraaville palveluille:

- tietoliikenne ja tietoliikennelaitteiden seuranta
- levyjärjestelmä ja palvelinten varmuuskopiointi
- tallennusverkon seuranta
- datakeskuksen LVIS-toiminnot
- datakeskuksen virransyöttö
- nimipalvelut ja IP-osoitteiden hallinta
- fyysisten palvelinten valvonta
- turvatulostuspalvelun seuranta
- haittaohjelmien torjunta, työasemakohtainen virusturva

- palomuurin valvontanäkymät
- etäkäyttöratkaisut
- sähköpostijärjestelmä.

9.3 Herätteet ja häiriöt

Valvontanäkymien lisäksi herätteitä tulee eri lähteistä yhteiskäyttöiseen sähköpostilaatikkoon, joka on päivystäjien ja IT-infrastruktuurista vastaavien asiantuntijoiden käytössä. Kriittisistä palveluista on määritetty herätteet tekstiviestillä päivystäjän aina mukana pitämään puhelimeen, jotta reaktioaika olisi mahdollisimman lyhyt ja tieto häiriötilanteista saavuttaisi asiantuntijan mahdollisimman nopeasti. Palvelinten valvontatyökalusta on ohjelmoitu palvelinkohtaisia hälytyksiä, joista muodostuu suoraan palvelupyyntö Oulun Tietotekniikan palvelunohjausjärjestelmään. Näihin automaattisesti generoituihin ilmoituksiin reagoidaan arkisin klo 8.00 – 16.00, joten ne eivät ole välitöntä huomiota vaativia tapahtumia. Ne on kuitenkin syytä ottaa käsittelyyn mahdollisimman nopeasti, koska esimerkiksi levytilan loppuminen kriittisesti tärkeässä palvelimessa voi aiheuttaa laajavaikutteisemman häiriötilanteen. Vuonna 2016 lokakuun loppuun mennessä tällaisia automaattiherätteitä on tullut palvelunohjausjärjestelmään yhteensä 1569 kappaletta, joista osa on kuitenkin samasta tapahtumasta useaan kertaan tulleita ilmoituksia. Suurin osa on määritetty Windows-palvelimille, mutta esimerkiksi ilmoitukset levytilan loppumisesta tulevat myös Linux-palvelimilta.

Herätteitä tulee palvelunhallintajärjestelmään seuraavista tapahtumista:

- Alert: database backup failed to complete resolution state: new/closed
- Alert: windows service stopped
- Alert: log backup failed to complete
- Server Alert: database backup failed
- Alert: logical disk free space is low
- Alert: % free space is too low
- Alert: networker service monitor
- Alert: an sql job failed to complete successfully
- Alert: IS package failed
- Alert: HP windows (snmp) nic teaming failed

Mikäli häiriötilanne vaikuttaa palveluiden saatavuuteen ja näkyy välittömänä palvelukatkoksena loppukäyttäjille, aloitetaan välittömästi häiriön havaitsemisen jälkeen tilannetiedotus ja korjaustoimenpiteet. Pienempivaikutteisissa häiriötilanteissa tiedotus laitetaan ainoastaan kaupungin sisäisille nettisivuille ja mikäli mahdollista, suoraan häiriöstä kärsivälle asiakkaalle. Mikäli häiriötilanne on laajavaikutteinen ns. kriittinen häiriötilanne, perustetaan sitä ratkaisemaan oma ryhmä, joka alkaa välittömästi korjaamaan häiriötä. Tällaisissa tapauksissa myös tiedotus on laajempaa ja häiriöviesti lähtee sisäisten nettisivujen lisäksi myös tekstiviestillä ja sähköpostitiedotuksena ennalta sovituille asiakkaiden kontaktihenkilöille. Kun häiriötilanteet saadaan ratkaistua ja korjaukset tehtyä, tiedotetaan jälleen asiakkaita ja loppukäyttäjiä samoilla kanavilla. Vuonna 2015 häiriötilanteita oli 15 kappaletta ja kriittisiä häiriötilanteita 19 kappaletta. Lokakuun loppuun mennessä vuonna 2016 häiriötilanteita on ollut 7 kappaletta ja kriittisiä häiriötilanteita 4 kappaletta. Esiintyneiden häiriöiden lukumäärän suurta eroa selittää osaltaan se, että vuonna 2015 tehtiin suuri tietoliikenneoperaattorin vaihtoprojekti. Toinen häiriöiden vähentymiseen johtava tekijä on vuonna 2016 maaliskuussa käyttöön otettu ITIL-muutoksenhallintaprosessi, jonka avulla erilaisten huolto- ja muutostöiden yhteentörmäystä voidaan välttää ja tieto tehdystä muutoksesta on muutoksenhallintakalenterin kautta kaikkien organisaation työntekijöiden tiedossa. Lisäksi muutosluvan saaminen vaatii aiempaa huolellisempaa ennakkovalmistelua ja hyväksymiskäytäntöä joko esimiehen, linjapäällikön tai muutoksenhallintakomitean toimesta.

Kun tarkastellaan sattuneiden häiriötilanteiden juurisyitä, voidaan todeta, että suurin osa olisi todennäköisesti tapahtunut huolimatta keskitetystä herätehallinnasta. Muutamia tilanteita olisi todennäköisesti voitu välttää ja osa häiriötilanteista johtui organisaation ulkopuolisista tekijöistä. On kuitenkin todennäköistä, joskaan ei faktatietoon perustuvaa päättelyä, että useimmissa häiriötilanteissa selvitystyö olisi ollut nopeampaa ja katkokset jääneet lyhemmäksi, mikäli käytössä olisi ollut kokonaisvaltainen herätehallinta- ja valvontaratkaisu.

9.4 Tietoturvapoikkeamat

Tieturvatapahtumia on ollut verrattain vähän ja niistä ei ole toistaiseksi aiheutunut laajamittaisia häiriötilanteita lukuun ottamatta vuonna 2016 huomattavasti yleistyneitä kiristyshaittaohjelmia. Tällaisissa tapauksissa haittaohjelma pääsee yleensä loppukäyttäjän koneelle sähköpostin liitetiedoston kautta käyttäjän avatessa tiedostoa. Kun haittaohjelma on päässyt koneelle, se salaa

kotihakemistoista löytyvät tiedostot ja huomattavana uhkatekijänä useimmiten myös käyttäjän verkkolevylle tallentamat tiedostot. Mikäli käyttäjällä on pääsy tärkeisiin ja laajoihin verkkolevyihin, voi lopputuloksena olla kriittinen häiriötilanne, joka vaikuttaa isoon määrään loppukäyttäjiä. Normaaleja viruksia ja pienempivaikutteisia haittaohjelmia torjutaan sähköpostijärjestelmän suodatuksella, mutta myös työasemilla olevilla paikallisilla virustorjuntaohjelmistoilla. Erittäin suuri osa haittaohjelmista kuten myös erilaiset verkkohyökkäykset ja murtoyritykset torjutaan palomuurin avulla. Palomuuriympäristöön on hankittu lisätoiminnallisuus, jonka avulla saadaan suojattua verkkoa hieman normaalia paremmin. Tämä toiminto täydentää muureilla olevaa haittaohjelmien torjunnan toiminnallisuutta uusien ja tuntemattomien uhkien osalta. Normaalisti AntiVirus-tunnisteet päivittyvät noin vuorokauden välein, kun taas lisäkomponentti päivittää myös haittaohjelmatunnisteita 15 - 30 minuutin välein, saaden näin aina tiedon tuoreimmista uhista. Uuden päivityksen myötä päivityssykli pienenee 5 minuuttiin. Lisäkomponentti seuraa verkkoliikenteestä esimerkiksi Adoben tiedostoformaatteja ja muita suoritettavia tiedostoja. Uuden tiedon kohdatessaan lisäkomponentti päästää tiedoston läpi, mutta tarkistuttaa sen myös palomuurivalmistajan virtuaalikoneissa. Mikäli tällöin havaitaan tiedoston sisältävän haitallista toiminnallisuutta, siitä tulee automaattisesti palomuureille tieto ja lisäys AV-tunnisteisiin. Tämän jälkeen haitalliset tiedostot eivät enää pääse läpi. Lisäksi uudet tunnisteet siirtyvät myös seuraaviin AV-tunnistepäivityksiin mukaan.

Top_25_murtoyritysta_hallinto

Threat/Content Name	ID	Threat/Content Type	Count
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
Apache Wicket Unspecified [redacted]	[redacted]	[redacted]	[redacted]
Microsoft Windows win.ini access attempt	[redacted]	[redacted]	627
WordPress Login Brute Force Attempt	40044	vulnerability	613
Generic HTTP Cross Site Scripting Attempt	31475	vulnerability	604
HTTP: User Authentication Brute Force Attempt	40006	vulnerability	596
HTTP Unauthorized Brute Force Attack	40031	vulnerability	596
HTTP /etc/passwd access attempt	35107	vulnerability	512
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerability	34804	vulnerability	510
HTTP SQL Injection Attempt	30514	vulnerability	257
Bash Remote Code Execution Vulnerability	36729	vulnerability	214
Generic HTTP Cross Site Scripting Attempt	31476	vulnerability	177
OpenSSL TLS Malformed Heartbeat Request Found - Heartbleed	36397	vulnerability	149
HTTP SQL Injection Attempt	33338	vulnerability	112
AWStats Rawlog Plugin File Disclosure Vulnerability	33781	vulnerability	64
HTTP SQL Injection Attempt	33340	vulnerability	45
PHP-Charts PHP Code Execution Vulnerability	37008	vulnerability	43
PHP Remote File Include Vulnerability	33327	vulnerability	38
HTTP SQL Injection Attempt	35823	vulnerability	36
Microsoft DCE RPC Big Endian Evasion Vulnerability	33510	vulnerability	33
Microsoft Windows RPC Fragment Evasion Attempt	32953	vulnerability	27
Oracle 9i Application Server Dynamic Monitoring Services Anonymous Access	33756	vulnerability	23
Microsoft SQL Server User Authentication Brute Force Attempt	40010	vulnerability	22

KUVA 5. Erilaisia palomuurin havaitsemia murtoyrityksiä 23.10.2016 – 29.10.2016 välisenä aikana.

Top_25_epailtya_hallinto

Threat/Content Name	ID	Count
Sipvicious.Gen User-Agent Traffic	13272	905
iMesh_Mediabar hijack IE auto search	11879	50
Virus/Win32.ExKit.d	1270352	13
Virus/Win32.WGeneric.kaajp	2087304	6
Virus/Win32.WGeneric.kkjkj	2527821	6
WGeneric.Gen Command And Control Traffic	14280	2
Adware/Win32.myp.j	2197063	2
Nemucod.JSDownloader.Gen Command and Control Traffic	14567	2
Win32.Conficker.C p2p	12544	1
TrojanDownloader/O97M.donoff.cep	1200991	1
Trojan-Downloader/MSExcel.cryptoload.os	1210590	1

KUVA 6. Epäilyttäviä verkkotapahtumia 23.10.2016 – 29.10.2016 välisenä aikana.

9.5 Esineiden internet ja nopeasti muuttuva maailma

Teknologia ja erilaiset teknologiaa hyödyntävät jokapäiväiset laitteet ja erilaiset uudet käyttökohteet teknologialle kehittyvät vauhdilla. Usein käy myös niin, että kaikkia uhkia ja mahdollisuuksia ei osata ottaa käyttäjien tai edes valmistajien toimesta huomioon ennen kuin taphtuu jonkin suuri vahinko tai esimerkiksi tietoturva-aukkoja hyödynnetään rikollisesti. Yksi tällaisista nykyteknologian nopeista kehitysaskelista on esineiden internet.

Perjantaina 21.10.2016 suoritettiin tietoturvahistorian laajin palvelunestohyökkäys yhdysvaltalaista Dyn-palveluntarjoajaa vastaan, joka on erikoistunut muun muassa nimipalveluiden tarjontaan. Hyökkäyksen johdosta miljoonat internetin käyttäjät Yhdysvaltojen itärannikolla eivät pystyneet käyttämään esimerkiksi Netflixiä, Paypalia, Etsyä tai Airbnb:tä. Myös tavalliset web-sivut saattoivat latautua hitaasti. Hyökkäyksen vaikutukset näkyivät osittain myös Euroopassa asti.

Palvelunestohyökkäyksessä hyödynnettiin laajamittaisesti tavallisia kuluttajalaitteita, kuten astianpesukoneita, itkuhälyttimiä ja erilaisia kameroita. Tällaisia joka kodin laitteita, jotka eivät ole varsinaisesti tietokoneita, mutta joilla on yhteys internettiin, kutsutaan esineiden internetiksi (Internet of Things, IoT). Yleistä näille laitteille on, että niiden tietoturva on heikolla tasolla ja yleensä laitteiden salasanoja tai käyttäjätunnuksia ei ole vaihdettu käyttäjän toimesta, tai niitä ei edes ole mahdollista vaihtaa. Tämä luo mahdollisuuden kaapata suuren määrän laitteita nopeasti ja yksinkertaisesti. Laitteille ei välttämättä koskaan vaihdeta käyttöönoton jälkeen käyttäjätunnuksia tai salasanoja, joten niiden kaappaaminen palvelunestohyökkäykseen on verrattain helppoa. Tämän jälkeen hyökkääjä voi asentaa laitteelle haittaohjelman, joka valjastaa laitteen hyökkääjän

käyttöön. Tämä voidaan tehdä laajasti automatisoituna toimenpiteenä, jolloin hyökkääjän ei tarvitse murtautua jokaiseen laitteeseen erikseen, vaan tämä toteutetaan tätä tarkoitusta varten kehitetyn ohjelmiston avulla. Tätä laitteiden kapasiteettiä hyödynnettiin osittain myös Dyn-palveluntarjoajaa vastaan tehdyssä hyökkäyksessä ja samalla se oli osoitus näiden laitteiden haavoittuvuuksista.

Yksi esimerkki tällaisesta automatisoidusta hyökkäysohjelmistosta on Mirai-bottiverkko, jota hyödynnettiin myös lokakuun hyökkäyksessä. Alun perin tätä on ilmeisesti käytetty pienemmällä voimalla hyökkäämällä ranskalaista palveluntarjoajaa ja tietoturvabloggaajaa vastaan. Nimimerkillä ”Anna_Senpai” toimiva henkilö on julkistanut Mirain lähdekoodin ja onkin odotettavissa, että useat muut tahot tulevat kopioimaan tätä tekniikkaa ja hyökkäyksien määrä voi yleistyä. Tekijästä tai tekijöistä ei kuitenkaan ole varmaa tietoa ja spekulointia eri tahoista esiintyy laajasti. Tällä hetkellä ei myöskään ole mitään varmaa keinoa suojautua IoT-laitteiden kaappausta vastaan, mutta on toivottavasti odotettavissa, että valmistajat tulevat tulevaisuudessa kiinnittämään tähän enemmän huomiota. (Helpnetsecurity 2016. Dyn DDoS attack: The aftermath, viitattu 28.10.2016.)

KUVA 7. (MalwareTech Twitter 2016. Mirai infections map, viitattu 6.11.2016.)

4.11.2016 uutisoitiin, että myös kokonaista valtiota vastaan on hyökätty hyödyntäen samaa Mirai-haittaohjelmaa. Hyökkäys on kohdistettu kahta liberialaista yritystä vastaan, jotka yhdessä omistavat ainoan maasta ulos johtavan runkoverkkoyhteyden. Iskujen seurauksena Liberia on ajoittain ollut eristettynä muusta internetistä. Hyökkäys on kestänyt uutisoinnin päivämäärään mennessä jo seitsemän päivän ajan ja epäilyksen alaisena on sama tekijä kuin Yhdysvaltojen iskulla. (tivi 2016. Kyberisku pudotti kokonaisen valtion verkosta, viitattu 4.11.2016.)

Kaikkia tällaisia nopeasti muuttuvia ja kehittyviä uhkia ei ole mahdollista torjua tai niihin on hankala varautua. Nykyiset tietoturvapalvelut ja erilaiset järjestelmät kuitenkin parantavat huomattavasti mahdollisuuksia joko estää yllättävätkin uhkat tai ainakin vähentää niistä koituvia seurauksia. Oulun Tietotekniikalla on tehty varautumissuunnitelmat ja tekniset järjestelyt tällaisen hyökkäyksen varalle, jolloin vahinkojen määrä voidaan minimoida. Uusien suojautumistapojen, -järjestelmien ja -palveluiden hankkiminen kuitenkin parantaa entisestään varautumista erilaisiin uhkiin.

10 HANKINTAPROJEKTI

Hankinta päätettiin suorittaa projektimuotoisena, jolloin sille voidaan määrittää selkeä alku- ja päätepiste. Samalla voidaan myös dokumentoida tehtyä työtä sekä siitä opittuja asioita ja parantaa näin organisaation tietoisuutta hankinnan etenemisestä. Opinnäytetyön tekijä toimii projektipäällikkönä ja on näin vastuussa kaikista projektiin kuuluvista asioista ja sen edistämisestä aikataulun mukaisesti. Ohjausryhmä valvoo puolestaan projektin toteutumista ja mahdollistaa projektille sen tarvitsemien resurssien saatavuuden.

Projektille määritettiin erilaisia tavoitepaikkoja eli päätöksentekopisteitä, joita olivat esimerkiksi esitietopyynnön julkaisu, kilpailutuksen käynnistäminen, toimittajan valinta ja sopimuksen allekirjoitus sekä projektin onnistumisen määrittäminen hankinnan ja käyttöönoton jälkeen. Projektin päättämisen jälkeen sen tuotokset raportoidaan ja dokumentoidaan sekä ohjausryhmälle että myös Oulun Tietotekniikan johdolle.

Ennen projektin aloittamista selvitettiin kokemuksia kumppaniorganisaatiolta, joka oli suorittanut herätehallintajärjestelmän hankinnan 2015 – 2016. Heiltä kysyttiin kokemuksia ja tyytyväisyyttä kilpailutuksen onnistumiseen, sekä alustavia suosituksia toimenpiteistä. Tiedonhankintahetkellä heillä oli kuitenkin menossa vielä kilpailutuksen valitusaika, joten saadut tiedot jäivät yleisluonteisiksi. Saimme kuitenkin hyviä neuvoja, jotka helpottivat oman työn aloittamista.

Hankittava ratkaisu tulee tukipalveluihin kuuluvan ja häiriöistä vastaavan ja niitä selvittävän tiimin vastuulle ja ylläpidettäväksi, joten sitä lähdetiin toteuttamaan siellä havaittujen tarpeiden mukaisesti kuitenkin niin, että hankittava järjestelmä palvelisi koko organisaation ja sen asiakkaiden tarpeita, eikä pelkästään yhtä tiimiä. Hankinta käynnistettiin tekemällä projektisuunnitelma, johon kirjattiin mahdollisimman tarkoin muun muassa hankinnan kohde, tavoitteet, vaatimukset ja resurssit. Projektin ohjausryhmäksi valittiin henkilöitä, joilla on aiempaa kokemusta julkisista hankintaprojekteista. Heidän tehtävänsä oli muiden ohjausryhmän tehtävien lisäksi tarvittaessa auttaa ja opastaa projektin edistämisessä ja siihen liittyvissä käytännön asioissa. Lisäksi projektille suunniteltiin alustavasti resurssit, jotka osallistuisivat aina tarpeen mukaan joko tarvemäärittelyyn tai kilpailutuksen jälkeen itse toteutukseen yhdessä palvelun tuottajan kanssa.

Projektille luotiin oma sähköinen työtila, jonne kaikki siihen liittyvät dokumentit taltioidaan. Työtilassa on myös kalenteri, johon merkitään tarpeelliset päivämäärät ja mahdolliset projektin kannalta tärkeät merkkipäivät, kuten tietopyynnön lähettäminen, kilpailutuksen käynnistäminen jne. Työtilaan on pääsy vain sinne erikseen sallituilla henkilöillä. Projektissa mainitaan joitakin tehtäviä

ja asioita, jotka liittyvät hankintaan, mutta ne rajataan ensimmäisestä hankintavaiheesta pois, jotta hankintaprojekti ei ajallisesti veny liian pitkäksi. Näitä asioita, kuten asiakasrajapinnan lisääminen, on kuitenkin hyvä mainita jo suunnitelmassa, koska ne ovat oleellinen osa hankinnalla tavoiteltavaa hyötyä.

Tämän tyyppisissä hankintaprojekteissa kaikkia vaiheita on mahdotonta kirjata etukäteen. Muutoksia suunnitelmiin ja yllättäviä tilanteita voi tulla, koska suunnitelmat tarkentuvat projektin edetessä. Oleelliset pääkohdat kuitenkin pyritään pitämään suunnitelman mukaisina. Projektin tavoitteet eivät saa muuttua.

Suunnitelman luonnin jälkeen projektiryhmä kokoontui käymään tavoitteita läpi ja arvioimaan kokonaisuutta. Koska Oulun Tietotekniikalla oli tarve myös hankkia osaamista ja järjestelmiä tietoturvallisuuden kehittämiseen, päätettiin hankintaan lisätä vielä tietoturvan osalta keskitetty lokien hallinta. Nämä eri järjestelmät tukevat toiminnoiltaan toisiaan ja tulisivat luontevasti saman hankinnan kautta. Projekti sai samalla työnimen Kyberturvallisuusratkaisut 2017. Nimensä mukaisesti projektilla lähdettiin hakemaan valmiita ratkaisuja vuodelle 2017.

KUVA 8. Projektin aikataulu.

11 TIETOPYYNTÖ

Markkinakartoitusta varten koostettiin tietopyyntö (”Request for Information”), jossa kerrotaan perustiedot organisaatiosta sekä nykytilanteesta liittyen tietopyynnön kohteena olevaan järjestelmään ja palveluun. Lisäksi tietopyynnöstä tulee selvitä sen tarkoitus ja tavoitetila. Tietopyyntöä ei haluttu tehdä ennakkoon liian tarkoin rajaavaksi, vaan toimijoille haluttiin jättää mahdollisuus tarjota erilaisia ratkaisuja ja vaihtoehtoisia toteutustapoja. Tietopyynnössä ilmoitetaan selkeästi myös tulevan hankinnan sopimusmalli, tässä tapauksessa OTT etsii kumppania, jonka kanssa sovitaan puitesopimus, jonka tavoitteena on hankkia OTT:n tarpeet täyttäviä palveluita, laitteita ja ohjelmistoja.

Tietopyynnöstä tulee käydä selvästi ilmi, että se ei ole varsinainen kutsu kilpailumenettelyyn, eikä sido osapuolia tässä vaiheessa mihinkään.

Tietopyyntöön on kirjattu selvennys tavoitteista seuraavasti:

> Tämä dokumentti ei ole tarjouspyyntö, hankintailmoitus tai kutsu neuvottelumenettelyyn, vaan markkinakartoitukseen liittyvä tietopyyntö (”Request for Information”) mahdollisille palveluntuottajille. Tietopyynnöllä on tarkoitus selventää ja tarkentaa tulevaan hankintaan liittyviä mahdollisuuksia ja palveluntuottajien kiinnostusta. Tietopyyntö ei sido millään tavalla OTT:aa eikä siihen vastaavia yrityksiä. Tietopyyntöön vastaaminen ei ole edellytys mahdolliseen myöhempään kilpailutukseen osallistumiselle.

Päätökset mahdollisen hankintaprosessin käynnistämisestä tehdään erillisesti markkinakartoituksen jälkeen. Selvyyden vuoksi todettakoon, että 25.8.2016 julkaistu ennakkoilmoitus ja tämä tietopyyntö eivät aseta OTT:lle velvoitetta käynnistää tarjouspyyntöprosessia ja OTT voi jättää hankinnan kokonaan toteuttamatta. OTT ei maksa korvauksia tietopyyntöön vastaamisesta. (Oulun Tietotekniikka. 2016c. Tietopyyntö,1)

11.1 Tietopyynnön sisältö

Hankittava järjestelmä ja palvelu jaettiin kahteen osaan, joista molemmille kirjoitettiin vaatimusmäärittely ja mahdolliset vaatimusta tarkentavat tekijät. Valvontaan ja keskitettyyn herätehallintaan määriteltiin tavoitteeksi ratkaisu, jonka avulla on muun muassa mahdollista mallintaa riippuvuudet erilaisista teknisistä järjestelmistä muodostuvista IT-palveluista. Lisäksi toiveena on IT-palveluiden terveydentilan ja palvelutason seuranta tilannekuvan muodostamiseksi.

Ratkaisun tulee myös tarjota tilannekuvaan pääsy sekä OTT:n työntekijöille että asiakaskohtaisesti räätälöidyille näkymille asiakkaan IT-palveluiden terveydentilaan.

Ratkaisulta haetaan seuraavia ominaisuuksia:

- selkeä ja helppolukuinen kokonaiskuva IT-palveluiden toimivuudesta ja terveydentilasta
- ratkaisuun voidaan mallintaa järjestelmien ja palveluiden väliset riippuvuussuhteet
- herätteet normalisoidaan ja korreloidaan
- herätteitä voidaan hallita keskitetysti ja niiden käsittelyä voidaan pitkälti automatisoida
- palvelinten perusvalvonta (saatavuus, suorituskyky, haavoittuvuudet, kapasiteetti)
- sovellus- tai tietokantakohtaista valvontaa (prosessit, kapasiteetti, tietokantavarmistukset, haavoittuvuudet)
- palomuurin tuottamat hälytykset (haittaohjelmat, tunkeutumiset, havainnot palvelunestohyökkäyksistä)
- virus- ja haittaohjelmatilanne (tartunnat)
- varmistusjärjestelmien valvonta (kapasiteetti, varmistusten onnistuminen)
- tietoliikenneyhteyksien valvonta (saatavuus, liikennemärät, luvattomat laitteet)
- AAA-palvelu (epäonnistuneet autentikoinnit, kapasiteetti)
- palvelutasoraporttien muodostaminen tuotannon tilasta
- virtuaalialustan, palvelinlaitteistojen ja tallennusjärjestelmien valvonta (terveydentila)
- sähköpostijärjestelmä (palveluiden terveydentila, jonojen viiveet ja tilanne)
- etäkäyttöratkaisut (saatavuus)
- IPAM (nimipalveluiden ja DHCP:n toiminta)
- asiakaskohtaiset valvontanäkymät web-käyttöliittymällä
- sähköpostijärjestelmän seuranta (terveydentila, saatavuus, viestiliikennemäärät)
- web-pohjainen käyttöliittymä
- suomenkielinen tukipalvelu ja käyttöohjeistus
- koulutus järjestelmän käyttöön.

Tietopyynnössä määriteltiin vaatimuksia myös palveluiden tuottamisen osalta. Nämä palvelut kuuluvat kumppanin vastuualueelle ja ovat osa kokonaishintaa. Valittavan puitesopimuskumppanin tulee toteuttaa ja vastata keskitetyn herätehallinnan käyttöönottoprojektista. Kumppanin tulee vastata herätehallinnan alustan toimivuudesta ja lisäksi sen tietoturvan ja kapasiteetin valvonnasta. Tukipalvelutoiminnot tulee toteuttaa suomenkielisenä ja kumppanin tulee tarjota koulutus

järjestelmän käyttöön ja päivittäiseen ylläpitoon. Herätehallinnan automatisointi ja optimointi tehdään yhteistyössä OTT:n asiantuntijoiden kanssa. Lisäksi kumppani toteuttaa palveluiden mallinnuksen ja asiakaskohtaisten näkymien räätälöinnin.

Keskitetyn lokienhallinnan osalta vaatimukset eroavat hieman herätehallintajärjestelmän vaatimuksista, koska OTT:lla ei ole aiempaa kokemusta järjestelmän toteutuksesta tai tarvittavista suunnittelutoimenpiteistä. Ensimmäisessä vaiheessa tarpeena on konsultointityö, jonka lopputuloksena syntyy lokipolitiikka Oulun kaupungille.

Konsultointityö sisältää:

- koulutuksen keskitetyn lokienhallinnan merkityksestä, periaatteista ja hyödyistä
- asiakastarpeen selvityksen ja lokilähteiden kartoituksen eri sidosryhmiltä
- lokipolitiikan kirjoittamisen työpajatyöskentelynä
- järjestelmäkohtaisten lokikorttien luonnin ensimmäisessä vaiheessa keskitettyyn lokienhallintaan liitettävien järjestelmien osalta
- voimassaolevan lain ja EU-tietosuojalain edellyttämien lokien säilytyksen, käsittelyn, suojaamisen ynnä muiden vaatimusten kirjaaminen osaksi lokipolitiikkaa
- lokienhallintaan liittyvien roolien ja vastuiden kirjaaminen lokipolitiikkaan.

Lisäksi on tarpeen tehdä järjestelmäkohtaiset lokikortit, jotta yksittäisten järjestelmätietojen löytäminen ja päivittäminen onnistuvat tarpeen tullen nopeasti. Näin on myös helpompi käydä neuvotteluja asiakkaiden kanssa heidän tarvitsemistaan lokitustarpeista.

Järjestelmäkohtaisissa lokikorteissa otetaan muun muassa kantaa seuraaviin asioihin:

- käsitelläänkö järjestelmässä arkaluonteisia tietoja
- minkälaisia lokeja järjestelmässä luodaan
- säilytetäänkö loki paikallisesti vai tallennetaanko se keskitettyyn lokienhallintaan
- kauanko lokia säilytetään ja miten se kierrätetään
- miten loki siirretään lokienhallintajärjestelmään
- poikkeaako järjestelmän toiminta lokipolitiikassa määriteltyyn nähden.

Lokipolitiikka kirjoitetaan suomen kielellä. Lokipolitiikan määrittelyn jälkeen kumppani rakentaa yhteistyössä OTT:n kanssa keskitettyyn lokienhallintaan ja analysointiin ratkaisun, jonka tulee mahdollistaa:

- lokipolitiikan mukaisen lokitietojen tallentamisen erilaisista teknisistä järjestelmistä ja asiakkaiden tietojärjestelmistä

- järjestelmään tallennettujen lokitietojen muuttumattomuuden ja elinkaaren hallinnan
- lokitietojen automatisoidun analysoinnin ja herätteiden luonnin tietoturvatapahtumista sekä IT-palveluiden saatavuuteen, kapasiteettiin tai suorituskykyyn liittyvistä tapahtumista
- havaittujen tietoturvatapahtumien automaattisen normalisoinnin, korreloinnin ja hälytykset
- automaattisen raportoinnin ja tietoturvallisuuden tilannekuvan muodostamisen.

Keskitettyä lokienhallintaa tullaan hyödyntämään myös tietomurtojen havaitsemisessa sekä todisteiden keräämisessä siten, että tietomurrot voidaan todeta aukottomalla todistusketjulla. Keskitettyyn lokienhallintaan liitettävien tietojärjestelmien osalta tavoitteena on, että tietojärjestelmästä tallennettujen lokitietojen perusteella voidaan jälkikäteen todentaa, kuka on suorittanut henkilötietojen haun tietojärjestelmästä, mitä henkilötietoja on katsottu, muutettu, lisätty tai poistettu, sekä milloin toimenpide on suoritettu.

Puitesopimuskumppanin odotetaan rakentavan OTT:n tarpeet täyttävä lokienhallintaympäristö palveluineen.

Lakienhallinnan palvelulta odotetaan seuraavia ominaisuuksia:

- keskitetyn lokienhallinnan käyttöönottoprojekti
- keskitetyn lokienhallinnan alustan toimivuuden, tietoturvan ja kapasiteetin valvonta
- suomenkielinen tukipalvelu
- koulutus järjestelmän käyttöön ja päivittäiseen ylläpitoon
- erilaisten lokitietoa tuottavien teknisten järjestelmien ja asiakkaiden tietojärjestelmien integrointi osaksi keskitettyä lokienhallintaa
- tietoturvaan ja tietojärjestelmien tietosuojaan liittyvien herätteiden ja hälytysten optimointi sekä käsittelyn automatisointi
- erilaisten järjestelmä- ja asiakaskohtaisten raporttien tuottaminen
- reagointi havaittuihin tietoturvamurtoihin yhteistyössä OTT:n kanssa
- tietomurtojen forensiikka.

Hankinnan tavoitteet määriteltiin niin ikään helpottamaan toimijoiden kykyä arvioida omaa mielenkiintoaan ja osallistumismahdollisuuttaan. Toivomuksena oli lisäksi, että herätehallinnan ja valvonnan sekä myös lokienhallinnan tarpeet voidaan täyttää yhdellä teknisellä ratkaisulla.

Hankinnan tavoitteet:

- parantaa OTT:n kykyä havaita tietoturvapoikkeamia ja reagoida niihin

- mahdollistaa keskitetyn lokien tallentamisen, analysoinnin ja hallinnan
- mahdollistaa EU:n tietosuoja-asetuksen mukaisen tietosuojan valvonnan
- mahdollistaa keskitetyn herätehallinnan ja aiempaa proaktiivisemman tukipalvelun
- parantaa asiakkaiden näkymää omien IT-palveluidensa toimivuudesta
- muodostaa kattavan kokonaiskuvan IT-palveluiden terveydentilasta.

Lopuksi tietopyynnössä esitetään toimittajille kysymyksiä, joiden perusteella on helpompi arvioida heidän mahdollisuuksiaan toimittaa pyydettyjä ratkaisuja ja yleistä yritysten vakautta. Toimittajat saivat vastata kysymyksiin vapaamuotoisesti.

Kysymykset toimijoille:

Kysymys 1: Toimittajan nimi- ja yhteystiedot.

Kysymys 2: Kuvaus tarjoamastanne teknisestä ratkaisusta.

Kysymys 3: Kuvaus osaamisestanne, tarjoamastanne palvelusta ja sen palvelutasoista.

Kysymys 4: Pyydämme esittämään osaamisprofiileja palvelun tuottamiseen käytettävissä olevista henkilöistä tai henkilötyypeistä (työkokemus vuosina sekä ajallinen ja sisällöllinen kokemus hankinnan kohteen osaamisalueilta). Pyydämme, että ette liitä vastaukseenne henkilöiden ansioluetteloita.

Kysymys 5: Millaisia hinnoittelumalleja teillä on tarjoamillenne ratkaisuille?

Kysymys 6: Oletteko kiinnostuneita osallistumaan tarjouskilpailuun, mikäli sellainen järjestetään?

Kysymys 7: Voimassa olevat referenssit tarjotunlaisen palvelun tuottamisesta OTT:n kokoluokan ympäristössä.

11.2 Tietopyynnön julkistaminen ja toimijoiden vastaukset

Tietopyynnön sisällön valmistuttua se julkaistiin HILMAssa. HILMA on työ- ja elinkeinoministeriön ylläpitämä maksuton ja sähköinen ilmoituskanava, jossa hankintayksiköt ilmoittavat julkiset hankintansa. Yritykset saavat palvelusta reaaliaikaista tietoa käynnissä olevista hankintamenettelyistä ja ennakkotietoa tulevista hankinnoista. Palvelussa ilmoitetaan sekä

kansalliset että EU-kynnysarvon ylittävät hankinnat. EU-ilmoituksissa HILMAssa täytetään ennakkoilmoitus, hankintailmoitukset ja jälki-ilmoitukset. (HILMA 2016, viitattu 1.11.2016.)

Tietopyynnössä oli määritetty valmiiksi aikarajat, joiden mukaan hankinnasta kiinnostuneiden toimijoiden tulee osoittaa kiinnostuksensa hankintaa kohtaa. Koska tietopyyntö sisälsi tarkkaa teknistä informaatiota Oulun Tietotekniikan järjestelmistä, todettiin sen julkaisemisen sellaisenaan vaarantavan tietoturvaa. Tämän vuoksi toimijoita pyydettiin ottamaan yhteyttä tarkempien määrittelyiden toimittamista varten. Halukkaille toimijoille lähetettiin tarkempi tietopyyntödokumentti salattuna sähköpostina, jonka sisältöä ei ole mahdollista kaapata ulkopuolisten tahojen toimesta ja sähköpostia ei voi sellaisenaan välittää eteenpäin. Tietopyynnön aikarajat määriteltiin niin, että ennakkoilmoitus julkaistiin 25.8.2016. Toimijoilla oli mahdollisuus esittää tarkentavia kysymyksiä, jotka tuli esittää viimeistään 9.9.2016. Kaikki tulleet kysymykset ja niiden vastaukset koottiin yhteen dokumenttiin ja lähetettiin yhteisesti kaikille kiinnostuksena esittäneille toimijoille. Vastaukset tietopyyntöön tuli esittää 23.9.2016 klo 16.00 mennessä. Tämän jälkeen OTT katsoo tulleista vastauksista kiinnostavimmat ja kutsuu nämä toimijat yhteiseen tekniseen vuoropuheluun, joka käydään Oulussa OTT:n tiloissa. Aikaa näille toimittajatapaamisille varattiin kahden viikon ajanjaksolta. Alkuperäistä aikataulua jouduttiin hieman siirtämään ja toimittajatapaamiset sovittiin viikoille 45 ja 46.

Yhteensä kiinnostuksena lisätietoihin esitti 23 eri toimijaa, joille tiedot toimitettiin. Lopulta kiinnostuksena hanketta kohtaan osoitti 11 toimijaa, joista kymmenelle ilmaistiin halukkuus lisätietoihin ja tekniseen vuoropuheluun.

Erikoisuutena alkuperäisen tietopyynnön julkaisussa ilmeni sääntömuutos, josta emme olleet tietoisia. Julkaisimme tietopyynnön vallitsevien ohjeiden mukaisesti, mutta se palautettiin meille täydennettäväksi. Syytä tiedustellessa meille ilmoitettiin, että sen hetkisen ohjeistuksen mukaan EU-laajuisessa ennakkoilmoituksessa ei saanut käyttää sanoja tekninen vuoropuhelu tai markkinakartoitus. Jouduimme näiltä osin muotoilemaan tietopyynnön uudelleen, jonka jälkeen se hyväksyttiin. Ilmeisesti säädökset julkaisun sisällöstä olivat vaihtuneet vain muutamaa päivää ennen julkaisua ja siitä ei ollut ehditty tiedottaa käyttäjiä, eikä esimerkiksi hankintoihin erikoistunut lakimiestoimisto tiennyt vielä asiasta.

12 TOIMITTAJIEN RATKAISUKUVAUKSET

Hankinnasta kiinnostuneet toimittajat lähettivät teknistä tietoutta ja materiaalia tarjoamistaan palveluista sekä vastaukset esittämiimme kysymyksiin. Näiden materiaalien perusteella valittiin markkinavuoropuheluun 10 eri toimittajaa. Osalla heistä oli tarjottavanaan kolmannen osapuolen tekninen ratkaisu, jossa he toimivat kumppanina. Osa toimittajista tarjosi yksilöllistä ratkaisua, jollaista ei ollut tarjottavana muilla. Isoilla toimittajilla on yleensä tarjottavana myös useita erilaisia ratkaisumahdollisuuksia. Materiaalien kattavuus vaihteli hyvin suuresti, osa lähetti erittäin tarkat tekniset kuvaukset, kun osa yksinkertaisesti totesi omaavansa kyvyn toteuttaa ilmoitetut vaatimukset. Ainoa vuoropuhelusta pois jäänyt toimittaja ei vastannut kysymyksiin ja lähetti vain teknisen ratkaisun kuvauksen. Toimittajien lähettämät materiaalit talletettiin projektin sähköiseen työtilaan, jolloin tarjolla olevia ratkaisuja voivat tarvittaessa tutkia ja vertailla kaikki projektiin osallistuvat henkilöt.

Tarkastelemme seuraavassa tarkemmin eri toimittajien ratkaisuja. Koska suurin osa ilmoitti materiaalinsa salaiseksi ja materiaalin informaatioarvon vaihdellessa hyvin paljon, keskitymme jokaisen toimittajan osalta kolmeen eri alueeseen. Ensimmäisenä tarkastelemme, voiko toimittaja toteuttaa valvontajärjestelmän ja jos voi, niin millä tavalla toteutus tapahtuu. Toiseksi tarkastelemme, voiko toimittaja toteuttaa lokienhallinnan tai SIEM-järjestelmän ja jos voi, niin millaista toteutusta toimittaja voi tarjota. Kolmanneksi tarkastelemme toimittajan palvelukuvausta. Lisähuomiona mainitaan mahdollisia erityispiirteitä tai yleistä arviointia toimittajan kyvykkyydestä toteuttaa haluttu ratkaisu. Arviot on tehty pelkästään kunkin toimittajan toimittaman materiaalin perusteella ja niissä ei ole otettu huomioon myöhemmin tullutta lisätietoa aiheeseen. Tämän tarkoitus on kuvata tilannetta, jossa pelkän kirjoitetun materiaalin perusteella voi olla hankala saada todellista kuvaa tarjotusta kokonaisuudesta.

12.1 Toimittaja A

Materiaalin perusteella valvontapalvelua on mahdollista tilata vain niin, että kaikki valvonta suoritetaan toimittajan valvontaympäristössä ja he huolehtivat myös tilannekuvan seurannasta. Ilmeisesti heiltä ei ole mahdollista tilata pelkkää järjestelmäratkaisua siihen liittyvin oheispalveluin.

On erittäin todennäköistä, että tällainen palvelumalli tulee hyvin kalliiksi ja ei vastaa alkuperäistä vaatimusmäärittelyä tarjoten jopa ylipalvelua. Hintatietoja ei kuitenkaan ole tiedossa, joten tästä on vielä tässä vaiheessa hankala tehdä johtopäätöksiä. Valvontapalvelu itsessään vastaa kuvauksen perusteella vaatimuksia ja tarpeita.

Valvontaratkaisulla voidaan valvoa tietoverkkoon liitettyjen järjestelmien käytettävyyttä sekä niiden eri osa-alueiden tilaa. Lisäksi valvontaan voidaan liittää hallintapalveluita, jolloin aktiivilaitteiden häiriöihin reagoidaan sopimuksen mukaan joko reaktiivisesti tai proaktiivisesti. Asiakkaan tiloihin voidaan asentaa toimittajan valvontaan liitettävä valvontapalvelin, joka valvoo paikallisesti asiakkaan tietoverkossa sijaitsevia valvottavia laitteita.

Tekninen ratkaisu on kuvattu hyvin ja selkeästi ja heidän käyttämänsä tekninen alusta on yksi markkinajohtajista SIEM-ratkaisujen alalla. Teknisen kuvauksen perusteella toimittaja pystyy vastaamaan OTT:n vaatimuksiin SIEM-järjestelmän osalta ja lisäksi on mahdollista tilata lisäarvopalveluna ominaisuuksia, joita ei välttämättä tarvitse vielä ensivaiheessa. Myöskin valvontapalvelu on kattava ja sisältää riittävästi vaadittuja ominaisuuksia.

Toimittaja kuvailee yhteenvedossa olevansa Pohjoismaiden ja Baltian johtava IT-infrastruktuuritoimittaja, jolla on toimipisteitä useissa Pohjoismaissa ja Baltiassa. Toimittajalla on ratkaisuja ja palveluvaihtoehtoja useimpiin eri tietotekniikkaympäristön tarpeisiin. Toimittajalla on useita strategisia kumppaneita, joista valitaan sopiva vaihtoehto vastaamaan kulloisenkin asiakkaan yksilöllisiä tarpeita.

Toimittaja on selkeästi tuotteistanut palvelunsa niin, että valikoimasta on helppo valita sopiva kokonaisuus asiakkaan yksilöllisen tarpeen mukaan. Sekä palvelu että tekninen alusta ovat monipuolisia ja muokattavissa erilaisiin käyttötarkoituksiin.

12.2 Toimittaja B

Toimittajalla on valikoimissaan useita eri teknisiä ratkaisuja, joista on mahdollista valita asiakkaalle parhaiten sopiva vaihtoehto. Lokienhallinta- ja SIEM-järjestelmiä kuvataan materiaalissa vain nimellä, mutta näiden perusteella valikoimasta löytyvät kaikki suuret järjestelmät. Herätehallinta- ja valvontaratkaisujen teknisestä toteutuksesta ei ole tarkempaa mainintaa, mutta senkin luvataan olevan mahdollista toteuttaa.

Palveluvalikoima vaikuttaa kattavalta ja toimittaja muun muassa nimeää asiakaskohtaisen konsultointivastaavan, joka tuntee asiakkaan ympäristön ja kehityssuunnitelmat ja osaa tämän pohjalta suositella eri ratkaisuja. Lisäksi heillä on tarjota erilaisia palvelumalleja, kuten valvontapalveluiden toimitusta erilaisilla tasoilla, kuten valvonnan toteuttamista asiakkaan tiloissa tai jaettuna palveluna, jolloin osa valvonnasta toteutetaan asiakkaan tiloissa ja osa toimittajan ympäristössä. Eri palveluvaihtoehtoja ei kuitenkaan kuvata edellä mainittua tarkemmin.

Koska kyseessä on suurikokoinen yritys, on todennäköistä, että he pystyvät toimittamaan vaatimusmäärittelyn mukaisen kokonaisuuden, mutta jälleen lopullinen hinta jää kysymysmerkiksi. On hyvin mahdollista, että myös tämän toimittajan osalta valvontapalvelut ovat ylimitoitettuja.

12.3 Toimittaja C

Toimittajalla on tarjota selkeä erillinen ratkaisu sekä valvontaan että lokienhallintaan. Molemmat järjestelmät ovat toisistaan riippumattomia tekniseltä alustaltaan ja niitä voidaan räätälöidä tuotekohtaisesti. Materiaalista ei käy ilmi, onko järjestelmä omaa tuotantoa vai perustuuko se jonkin suuremman järjestelmätoimijan ratkaisuun. Huomionarvoista on kuitenkin, että molempia tarjotaan suoraan asiakkaan käytettäväksi ilman, että varsinainen valvonta ja lokienhallinta tapahtuisi toimittajan tiloissa. Teknisen kuvauksen perusteella järjestelmien ratkaisut vastaavat vaatimusmäärittelyyn hyvin ja varsinkin asiakkaan tiloissa tapahtuva ylläpito ja valvonta vastaavat erittäin hyvin vaatimuksiamme. Järjestelmien toimintaa ja käyttömahdollisuuksia kuvataan selkeästi ja hyvin esimerkein.

Toimittaja on suomalainen yritys, jolla on suuria kotimaisia asiakkaita. He toimittavat myös muita palveluita pyydettyjen ratkaisujen lisäksi. Asiakkaalle nimetään konsultti, joka vastaa palvelujen toimittamisesta yhteistyössä sovittujen tavoitteiden mukaisesti, ja erilaiset palvelutasot ovat myös räätälöitävissä.

Kokonaiskuvauksen perusteella kyseessä on hyvin varteenotettava vaihtoehto, joka vastaa erinomaisesti vaatimukseen paitsi teknisen toteutuksen ja palveluvaihtoehtojen osalta myös järjestelmän ylläpito- ja valvontaratkaisun puolesta. On todennäköisesti mielekkäämpää tilata itse tekninen toteutus ja siihen liittyvä palvelu, jota voi seurata oman organisaation työnä, kuin että kokonaisuus tulisi kokonaan palveluna toimittajan tiloista.

12.4 Toimittaja D

Toimitetun materiaalin perusteella toimittajalla ei ole tarjottavanaan ollenkaan herätehallinta- ja valvontaratkaisua, vaan toimittajan pääosaaminen keskittyy tietoturvan valvontaan ja lokienhallintajärjestelmän toimittamiseen. Tämän vuoksi toimittajaa ei ensin valittu tekniseen vuoropuheluun mukaan mutta he ilmoittivat myöhemmin, että pystyvät toimittamaan kumppanin kautta palveluna myös herätehallinta- ja valvontajärjestelmän. Tästä ei kuitenkaan ole minkäänlaista kuvausta saadussa materiaalissa. Itse lokienhallinnan ja SIEM-ratkaisun osalta toimittaja käyttää samaa teknistä alustaratkaisua kuin Toimittaja A. Vaikka tekninen alusta on sama, on kuitenkin joitakin toimittajakohtaisia eroja havaittavissa. Toimittaja ei kuvauksensa perusteella pysty toimittamaan asiakasnäkymää OTT:n asiakkaille tai työntekijöille, mutta tietoa on mahdollista välittää eteenpäin erilaisten rajapintojen kautta muille järjestelmille. Esittelymateriaalin perusteella on hankala myös saada kuvaa siitä, miten järjestelmän valvonta ylipäätään näyttäytyy asiakkaalle. Tekniset kysymykset on käsitelty kattavasti ja niiltä osin vaatimuksiin vastataan hyvin. Kokonaiskuvan muodostaminen on kuitenkin hankalaa.

Toimittaja on pohjoismainen tekniseen konsultointiin erikoistunut yritys, jolla on ilmeisen selvästi syvä tekninen osaaminen ja vankka tausta tietoturvaratkaisujen toimittamisessa. Materiaalin perusteella ei kuitenkaan saa muodostettua kunnollista kuvaa siitä, miltä osin vaatimusmäärittelyyn lopulta pystytään vastaamaan ja jäisikö tilaajan vastuulle hankkia mukaan vielä jokin kolmas osapuoli, jotta tahdottu toiminnallisuus saavutettaisiin, tai tarvittaisiinko omana työnä järjestelmän saattaminen halutulle toimintatasolle.

12.5 Toimittaja E

Tarjottu ratkaisu sisältää herätehallinnan ja valvonnan vaatimusmäärittelyn mukaisesti. Teknologia-alustana on kolmannen osapuolen tekniikka, jota muut hankkeesta kiinnostuneet toimittajat eivät ilmoittaneet käyttävänsä. Kuvauksen perusteella tarjottu ratkaisu vastaa hyvin toivottua ja kykenee hallitsemaan erilaisia herätelähteitä ja OTT:n käyttämien järjestelmien valvonta onnistuu suoralla kytköksellä tai vaihtoehtoisesti välirajapinnan kautta. Mielenkiintoisena lisäominaisuutena valvontajärjestelmä kykenee muodostamaan riippuvuuskarttoja ja

järjestelmämallinnuksia, jolloin vikaantuneen järjestelmän vaikutukset muihin palveluihin on helppo löytää.

Keskitetyn lokienhallinnan osalta vaatimuksiin vastataan, joskaan materiaalista ei käy selville, minkä valmistajan järjestelmää käytetään, vai onko kyseessä toimittajan oma ratkaisu. Tarjottu SIEM-palvelu kykenee hoitamaan toivotut perustehtävät kuten lokien korreloinnin ja normalisoinnin. Järjestelmä on myös mahdollista toteuttaa eri keinoin, kuten virtualisointialustan päälle asennettavin komponentein tai tarvittaessa erilliselle fyysiselle palvelinympäristölle. Kuvauksen perusteella järjestelmästä on mahdollista rakentaa hyvin vikasietoinen, jolloin käyttökatkokset tai häiriöt järjestelmissä eivät aiheuta lokitietojen ja datan hävikkiä.

Kokonaisuus voidaan toimittaa puhtaana ratkaisuna, jolloin teknisen alustan kokonaisuuteen sisältyy käyttöönottoprojekti ja itse valvonta jää tilaajan vastuulle. Toisena vaihtoehtona tarjotaan kokonaispalvelua, jolloin pakettiin sisältyy myös järjestelmän valvonta ja hallinta toimittajan puolesta. Itse järjestelmälle on mahdollista valita erilaiset palveluluokat, joilla on merkitystä esimerkiksi ilmenneiden vikatilanteiden korjaamiseen tai esimerkiksi herätteiden tunnistamiseen ja kategorisointiin käytettävään aikaan.

12.6 Toimittaja F

Toimittajan tarjoamat ratkaisut eroavat muista toimijoista oleellisesti ja eivät sinällään vastaa ilmoitettua vaatimusmäärittelyä. Toimittajalla on kuitenkin vahva tausta tietoturvallisuusratkaisujen parissa, joten yleisen tietämyksen ja osaamisen kehittämiseksi on mielenkiintoista kuulla tarkemmin heidän tarjoamistaan ratkaisuista.

Toimittaja tarjoaa kahta tuotetta, joista toinen keskittyy tietoturvauhkien havaitsemiseen ja torjumiseen. Varsinaista teknistä kuvausta ei tarjota, mutta kyseessä on kokonaisvaltainen palvelu, jolla pystytään havaitsemaan ja reagoimaan edistyneisiinkin tietoturvauhkiin. Palvelu sisältää myös asiantuntijapalvelut ja nopean tiedonvälityksen tietoturvatapahtumista. Toinen tuote puolestaan keskittyy haavoittuvuuksien seurantaan ja hallintaan sekä tietoverkon suojaamiseen. Kyseinen palvelu on ennen kaikkea tärkeää suurille julkisessa internetissä toimiville operoijille, kuten verkkokaupoille ja isoja palvelukokonaisuuksia internetin kautta tarjoaville yrityksille.

Ratkaisu voisi kuvauksensa perusteella sopia erinomaisesti lisäarvopalveluksi nyt hankinnassa olevan järjestelmäkokonaisuuden päälle. On kuitenkin todennäköistä, että kokonaiskustannukset kohoaisivat liian suuriksi.

12.7 Toimittaja G

Toimittaja on suuri kansainvälinen toimija, joka tuottaa erilaisia palveluita ja teknisiä ratkaisuja monenlaisiin IT-ympäristöihin. Toimittajan materiaaleissa on kuvattu seikkaperäisesti tarjottu tekninen ratkaisu ja erilaiset palveluvaihtoehdot. Huomionarvoista on, että kyseinen toimittaja kykenee kuvauksensa mukaisesti tarjoamaan sekä herätehallinnan, valvonnan että lokienhallinnan saman järjestelmän kautta, jolloin koko ratkaisu on yhteneväinen ja hallittavissa saman käyttöliittymän kautta. Tarjotun ratkaisun tekninen alusta on yksi johtavista lokienhallinnan ja SIEM-järjestelmien alustoista, mutta ainoa laatuaan tähän hankintaan tulleista esitietoilmoituksista. Tarjottu ratkaisu vastaa hyvin esittämiimme vaatimusmäärittelyihin ja lisäksi sen avulla voidaan toteuttaa mahdollisena jatkokehityksenä eritasoisia toimenpiteitä, joita ei vielä tässä vaiheessa ole arvioitu tarpeelliseksi, kuten esimerkiksi työasemien tietoturvavalvonta. Lisäpalveluna toimittaja tarjoaa myös haavoittuvuuksien analysointia ja uhkiin varautumista heidän valvontansa kautta.

Toimittaja esittää selkeät palvelukuvaukset ja erilaiset vastuualueet, jotka kuuluvat toimittajalle ja joihin tilaaja joutuu sitoutumaan. Palveluissa mainitaan muun muassa tietomurtojen forensiikka, asiakaskohtaiset näkymät tilannekuvaan ja suomenkieliset tukipalvelut ja itse järjestelmän ylläpitopalvelut Suomessa. Erityishuomiona toimittaja on koostanut erillisen dokumentin, jossa käydään yksityiskohtaisesti läpi palvelun laatuun liittyviä asioita ja esimerkiksi erilaiset vasteajat, mikäli heidän toimittamansa järjestelmä ja palvelu vikaantuvat. Materiaalin perusteella palvelu tuotetaan kokonaisuudessaan toimittajan taholta, jolloin on mahdollista, että kokonaiskäyttökustannukset kohoavat. Tiedoista ei käy selville, onko mahdollista tilata pelkästään ratkaisuvaihtoehtoa.

12.8 Toimittaja H

Toimittajan tarjoama tekninen toteutus pohjautuu samaan ratkaisuun kuin toimittajilla A ja D. Käytössä on siis vahvasti lokienhallintaan ja tietoturvatapahtumien seuraamiseen keskittyvä

ratkaisumalli. Pyydettyä teknistä herätehallintaa ja valvontaa ei voida kaikilta osin tällä tuotteella toteuttaa. Toimittaja kuitenkin kertoo pystyvänsä toimittamaan kolmannen osapuolen ratkaisun, joka määräytyy myöhemmin asiakkaan kanssa käytävien tarkentavien keskusteluiden pohjalta. Toimitetuissa dokumenteissa ei esitetä kuitenkaan tarkempia kuvauksia eri vaihtoehdoista tai niiden tarjoamista toiminnollisuuksista. Toimittaja kuitenkin on kirjoittanut kattavan kuvauksen kaikista vaatimusmäärittelyssä ilmoitetuista esimerkeistä ja kuvauksen perusteella valvontaa voidaan suorittaa myös tekniselle alustalle tarjotulla SIEM-järjestelmällä paremmin kuin mitä kävi ilmi aiempien toimittajien kuvauksista.

Toimittaja on selkeästi jakanut eri vaiheisiin lokienhallintajärjestelmän ja lokipolitiikan muodostamiseen tarvittavat työtehtävät. Kuvauksen mukaan toimittaja on tehnyt useita vastaavia selvityksiä erilaisille organisaatioille ja toimitetun materiaalin perusteella tälle väittämälle on myös perusteet. Lokipolitiikan muodostamisen jälkeen kokonaisuus toimii myös SIEM-järjestelmänä, joka pystyy yhdistämään eri tapahtumaketjuja ja tuottamaan niistä hälytyksiä, näkymiä ja raportteja.

Toimitetuissa materiaaleissa on mukana myös kattavat kuvaukset palveluhallinnan osalta ja tarkasti määritellyt palvelutasot, joiden perusteella toimija tarjoaa kokonaispalvelua pyydetyille ratkaisuille

12.9 Toimittaja I

Toimittaja on lähettänyt lyhyen kuvauksen tarjoamistaan palveluista, joiden mukaan kykenee toimittamaan usean eri valmistajan teknisiä ratkaisuja. Materiaalissa on kuvattu lyhyesti muutamaa mahdollista tuotetta, mutta niiden tarkempaa esittelyä ei ole sisällytetty toimitettuun dokumentointiin. Toimitetun sisällön perusteella myös tämän toimittajan ratkaisu painottuu vahvasti lokienhallinnan ja SIEM-ratkaisun suuntaan. Ratkaisukuvauksessa ei ole otettu kantaa teknisen herätehallinnan ja valvonnan määrittelyyn ja toimitusmahdollisuuteen.

Toimittaja on liittänyt mukaan projektiehdotuksen, jonka mukaan ensin kannattaa suorittaa käyttöympäristön mitoitus, jotta oikean SIEM-järjestelmän valinta voitaisiin suorittaa kokonaiskapasiteettitarpeen perusteella. Tällöin hankinta jakautuisi niin, että mittausvaiheessa toimittaja asentaa käyttöympäristöön tiedon keräimiä niin, että saadaan käsitys kerättävän tiedon määrästä. Toisesta vaiheessa toimittaja analysoi kerättyjä lokeja sekä miettii asiakkaan kanssa tulevia tarpeita. Kolmannessa vaiheessa toimittaja tilaa omalta päämieheltään tarpeelliset lisenssit

ja suorittaa SIEM-järjestelmän komponenttien asennuksen. Tässä vaiheessa myös järjestetään asiakkaalle koulutus ympäristön hallintaan ja ylläpitoon. Hankaluutena tällaisessa järjestelyssä on kilpailutusvaihe, jolloin kaikki tulleet tarjoukset pitää pystyä arvioimaan myös kustannusten osalta ja koska tässä tiedetään lopulliset kustannukset vasta projektin loppuvaiheessa, voi hinta-arviointia olla mahdoton suorittaa.

12.10 Toimittaja J

Palvelukuvauksessaan toimittaja vastaa määrittelyvaatimuksiin ehdottamalla toisistaan eriytettyjä ratkaisuja. Tällöin herätehallinta ja valvonta esimerkiksi palveluiden saatavuuden, kapasiteetin hallinnan ja tietototurvan osalta toteutettaisiin omalla ratkaisulla. Lisäksi verkko-, palvelin- ja sovellusvalvonnalle olisi oma järjestelmä, samoin kuin herätteiden hallinnalle. Materiaalista ei kuitenkaan käy ilmi, millä teknisellä järjestelmällä tai toteutuksella nämä eri vaihtoehdot toimitettaisiin. Ilmeisesti kyse on kokonaispalvelusta, jolloin asiakkaan toimesta määritellään valvottavat kohteet ja varsinainen valvonta ja hallinta suoritetaan toimittajan tiloissa. Edellä mainittujen vaihtoehtojen lisäksi toimittaja tarjoaa SOC-palvelua, joka on puhtaasti tietoturvaan erikoistunut palvelu. Myös tämä vaihtoehto toimitetaan kokonaispalveluna. Lisäksi toimittajalla on meneillään tuotteistus uudesta tietoturvan tilannekuvapalvelusta, joka on tarkoitettu lähinnä yritysten ylemmän johdon käyttöön. Tässä palvelussa toimitetaan näkymiä ainakin tietoturvapatauksiin asiakkaan ympäristössä, haavoittuvuuksiin, operatiivisen toiminnan tehokkuuteen sekä erilaisten sääntöjen, lakien ja määräysten noudattamisen toteutumaan.

Toimittaja ei myöskään määrittele esityksessään tarkemmin käytettävissä olevia teknisiä alustoja lokienhallinnan ja SIEM-ratkaisujen osalta. Materiaalissa todetaan keskitetyn lokienhallinnan olevan mahdollista ja suosituksena on tietoturvaan liittyvien lokilähteiden hallintaa SIEM-järjestelmää käyttäen. Operatiiviset lokit voidaan tuoda samalle alustalle, jossa toimii myös sovellus- ja palvelinvalvonta. Tämä nopeuttaa ongelmanratkaisuaikoja, kun kaikki tarvittava tieto on nopeasti saatavilla yhdestä keskitetystä paikasta.

Toimittaja tarjoaa mahdollisia ratkaisujaan kokonaispalveluna ja materiaalin perusteella ei ole mahdollista tilata pelkkää ratkaisutoimitusta oheispalveluineen. Toimittaja on keskisuuri IT-palvelutalo, jolla on toimintaa Pohjoismaiden lisäksi Keski-Euroopassa, joten tämän tyyppinen palvelumalli on heille tuttua ja materiaalin perusteella he ovat panostaneet myös kehitykseen tulevaisuuden tarpeita varten.

12.11 Toimittajamateriaalien yhteenveto

Toimittajien lähettämät ratkaisuehdotukset poikkesivat toisistaan huomattavastikin. Muutamalla toimittajalla oli vain lyhyt kuvaus heidän tarjoamistaan järjestelmistä ja palveluista, kun taas osa toimittajista laittoi hyvinkin kattavat kuvaukset alkaen itse teknisestä järjestelmästä aina palvelun SLA-raportointiin. Karkeana yleistyksenä voidaan päätellä, että mitä isompi tai pitempään alalla ollut toimija, sen kattavampi ja valmiimpi materiaali heillä oli tarjota. Toisaalta kyseessä on vasta teknisen vuoropuhelun alustus eikä varsinainen hankintatilanne, joten tietoja voidaan täydentää vielä toimittajien ja hankintayksikön välisissä keskusteluissa.

Osa kiinnostuneista toimittajista oli myös selkeästi painottunut toimittamaan lokienhallintaa ja SIEM-ratkaisuja. Heillä ei ollut tarjota ollenkaan ratkaisua herätehallintaan tai valvontaan tai asia oli huomioitu ilmoittamalla mahdollinen kumppanuus kolmannen osapuolen kanssa. Vaikka vaatimusmäärittelyssä toivottiin kokonaisratkaisua ja toimitusta yhden kumppanin kanssa, katsoimme parhaaksi kutsua myös näitä toimittajia tekniseen vuoropuheluun. Hankinnan tässä vaiheessa on edullista hankkia niin paljon tietoa eri ratkaisuista kuin mahdollista. Tämä auttaa myöhemmin myös itse varsinaisen hankinnan vaatimusmäärittelyn teossa.

Materiaalien perusteella kuitenkin sai hyvän yleiskuvan markkinatilanteesta ja erilaisista ratkaisuvaihtoehdoista. Vaihtoehdot näyttivät jakautuvan pääsääntöisesti niin, että joko toimittaja tarjoaa kokonaispalvelua, ratkaisutoimitusta tai asiakas voi valita näiden väliltä. Osa materiaalista sisälsi niin vähän informaatiota, että niiden perusteella ei voinut tehdä johtopäätöksiä kumpaankaan suuntaan ja joissain tapauksissa myös varsinainen tekninen kuvaus oli hyvin rajoittunutta.

Kokonaispalvelu olisi hankintayksikön resurssien kannalta paras vaihtoehto, koska tällöin koko palvelu ylläpitoineen ja hallintoineen tulisi toimittajalta. Toisaalta myös tämä vaihtoehto vaatisi tilaajan resurssien käyttöä kokonaisuuden toimintaan saattamisessa ja myöhemmin ylläpitovaiheessa. On myös oletettavaa, että tämä vaihtoehto on kallein kaikista mahdollisista, joskaan varmuutta ei voi saada ennen kuin varsinainen kilpailutus on pidetty ja tulokset hintatietoineen voitu tarkistaa.

Ratkaisutoimituksessa toimittaja rakentaa teknisen alustan vaadituilla ominaisuuksilla ja tarjoaa joko konsultointiapua tai tekee myös vaadittavat palvelumääritykset tilaajalle valmiiksi. Varsinainen

valvonta ja ratkaisun hallinta jäävät tilaajan vastuulle. Tämä vaihtoehto on lähimpänä sitä lopputulosta, mitä hankintayksikkö on tällä hetkellä hakemassa. Tämä on myös todennäköisesti kustannuksiltaan edullisempi kokonaispalveluun verrattuna.

Muutaman toimittajan materiaaleista selvisi myös, että seuraava trendi alalla tulee olemaan haavoittuvuussuojauspalveluiden lisääntyminen. Haavoittuvuussuojauksella tarkoitetaan tässä yhteydessä kykyä parantaa organisaation palvelinten ja tietoverkkojen tilaa erilaisia haavoittuvuuksia vastaan sekä suorittaa entistä tehokkaampaa valvontaa näiden osalta. Näitä palveluja oli tällä hetkellä tarjolla kahdella toimijalla.

Toimittajamateriaalien ja tapaamisten yhteydessä kannattaa myös arvioida kriittisesti opitun tiedon paikkansapitävyyttä. Myyntimateriaali on luonnollisesti koostettu niin, että oman tuotteen paremmuutta pyritään korostamaan ja näin ollen pelkästään näihin materiaaleihin ja tapaamisiin pohjautuvat päätökset saattavat johtaa epätoivottuun lopputulokseen. Vaikka tässä opinnäytetyössä ei tarkemmin käsitelty tiedon kriittistä arviointia, on siis syytä tehdä ristiin vertailua ja kokonaisarvion perusteella määritellä myös vaatimusmäärittely kilpailutusta varten, kuten myös arvioida kaikkea saatua tietoa.

13 TEKNINEN VUOROPUHELU

Kullekin tekniseen vuoropuheluun valitulle toimittajalle toimitettiin kutsu, jossa ilmoitettiin kiinnostus kuulla tarkemmin heidän tarjoamastaan ratkaisusta. Toimittajatapaamiset ajoitettiin kahden viikon ajanjaksolle niin, että kukin toimittaja sai ehdottaa itselleen parhaiten sopivaa päivämäärää. Jokaiselle toimittajalle oli varattuna kaksi tuntia aikaa, jonka aikana heidän tulisi ehtiä pitää oma esittelynsä. Tapaamisia varten valmisteltiin esitysdokumentti, jotta tarvittavat asiat olisi helpompi käydä järjestyksessä läpi. Tällä tavoin myös varmistetaan toimittajien yhdenmukainen kohtelu, jolloin kukaan ei saa etua toisiin nähden. Tapaamisissa syntyneet kysymykset kerätään yhteen ja niihin vastataan tapaamisen jälkeen niin, että jokaiselle toimijalle lähetetään kaikki kysymykset ja vastaukset.

Toimittajatapaamisissa käytiin läpi uudestaan hankinnan perusteet, miksi hankintaa ollaan tekemässä, millainen on toimintaympäristön nykytilanne ja millaista lopputulosta hankintayksikkö on tavoittelemassa.

Tapaamisissa oli mielenkiintoista havaita miten eri tavoin erilaiset yritykset esittelyjä tekevät. Osa yrityksistä saapui paikalle teknisen näkökulman kanssa, jolloin itse tuotteen esittely oli pääosassa ja sen toimintaa käytiin läpi hyvinkin tarkalla tasolla. Toisaalta useat yritykset saapuivat erillisen myyntihenkilöstön voimin, jolloin yleensä esitykset olivat erilaisten palveluiden ja palvelumallien esittelyä ja myös tuotteiden osalta havainnollistaminen tapahtui Powerpoint-diaesitysten avulla. Karkeana yleistyksenä voidaan arvioida, että mitä isompi yritys oli kyseessä, sen enemmän painotus oli myyntihenkilöiden osallistumisessa.

Periaatteessa toimittajien esityksien ydinkohdat olivat selvinneet jo aiemmin toimitetusta materiaalista, mutta varsinkin sellaisten yritysten kohdalla tuli paljon lisätietoa, joiden alustava materiaali oli hyvin yleisellä tasolla. Yleisesti ottaen tapaamisissa tuli jokaisen toimijan kohdalta lisää tarpeellista tietoa ja varsinkin mahdollisuus kysyä tarkentavia kysymyksiä ja keskustella kasvokkain auttoi paljon kokonaisuuden hahmottamisessa.

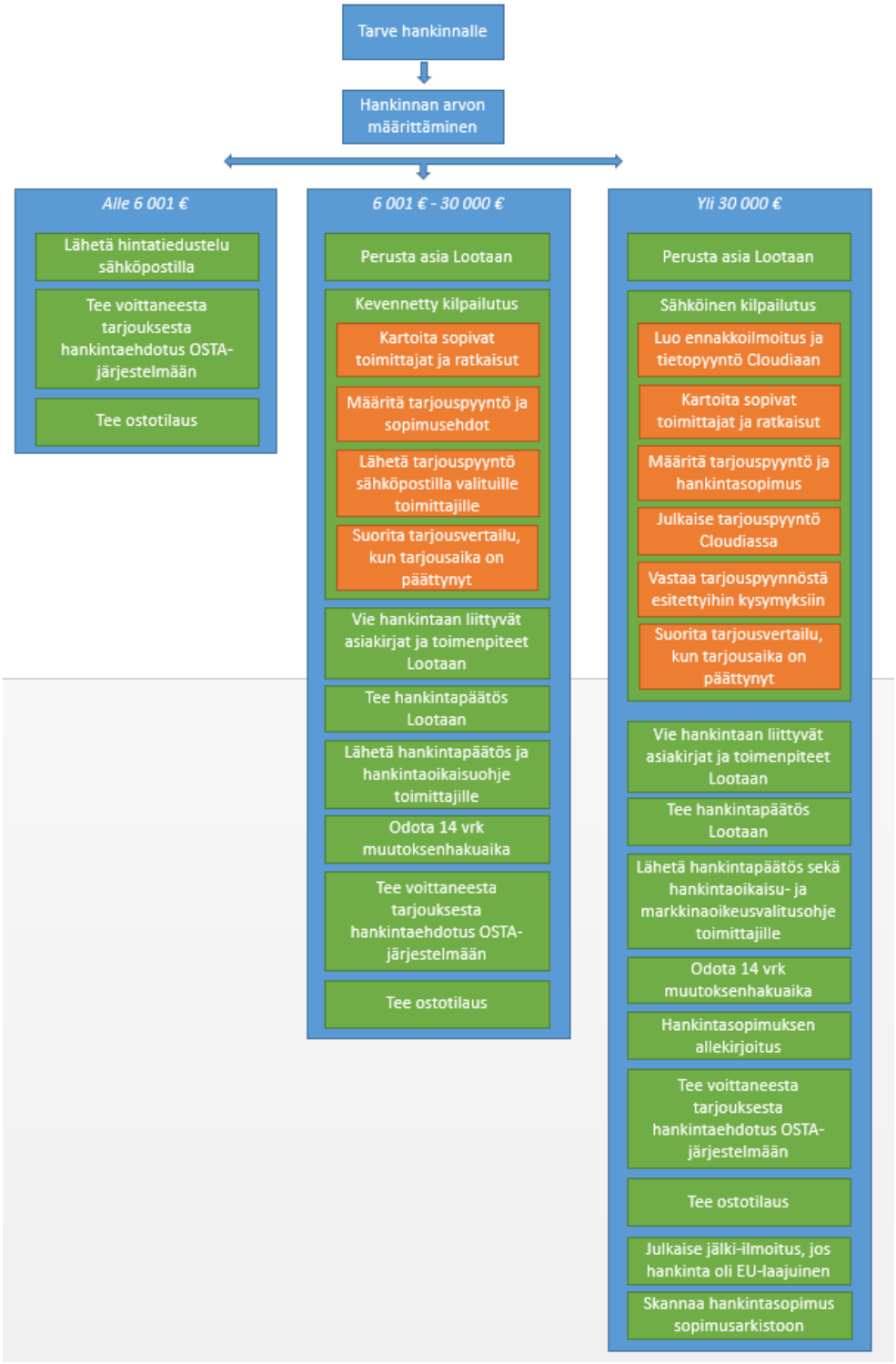
Tilaisuuksissa selvisi myös, että alkuperäisen materiaalin perusteella tehty arvio toimittajien jakaantumisesta palvelutoimittajiin ja kokonaisratkaisua toimittaviin piti hyvin paikkansa. Kuitenkin alustavien keskusteluiden perusteella palvelutoimitus ei välttämättä ole lopulta hintansa puolesta pois suljettu mahdollisuus.

Toimittajien osalta oli myös huomattavaa, että tarjottujen ratkaisujen hinnoittelumallit vaihtelevat jokaisen toimijan mukaan, joten on odotettavissa hankalaa vaatimusmäärittelyä kilpailutukseen. Osa ratkaisuista hinnoitellaan esimerkiksi SIEM-järjestelmän osalta skannattavien IP-osoitteiden perusteella, kun taas jotkut tuotteet maksavat tapahtumia sekunnissa -määritelmän perusteella. Tällöin lasketaan eri lokilähteistä tulevat tapahtumamäärät sekunnin aikana ja tämän perusteella tapahtuu tuotehinnoittelu. Joillakin toimittajilla oli myös datan määrään sitoutuva laskutusperiaate. Näiden lisäksi tulee myös vielä erilliset hinnoittelut palveluista, konsultointitehtävistä ja järjestelmien rakentamisesta.

14 JATKOTOIMENPITEET

Toimittajatapaamisten jälkeen projektityöryhmä kokoontuu yhteen keskustelemaan läpikäydyistä vaihtoehdoista ja tapaamisissa opituista asioista. Tässä vaiheessa aletaan myös tehdä varsinaista vaatimusmäärittelyä kilpailutusta varten. Koska tämä vaihe alkaa selkeästi vasta sen jälkeen, kun tämä opinnäytetyö on valmistunut, ei tässä voida ottaa sen tarkemmin kantaa vielä tähän prosessiin ja siihen, millaiseksi lopullinen haluttu järjestelmä ja palvelukokonaisuus muotoutuvat. On kuitenkin todennäköistä, että alustavaa ennakkotietopyyntöä tullaan käyttämään vahvasti pohjana ja sitä täydennetään tarpeen mukaan.

Hankintaprosessia varten on olemassa hyvin selkeät toimenpiteet, joiden avulla hankintaa tullaan jatkamaan. Nämä on kuvattu seuraavassa OTT:laisen hankintaoppaan hankintaprosesssikaaviokuvassa:



KUVA 9. Hankinnan eteneminen avoimena menettelynä sen arvon perusteella. (Oulun Tietotekniikka 2016b. Hankintaopas OTT:laiselle, 7.)

Varsinaisen vaatimusmäärittelyn täytyy olla hyvin tarkasti kuvattu ja yksiselitteinen kaikille toimittajille, joten tätä vaihetta varten kysytään mielipidettä ja ajatuksia Oulun Tietotekniikan asiantuntijoilta, jotka ovat tulevan järjestelmän kanssa tekemisissä tai voivat määrittelyn

muodostamiseen omalla osaamisellaan tuoda lisäarvoa. Projektin ydinryhmä muodostaa näistä läpikäydyistä asioista lopullisen kilpailutusmateriaalin, jonka arvioitu valmistumisajankohta on tammikuun loppupuolella 2017. Vaatimusmäärittelyn jälkeen kilpailutus julkaistaan sähköisessä hankintajärjestelmä HILMAssa ja varsinainen kilpailutusprosessi voi alkaa. Toimittajavalinnan jälkeen, ja mikäli vaaditun valitusajan aikana ei tule valituksia, allekirjoitetaan sopimukset toimittajan kanssa. Tämän jälkeen voidaan aloittaa varsinainen järjestelmän ja palvelun rakentaminen.

Riippuen valittavasta toimittajasta ja sopimuksen sisällöstä, on tarkoituksena päästä rakentamaan hankinnan mukaista kokonaisuutta keväällä 2017. Varsinkin lokienhallinnan ja lokipolitiikan osalta on odotettavissa, että määrittelytyö tulee kestämään useampia kuukausia. Lokipolitiikan määrittelyn jälkeen voidaan aloittaa SIEM-ominaisuuksien liittäminen mukaan. Ennakoitu valmistumisaika tälle työlle on loppuvuodesta 2017 ja samalla voidaan katsoa projekti läpiviedyksi. Alustavassa suunnitelmassa on myös määritelty, että projektin valmistumisen jälkeen jatkotoimenpiteenä lisätään asiakasrajapinta valvontajärjestelmään.

Asiakaskohtaisten näkymien osalta tuotetta pyritään tekemään niin, että se olisi houkutteleva ainakin isoimmille Oulun Tietotekniikan asiakkaille. Tällöin tuotteen pitäisi pystyä tarjoamaan heille sellaista lisäarvoa, josta he olisivat valmiit maksamaan ja kokisivat saavansa siitä varsinaista hyötyä. Tämän määrittelyn osalta avuksi otetaan organisaation muita palvelulinjoja, jotka tekevät paljon yhteistyötä suoraan asiakkaiden kanssa. Yhteistyössä heidän kanssaan voidaan tehdä markkinakartoitusta ja selvittää asiakkaiden tarpeita ja kiinnostusta tällaiseen palveluun. Mikäli kiinnostusta on riittävästi, tuotteistetaan palvelu. Kun asiakas haluaa tilata tällaisen omalle organisaatiolleen räätälöidyn järjestelmän, on siitä silloin olemassa valmiina selkeät palvelukuvaukset, hinnoittelumallit ja ohjeistukset. Tämän jälkeen palvelu tuotetaan yksilöllisesti asiakkaan kanssa yhteistyössä.

Hankinnan edetessä tullaan myös tiedottamaan omaa organisaatiota hankkeen tilasta ja eri valmistumisen asteista. Kun esimerkiksi herätehallinta- ja valvontakomponentit saadaan käyttöön, järjestetään siitä koulutus koko henkilökunnalle. Ratkaisun on tarkoitus palvella kaikkia OTT:n työntekijöitä ja projektin puitteissa myös huolehditaan siitä, että tämä onnistuu mahdollisimman hyvin. Tarkoituksena on myös rakentaa ympäristö niin, että kun organisaatio tuottaa uusia palveluita ja teknisiä ratkaisuja, niiden lisääminen valvontaan ja lokitukseen sujuu automaattisesti ennalta määritettyjen prosessien avulla.

15 POHDINTA

Tämä opinnäytetyö ja siihen liittyvä kehittämistehtävä oli Oulun Tietotekniikan IT-palvelutuotannon laadun ja toimintavarmuuden kehittäminen hankkimalla ulkopuoliselta toimijalta kyberturvallisuuden kokonaisratkaisu. Jotta hankinta onnistuisi, tulisi sitä varten hankkia ensin riittävästi tietoa sekä julkisten hankintojen toteuttamisesta että myös itse hankinnan kohteesta kaikkine siihen liittyvine asioineen. Jotta hankinta saataisiin dokumentoitua ja varmistettua sen sujuva eteneminen, päätettiin se tehdä projektimuotoisena. Projektilla täytyy olla selkeä alku ja loppu, sekä kuvaukset ja määritykset mitä se pitää sisällään. Huolellinen projektin viitekehyksen ja tavoitellun ratkaisun selkiyttäminen helpottaa itse hankintatapahtumaa ja vaatimusmäärittelyn jäsentelyä kilpailutusta varten.

Kehittämistehtävän tavoitteet jaettiin kahteen eri osaan:

1. opinnäytetyön tekijän kyvykkyyden ja tiedon lisääminen palveluhankinnasta ja hankintakohteesta
2. kyberturvallisuusratkaisujen hankintaprojektin aloittaminen.

Hankintaprojektin pitkäkestoisuuden vuoksi opinnäytetyön osalta ei voitu määrittää tavoitteita sisältämään koko hankintatapahtumaa, vaan pääkohteeksi asetettiin riittävän tietoperustan omaksuminen ja itse hankinnan käynnistäminen, jolloin tehtyjä toimenpiteitä voitaisiin dokumentoida opinnäytetyöhön niin pitkälle kuin mahdollista.

Työelämässä on harvoin mielekästä tai mahdollista käyttää perinteisen tutkimuksen menetelmiä. Nämä menetelmät soveltuvat paremmin teoreettisen tiedon etsimiseen ja tutkimiseen sekä tieteenfilosofisten kysymysten metsästämiseen. Tämän vuoksi menetelmäksi tätä opinnäytetyötä varten valikoitui tapaustutkimus, joka määritelmänsä mukaan pitää sisällään ajatuksen tiedon konkreettisesta hyödyntämisestä, projekti- ja prosessiluonteisuudesta sekä kehittämisen kohteen syvällisestä ymmärtämisestä. Myös tapaustutkimuksen ajatuskehitelmä oman työn mukautuvaisuudesta työn edetessä, evaluoivan kehittämisen lähtökohta ja ekstensiivinen tutkimusmetodiikka sopivat erittäin hyvin, kun tehdään vertailua useiden eri toimittajien ratkaisujen välillä suhteessa omaan vaatimusmäärittelyyn.

Opinnäytetyö aloitettiin keskustelemalla Oulun Tietotekniikan johdon kanssa sopivasta tavasta kehittää hallintakeskuksen toimintaa. Opinnäytetyön tekijällä oli jo pitempään ollut tarve saada työnsä luonteen vuoksi parempi käsitys teknisen tilan terveydentilasta. Keskusteluissa todettiin

tämän sopivan hyvin yhteen OTT:n kehittämissuunnitelmien kanssa, joten hankinnan katsottiin olevan hyvin linjassa molempien osapuolten tavoitteiden kanssa.

Alkuun tietoperustaa kartutettiin tutustumalla hankintakäytäntöihin ja keskustelemalla toisen organisaation edustajan kanssa, jolla oli meneillään samanlainen hankinta. Tavoitteiden, tiedon ja yleisen ymmärryksen lisääntyessä hanke päätettiin tehdä projektina ja projektisuunnitelman valmistuttua huomattiin yhteenvetopalaverissa, että hankintaan voisi hyvin yhdistää lokienhallinnan ja tietoturvaratkaisut, koska myös niille on käytännön tarve koko organisaation osalta. Projektille luotiin työnimi Kyberturvallisuusratkaisut 2017, jonka alaisuudessa lähdettiin muodostamaan tietopyyntöä eri toimittajien kartoittamiseksi ja tiedon lisäämiseksi markkinoilla olevista ratkaisuista.

Tietopyynnön julkaisun jälkeen kiinnostuneista toimittajista kutsuttiin osa käymään tarkempaa teknistä vuoropuhelua ja esittelemään omia ratkaisujaan. Tämä on myös projektin vaihe, johon tämä opinnäytetyö päätetään. Projekti kuitenkin jatkuu kuten on suunniteltu ja tavoitteena on saada Oulun Tietotekniikalle parhaiten sopiva kokonaisuus.

Voidaan todeta, että hankkeen alussa opinnäytetyölle määritettyihin tavoitteisiin on päästy. Sekä opinnäytetyön tekijän tietoperusta, ymmärrys ja osaaminen on lisääntynyt riittävästi, jotta hankintaa voidaan jatkaa ja lisäksi hankintaprosessi on aloitettu ja se etenee jouhevasti eteenpäin.

Kyberturvallisuusratkaisuja ei ole syytä hankkia niiden itseisarvon takia. Arvokaskaan järjestelmä ja palvelu eivät tuota lisäarvoa tai auta organisaatiota, mikäli sen oikeaa tarkoitusta ja arvoa ei sisäistetä. Vaikka hankinta suoritettaisiin kokonaispalveluna, on yrityksellä syytä olla riittävästi osaavaa henkilöstöä, joka osaa kehittää ja tarpeen vaatiessa säätää järjestelmän toimintaa. Oikein määritettynä järjestelmät auttavat proaktiivisessa häiriövarautumisessa ja tietoturvan parantamisessa paljon, mutta ilman tarkkaa käsitystä käyttötarkoituksesta jää sen potentiaali helposti hyödyntämättä. Jotta Oulun Tietotekniikalla saataisiin ratkaisuista kaikki tavoiteltu hyöty irti, täytyy sen käyttämiseen kouluttaa ja opettaa henkilökuntaa ja määritellä heti käynnistysvaiheessa käyttöönottoprosessi, jonka avulla saadaan tuotua sekä entiset järjestelmät mutta myös tulevaisuudessa uudet palvelut onnistuneesti mukaan seurantaan ja lokituslähteiksi. Ihmisten kouluttaminen ja ymmärryksen lisääminen ovat oleellinen osa onnistunutta kokonaisuutta.

Useamman toimittajan ja nettilähteen perusteella voidaan lopuksi vielä kärjistetysti todeta, että on olemassa kahdenlaisia yrityksiä: niitä, joiden järjestelmiin on murtauduttu ja niitä, jotka eivät vielä tiedä, että heidän järjestelmiinsä on murtauduttu.

LÄHTEET

Anttila, P. 2007. Realistinen evaluaatio ja tuloksellinen kehittämistyö. Hamina: Akatiimi Oy

AXELOS Limited 2014. ITIL Continual Service Improvement. 2011 Edition. TSO:London

AXELOS Limited 2014. ITIL Service Design. 2011 Edition. TSO:London

AXELOS Limited 2014. ITIL Service Operation. 2011 Edition. TSO:London

AXELOS Limited 2014. ITIL Service Strategy. 2011 Edition. TSO:London

AXELOS Limited 2014. ITIL Service Transition. 2011 Edition. TSO:London

Elinkeinoelämän keskusliitto. 2016. Julkiset hankinnat. Viitattu 24.10.2016, https://ek.fi/mita-teemme/yrityslainsaadanto/julkiset-hankinnat/

Eriksson, P. & Koistinen, K. 2005. Monenlainen tapaustutkimus. Helsinki: Kuluttajatutkimuskeskus

FiCom ry. 2016. Kyberympäristö ja kyberturvallisuus. Viitattu 23.10.2016, http://www.ficom.fi/linked/fi/ohjeita/Kyber_esite_WEB.pdf

Harris, S. 2005. CISSP® All-in-One Exam Guide, Third Edition. TSO:Emeryville

Helpnetsecurity. 2016. Dyn DDoS attack: The aftermath. Viitattu 28.10.2016, https://www.helpnetsecurity.com/2016/10/24/dyn-ddos-attack-aftermath/?utm_source=dlvr.it&utm_medium=twitter

HILMA. 2016a. Kynnysarvot. Viitattu 24.10.2016, https://www.hankintailmoitukset.fi/fi/docs/kynnysarvot/

HILMA. 2016b. Tervetuloa HILMAn sivuille!. Viitattu 1.11.2016, https://www.hankintailmoitukset.fi/fi/

itSMF Finland Ry. 2016. ITIL ja Parhaat käytännöt. Viitattu 19.10.2016, http://itsmf.fi/itil-parhaat-kaytannot/

Kaupunginhallitus. 2013. Oulun kaupungin hankintakäsikirja

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy

MalwareTech Twitter. 2016. Mirai infections map. Viitattu 6.11.2016, https://twitter.com/MalwareTechBlog/status/790202102530318336

Marty, R. 2007. Event Processing – Normalization. Viitattu 28.10.2016, http://raffy.ch/blog/2007/08/25/event-processing-normalization/

Millog. 2015. Palvelujen elinkaaren prosessit ITIL:n mukaan. Viitattu 12.11.2016, http://docplayer.fi/4856222-Sap-sovellushallinta-kayttopalvelu-ja-kehitysratkaisut.html

Nixu. 2016. Tietoturvatiedon ja tapahtumien hallinta (SIEM). Viitattu 7.11.2016, https://www.nixu.com/fi/palvelualueet/tietoturvatiedon-ja-tapahtumien-hallinta-siem?gclid=CJjbt6fAI9ACFU5eGQodV3EGQg

Ojasalo, K., Moilanen T. & Ritalahti, J. 2014. Kehittämistyön menetelmät. Helsinki: Sanoma Pro Oy

Oulu Tietohallinto. 2013. Oulun kaupungin tietoturvapolitiikka

Oulun Tietotekniikka. 2016a. Palveluluettelo

Oulun Tietotekniikka. 2016b. Hankintaopas OTT:laiselle

Oulun Tietotekniikka. 2016c. Tietopyyntö

Oulun Tietotekniikka liikelaitos Toimintakertomus. 2015, 2015

PTCServices. 2016. Hankintadirektiivien uudistus. Viitattu 25.10.2016, http://www.ptcs.fi/fi/direktiiviuudistus

Rousku, K. 2014. Kyberturvaopas. Sähkökirja: Talentum Media Oy

Secmeter. 2016. Forensiikka. Viitattu 28.10.2016, https://www.secmeter.com/turvatieto/forensic_prosessi.html

Securosis. 2010. Understanding and Selecting a SIEM/LM: Correlation and Alerting. Viitattu 28.10.2016, https://www.securosis.com/blog/understanding-and-selecting-a-siem-lm-correlation-and-alerting

Suomen Internetopas. 2016. Tietoturva. Viitattu 27.10.2016, http://www.internetopas.com/yleistietoa/tietoturva/

Suomen rikoslaki. 2016. Asetus tietomurrosta. Viitattu 23.10.2016, http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

TechRebublic. 2011. How to choose a SIEM solution: An overview. Viitattu 28.10.2106 http://www.techrepublic.com/blog/it-security/how-to-choose-a-siem-solution-an-overview/

tivi. 2016. Kyberisku pudotti kokonaisen valtion verkosta. Viitattu 4.11.2016, http://www.tivi.fi/Kaikki_uutiset/kyberisku-pudotti-kokonaisen-valtion-verkosta-6596641

Työ- ja elinkeinoministeriö. 2016b. Hankintalain kokonaisuudistus – Siirtymävaiheen toimenpiteet ja järjestelyt. Viitattu 25.10.2016, http://tem.fi/documents/1410877/2132242/Hankintalain+kokonaisuudistus+-+siirtym%C3%A4vaiheen+toimenpiteet+ja+j%C3%A4rjestelyt/d42cc677-8dcd-4c8a-a6b1-6a7b93678273

Työ- ja elinkeinoministeriö. 2016a. Hankintalainsäädännön kokonaisuudistus. Viitattu 25.10.2016, http://tem.fi/hankintalain-kokonaisuudistus

Viestintävirasto. 2016. Lokien keräys ja käyttö. Viitattu 28.10.2016. https://www.viestintavirasto.fi/attachments/tietoturva/Lokitusohje.pdf

Yhteiskunnan turvallisuus. 2013. Suomen kyberturvallisuusstrategia. Viitattu 20.10.2016, http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit