Näkökulmia tietojärjestelmien monitorointiin

Puurula, Risto

2019 Laurea

Laurea-ammattikorkeakoulu

Näkökulmia tietojärjestelmien monitorointiin

Näkökulmia tietojärjestelmien monitorointiin

Risto Puurula
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
05, 20192019

Laurea-ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Tiivistelmä

Näkökulmia tietojärjestelmien monitorointiin

Vuosi 2019 Sivumäärä 64

Tämän opinnäytetyön tavoitteena on jäsentää ja tutkia laaja-alaisesti työn kontrollia, prosessien ja tietojärjestelmien monitorointia ja valvontaa, työkalujen kyvykkyyksiä tutkien sekä pohtia kohtaavatko valvonnan ja monitoroinnin tarve sekä tarjolla olevien työkalujen ominaisuudet muuttuvassa liiketoimintaympäristössä sekä operatiivisessa työskentelyssä.

Työn toimeksiantajana on kansainvälisesti toimiva IT-alan yritys ja kyseessä on kehittämistehtävä. Työn tuloksia tullaan hyödyntämään yleisesti erilaisten monitorointi, ja valvontaratkaisuiden kehityksen kanssa.

Lopputyön laadullinen tutkimus toteutettiin asiantuntijoiden teemahaastatteluiden muodossa. Haastateltavat asiantuntija ovat kohdeyrityksen eri teknologia-alueiden syväasiantuntijoita ja haastattelut suoritettiin haastateltavien työpaikoilla.

Lopputyötä tehdessä selvisi, osin oletetustikin, etteivät tämänhetkiset, käytössä olevat monitorointi, ja valvontatuotteet sekä työkalut palvele kokonaisarkkitehtuurin mukaista kokonaisvaltaista tietojärjestelmien toimintaan vaikuttavien osien valvontaa riittävästi liiketoiminnallisesta näkökulmasta. Eri monitorointivälineiden, arkkitehtuurikerrosten, eri toimittajien välillä ja toimesta tapahtuva, useimmiten toisistaan irrallinen monitorointi sekä valvonta lisää viiveitä tietojärjestelmien häiriötilanteiden selvittämisen kanssa, etenkin usean toimittajan ratkaisuissa. Lisäksi muuttuneet palvelutuotantomallit (mm. Pilvi) sekä tietoturvan korostuminen muuttavat painopistettä monitoroinnin, valvonnan ja niihin liittyvän työn alueilla. ICT-ala itse tarvitsee automatisointia, sopimuksellista läpinäkyvyyttä, toimialakohtaista standardointia sekä myös kokonaan uusia käytäntöjä sovellusten sekä konfiguraatio-osien monitorointiin ja valvontaan

Lopputyön tulokset vahvistivat odotetusti käsitystä nykyisistä monitorointi- ja valvontaratkaisuista, mutta avasi myös kokonaan uusia näkökulmia kirjallisuutta ja työn kontrollin tarvetta peilaten. Lisäksi työn tuloksena syntyi johtopäätöksiä ja kehitysehdotuksia, jotka esitellään omassa kappaleessaan.

Asiasanat: Tietojärjestelmät, ITSM, Monitorointi

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

Risto PuurulaRisto Puurula

Viewpoints on IT-System Monitoring

Year 2019 Pages 64

The primary objective of this study was to approach the control of work, processes and business system monitoring and to find out if the current set of applications in use for this purpose meets the requirements of the changing business environments and run-time system work.

The work was done for an international IT-company as a development study. The results of the study will be used in general for different monitoring and control solutions related development within the company. The study was conducted as a qualitative research by analysing related literature and by semi-structured interviews of experienced experts on different enterprise architectural levels and related IT-service production units and functions. The Interviews were held at the workplace within several different sessions during 2017.

During the study it was- partly as expected – found, that the current set of tools in use for monitoring and control of the IT-systems are not fit for the purpose and adequate for the full scope of systems monitoring. When looking from the perspective of enterprise architecture, all the separate layers are monitored and controlled by a specific group of experts representing specific areas expertise. Full IT-system monitoring was rarely done, and most customers business systems were in all monitored by many separate layers and companies with different set of tools. This causes unnecessary delays with service restoration in blackout situations as the whole picture of the situation is in most cases either non-existing or not available for all the parties involved. In addition to this the changing business models (e.g. Cloud) and security requirements are rapidly changing the need for monitoring and control in all.

As a conclusion of the study I see that the whole IT-industry needs automation, transparency, standardization and all new practices and tools for monitoring customer IT systems; it´s components, dependencies and value chains within production.

The results of the study were as expected and verified the current understanding of the situation in all, but also gave new insights, conclusions and ideas for the development and the future use of these tools.

Keywords: IT-Systems, ITSM, System monitoring

Sisällys

1 Johdanto 9
2 Työn lähtökohdat 9
2.1 Kohteen kuvaus 9
2.2 Tutkimuskysymykset 9
2.3 Aiheen rajaus 10
2.4 Tutkimuksen kysymykset 10
3 Monitorointi ja valvonta yleisesti 10
3.1 Työn monitorointia vai Tietojärjestelmien monitorointia 11
3.2 Tietojärjestelmien valvontamekanismeja 13
3.3 Sovelluksenvalvontajärjestelmä (APM) 15
4 ITIL Viitekehys ja monitorointi 16
4.1 Tietojärjestelmän monitoroinnin ja valvonnan tarkoitus 17
4.2 Raportointi, monitorointi ja kontrolli 17
4.3 Monitorointi ja valvonta ITIL Viitekehyksessä 18
4.4 Herätteidenhallinta 18
4.5 Palveluomaisuuden hallinta ja konfiguraationhallinta 19
4.6 Jatkuva palveluiden parantaminen 20
4.7 Tilannekuva ja Perustason/Lähtötason mittaaminen 21
5 EA-näkökulma valvontaan ja monitorointiin 22
5.1 Kokonaisarkkitehtuurin ajonaikainen monitorointi 23
5.2 Palveluiden käyttäjien kategorisointi 24
5.3 Yleisimmät pilvipalveluiden palvelumallit 24
6 Menetelmäosuus 24
6.1 Laadullinen eli kvalitatiivinen tutkimus 25
6.2 Fenomenologinen tutkimus 25
6.3 Aineistonhankintamenetelmät 25
6.4 Reliabiliteetti ja validiteetti 26
7 Haastattelututkimus 26
7.1 Haastatteluiden tulokset 27
7.2 Haastatteluiden yhteenveto 27
8 Näkökulmia monitoroinnin kehittämiseksi 29
8.1 Tilaajan ja toimittajan välinen yhteistyö 32
8.2 Monitoimittajaympäristöt 32
8.3 Monitorointi ja valvonta kehikon hahmottelua 34
8.4 Goal Directed Design, ”Personat” 35
8.5 Hierarkia, rakenneosat ja holistinen näkymä 37

8.6 Kontrollihuone 39
8.7 Kontrollihuoneessa seurattavat kohteet 39
9 Yhteenveto 40
10 Pohdintaa 41
10.1 Monitoroinnin ja valvonnan tulevaisuus 42
10.2 Monitorointi, koneoppiminen ja tekoäly (Artificial Intelligence, AI) 43
11 Johtopäätökset 48
12 Jatkotutkittavaa 49

1 Johdanto

Tämä lopputyö koostuu kahdestatoista erillisestä osasta. Ensimmäisessä osassa, johdannossa, kerron taustaa siitä, miksi olen valinnut lopputyöni aiheeksi: Näkökulmia tietojärjestelmien monitorointiin. Toisessa osassa kerron työni lähtökohdista. Kolmannessa, neljännessä ja viidennessä esittelen lukijalle aihealueen keskeistä käsitteistöä. Kappaleissa kuusi – yhdeksän keskityn menetelmiin ja tehtyyn tutkimukseen. Yhdeksännessä kappaleessa on yhteenvetoosio, jossa käsittelen haastattelujen sekä tietoaineiston pohjalta valvonnan ja monitoroinnin epäkohtia sekä vastauksia ensimmäisessä luvussa esitettyihin kysymyksiin sekä yleisellä tasolla päätelmiä ja kehitysehdotuksia näihin. Kappaleissa kymmenen – kaksitoista käyn laajempaa pohdintaa aihealueesta, esittelen johtopäätöksiä sekä mahdollisia jatkotutkimusaiheita.

2 Työn lähtökohdat

Oma motivaationi valittuun aiheeseen liittyy havaintoihin ja kokemuksiini 20 vuoden ajalta IT yrityksien, Internetin ja tietojärjestelmien parissa. Kärjistäen voisi sanoa, että mitä kattavammin monitorointi on rakennettu ja mitä paremmin operatiivinen henkilökunta osaa tätä työkaluna käyttää, sitä nopeampaa on virhe- ja häiriötilanteista toipuminen. Monitoroinnista keskustellessa kuitenkin olen havainnut monenlaista risteävää ymmärrystä siitä, mitä monitoroinnilla ja valvonnalla tarkoitetaan, ja miksi sitä tulisi tehdä.

2.1 Kohteen kuvaus

Tutkimuksen toimeksiantajana on kansainvälinen IT-alalla toimiva yhtiö; konesali- ja kapasiteettipalveluiden palveluyksikkö. Yksikkö tuottaa konesali- ja kapasiteettipalveluita asiakkailleen. Palveluita sekä näitä tuottavia teknologiaryhmiä on runsaasti, joista jokaisella on oma alakohtainen termistönsä sekä vuosikymmenten aikana hioutuneet käytännöt tuotannon ylläpitämiseksi. Monitorointi ja valvonta on kuitenkin yhdistävä tekijä, sillä usein asiakkaiden palvelukokonaisuuksiin liittyy useita eri teknologia-alueita ja monitoroinnin avulla on mahdollista saada asiakas tai loppukäyttäjän kokema näkyviin reaaliaikaisesti. Monitoroinnin ja valvonnan kehittämiseen on kuitenkin yhtä monta mielipidettä ja tahtotilaa, kun on palvelua tuottavia ryhmiä ja asiantuntijoita. Tässä katsauksessa pyrin etsimään haastatteluiden ja teoria- sekä palvelutarjontakatsauksen avulla yhteistä maaperää sekä tahtotilaa aihealueeseen liittyen.

2.2 Tutkimuskysymykset

Katsauksen tulisi vastata mm. seuraaviin kysymyksiin: Minkälaisia haasteita ja toiveita on ylläpitotyötä tekevällä henkilöstöllä valvontanäkymiä kohden? Miten ITIL kirjaston parhaiden käytäntöjen mukaisesti ja tarjolla olevien sovellusten avulla monitorointi- ja valvontanäkymät jäsentyvät kokonaisvaltaisesta näkökulmasta? Millaisin periaattein tulisi kokonaisvaltainen

tuotannon seuranta- ja kontrollinäkymä rakentaa useista eri teknologioista, toimittajista, tietojärjestelmistä ja arkkitehtuureista koostuvaan kokonaisuuteen? Kuinka moniulotteinen tehtävä monitoroinnin ja valvonnan kokonaisuus ylipäätänsä on?

2.3 Aiheen rajaus

Vaikka tutkittavalta alueelta olisi saatavilla hyvin runsaasti numeraalista, mitattavaa dataa kvantitatiivisen tutkimuksen materiaaliksi, tarkastelen monitorointia ja valvontaa asiantuntijoiden kokemusperäisenä, työnkulun kannalta oleellisena tietotaitona, sekä rakenteellisena holistisena kokonaisuutena. Monitoroinnin tuottamaa dataa syntyy aihealueelta nykyisin kuormituksellisesti jopa liikaa, ja tämän tutkimuksen tarkoituksena on selvittää haastatteluiden ja kirjallisuuden avulla, sekä tehtävän järjestelmäylläpitotyön kannalta kunkin alueen kokemusperäisiä haasteita nykyisissä työtehtävissä sekä kartoittaa tulevia tarpeita.

Työhön liittyy paljon toimialakohtaista sanastoa, sekä vielä suomenkieliseksi vastineiksi vakiintumatonta termistöä, jota en ole lähtenyt itse kääntämään, jotta sanojen merkitys ei muuttuisi. Keskeinen käsitteistö ja termistö esitellään liitteessä 4.

2.4 Tutkimuksen kysymykset

Informaatioteknologian maailmassa Pilvi-palvelun (Cloud) tarjoajan tai runkoverkon häiriön ollessa sovellustoimittajan palvelupäällikölle näkymätön, on palvelupäällikkö vaativan ongelmanratkaisun edessä; tietojärjestelmän käyttäjän kokema virhetilanne on ”jossain”. Loppukäyttäjä kokee ongelman järjestelmän käytössä, joka estää järjestelmän avulla tehtävän liiketoimintatapahtuman. Ongelman aiheuttaja taas saattaa olla missä tahansa käyttäjän päätelaitteen ja sähköntuotantoverkon välillä, mutta realisoituu viimekädessä huonona käyttökokemana. Mitkä ovat olennaiset tietosyötteet sekä impulssit? Miten tulisi valita seurattavat kohteet erilaisista tietojärjestelmäkokonaisuuksista? Millainen on valvonnan ja monitoroinnin tulevaisuus?

3 Monitorointi ja valvonta yleisesti

Työtä on monitoroitu läpi aikojen. Työn ensin koneistuessa, sitten automatisoituessa, myös työn seurannalle on tapahtunut vastaavasti. Yleistäen tietojärjestelmien automaattisen monitoroinnin ja valvonnan perimmäisenä tarkoituksena on varmistaa työn ja liiketoiminnan sujuva kulku. Ennen tietotekniikan esiinmarssia vastaavaa työn seurantaa suorittivat esimiehet, joiden tehtävänä oli varmistaa ja seurata alaistensa työtä sekä työn tehokkuutta. Työn ja työsuoritteen tehokkuuden kasvaessa koneistamisen ja tietotekniikan avulla, myös valvontatyö siirtyi ensin koneistetuksi sekä sittemmin tietotekniikan suorittamaksi (Zuboff 1990, 25 - 29). Vaikka keskityn työssäni kuvaamaan nykyisiä tietotekniikan ajan ja maailman monitorointi-

sekä valvontaratkaisuja, otan silloin tällöin laajemman näkökulman esiin. Seuraavissa kappaleissa käyn lävitse ja esittelen lyhyesti viitekehyksien ja parhaiden käytäntöjen mukaista käsitteistöä monitorointiin ja valvontaan liittyen.

3.1 Työn monitorointia vai Tietojärjestelmien monitorointia

Verrattaessa teollisen aikakauden tehdastyön kontrollin ja valvonnan haasteita ja ATK:n esiinmarssia (Zuboff 1990) nykyisiin informaatioteknologian aikakauden valvontahaasteisiin, nousee esiin mielenkiintoisia yhtäläisyyksiä sekä eroja. Esimerkiksi, siinä missä aiemmin valvonta tapahtui tehtaan työskentelytilan valvontasillalta käsin ja sittemmin kontrollihuoneesta, josta Zuboff kuvaa aikakauden siirtymää manuaalisesta lähtötilanteesta tietokoneavusteiseksi ja prosessiohjatuksi työksi, on nykyisissä tietojärjestelmissä valvottavat kohteet ”piilossa” ja usein vain lopputulos on konkreettisesti näkyvillä. Valvontasillat tai tehtaan kontrollihuone välkkyvine seinäpaneeleineen on muuttunut tietokoneen ruuduksi, sekä monien toimittajien muodostamien arvoketjujen monitorointiketjuiksi.

Nykyisille tietojärjestelmille on ominaista niiden monikerroksellisuus; alkaen sähköntuottamisesta, tietoliikenneverkkoihin ja kaapeleihin, konesaleihin, kytkimiin, reitittimiin, klustereihin, erityyppisiin palvelimiin, käyttöjärjestelmiin, liiketoimintasovelluksiin ja viimeisenä ihminen näiden operoijana. Ajatus siitä, että valvontaa suorittaisi jokaisen osakomponentin kohdalla - kaleerin kapteenin kaltaisesti yksittäinen ihminen - olisi konesalit täynnä yksittäisten komponenttien valvontaa suorittavia henkilöitä. Järjestelmien kokoluokan kasvaessa kasvaa myös niiden kompleksisuus. Lisäksi tätä osaltaan monimutkaistaa tietojärjestelmäpalveluiden nykyinen tuotantomalli ja/tai ostomalli, jossa tietojärjestelmien tarvitsemat palvelut ostetaan useimmiten kerroksittain usealta eri toimittajalta, joka johtaa usein kokonaisuuden hallinnan pirstaloitumiseen ja kontrollin lisääntyvään heikkenemiseen.

Gorton esittelee artikkelissaan tietojärjestelmien kasvun myötä esiin tulevia piirteitä, mm. seuraavasti: järjestelmien koon kasvaessa kasvaa myös tietojärjestelmien applikaatioiden sekä fyysisten komponenttien häiriöiden määrä. Toisena piirteenä Gorton mainitsee järjestelmien koon myötä kasvavan kompleksisuuden, joka puolestaan tekee häiriönkohdistamisesta haastavampaa. Järjestelmien koon kasvaessa, komponenttien vikaantuminen on todennäköisempää ja siihen tulisikin suhtautua uutena ”normina” ja tästä syystä applikaatiot tulisi rakentaa viankestäviksi ja niin, että ne käsittelevät vikatilanteita oikein. Ratkaisuna tähän Gorton esittelee 4-portaisen mallin havainnointidata-pinosta (Observability Stack), jossa ensimmäisenä vaiheena on datan keruu, toisena vaiheena datan yhdistäminen/aggregointi, kolmantena datan tallennus ja neljäntenä datan analysointi. Lisäksi Gorton nostaa esiin huomiona

sen, että sovelluksen skaalautumisen myötä syntyvät ongelmat voivat nousta esiin järjestelmän omissa sovelluskomponenteissa tai kolmansien osapuolten komponenteissa. ”Et voi hallita sitä mitä et monitoroi” (Gorton 2014.)

Palvelutoimittajalla on yleensä oma Service desk ja palveluorganisaatio teknologia- sekä asiantuntijatasoineen ja näillä monitorointi- ja valvontajärjestelmänsä – mutta, useimmiten ilman keski-näistä, edes sopimuksellista, relaatiota toisten toimittajien kanssa. Järjestelmien toimittajaintegraatiota harvoin suunnitellaan monitorointi- ja valvontaratkaisuihin muilta osin kuin yksittäisten liiketoimintaprosessien valvonnan osalta. Miten siis saadaan rakennettua valvontapaneeli tai kontrollimekanismit järjestelmään, jota tuottaa useat eri tahot, joilla ei näennäisesti ole tekemistä toistensa kanssa?

Tietojärjestelmien arkkitehtuuri esittää tyypillisesti tietojärjestelmän kokonaisrakenteen, siihen liittyvät komponentit ja näiden väliset tietovirrat. Tätä loogisen tason järjestelmäkuvausta tarkennetaan monilla erilaisilla täydentävillä kuvauksilla järjestelmän elinkaaren eri vaiheissa. Tuotantovaiheessa näitä ovat mm. RACI-kuvaukset, joissa sovitaan toimittajavastuista, kuten mm. konesali- ja tietoliikennepalveluiden, sovellushallintapalveluiden tehtävät. Järjestelmän omistavan taho ostokäyttäytymisen vuoksi toimittajien välinen jako tapahtuu usein vanhastaan konesali- ja tietoliikennepalveluiden sekä ohjelmistopalveluiden välillä, molempien toimijoiden tuottaessa palveluita kuitenkin kiinteästi kohden samaa asiakkaan tietojärjestelmäkokonaisuutta. Myös Pilvi- ja As-A- Service palvelurakenteet sisällyttävät ja edelleen kompleksisoivat osaltaan samaa haasteellisuutta kontrollin näkökulmasta. Tietojärjestelmän tuotantovaiheessa järjestelmän käyttäjät ja liiketoimintaprosessit ovat usein tahoja, jotka ensimmäisenä havaitsevat järjestelmien käyttökatkot tai häiriöt järjestelmien toiminnallisuudessa. Järjestelmän omistajan tehtävänä on usein luokitella ja kohdistaa häiriö oikean toimittajan korjattavaksi.

Kuten todettua, tietojärjestelmät rakentuvat useista kerroksista sekä komponenteista; fyysisistä että ohjelmallisista. Palvelutuottajilla asiakkaan tietojärjestelmän jokaisen kerroksen asiantuntijataholla on omat työkalunsa ja sisäänrakennetut herätteensä järjestelmän tai sen käyttämän osateknologian häiriötilanteista. Esimerkiksi; Levyresurssin tilan hälytysarvot, prosessorin käyttöaste, kapasiteetin tarpeen äkilliset heilahtelut, sovelluksen poikkeustilanteet lokilla tai poikkeamat tietoliikenteessä. Kaikista näistä tilanteista syntyy erilaisia herätteitä ko. teknologian asiantuntijaryhmille, jotka osaavat ohjeistetusti tai kokemusperäisesti reagoida kunkin tilanteen edellyttämällä tavalla.

Tietojärjestelmän kokonaisuuden seuranta ja kaikkien siitä syntyvien herätteiden seuranta on silti ihmisvoimin suoritettuna haasteellinen työsarka jopa yhden yksittäisen tietojärjestelmän osalta. Tietojärjestelmien määrän kasvaessa, kasvaa myös näistä syntyvien valvontaherätteiden massa suureksi myös valvontatyötä tekeville asiantuntijaryhmille. Shoshana Zuboff totesi

ja osin myös ennakoi tätä kirjassaan ”Viisaan koneen aikakausi”, 1988, kirjoittamalla teknologian kehittymisen myötä tulevista laitteista, jotka automaattisesti keräävät tietoa samalla synnyttäen uusia informaatiovirtoja (Zuboff 1990, 25 - 29).

Nykyisin, yleisenä haasteena onkin tunnistaa kaikesta syntyvästä informaatio- ja hälytysvirrasta juuri ne yksittäisen tietojärjestelmän tai liiketoimintatapahtuman toiminnan kannalta olennaiset hälytykset, joiden perusteella voidaan ehkäistä potentiaalinen syntyvä virhetilanne. Häiriön jo toteuduttua tulee toivuttaa järjestelmä mahdollisimman nopeasti kohdentamalla virhetilanne spesifiin tietojärjestelmään, sen kerrokseen, esim. teknologiaan, ohjelmisto- tai fyysiseen komponenttiin. Informaatioyhteiskunnan aikakaudella alati kasvava informaation määrä ja sen käsittelytarve asettaa hyvin erityyppisiä ja kasvavia tarpeita tietojärjestelmille ja samalla myös näiden valvonnalle ja monitoroinnille. Yleisesti ottaen monitoroinnin, valvonnan ja seurannan tavoitteena on kuitenkin edelleen jo vuosituhansia vanha tavoite: varmistaa työn kulkua, nopeuttaa häiriötilanteista toipumista sekä varmistaa liiketoiminnan tehokkuutta ja jatkuvuutta.

3.2 Tietojärjestelmien valvontamekanismeja

Passiivinen monitorointi on raja-arvoihin perustuva komponentin, palvelun tai prosessin monitorointi, josta syntyy raja-arvojen ylityksestä hälytys valvovalle taholle. Aktiivisella monitoroinnilla taas tarkoitetaan komponentin, palvelun tai prosessin monitorointia, joka perustuu järjestelmälle annettuihin säännöllisiin syötteisiin, skripteihin. Transaktiopohjainen monitorointi puolestaan perustuu nimensä mukaisesti siihen, että tietojärjestelmään aiheutetaan synteettinen transaktio, jonka vasteaikaa mitataan ja seurataan ja jonka perusteella saadaan loppukäyttäjän toimintaa vastaava vasteaika, lähtötilanne/viitearvo (baseline) ja toistuvista transaktioista syntyy lähtötilanteeseen vertailtavaa vasteaika dataa.

Synteettinen transaktio on skripti, joka on luotu nauhoittamalla tai koodaten ja joka suorittaa tietojärjestelmään halutun komentoketjun. Tyypillisesti tämä on valvonta- ja monitorointiohjelmistolla nauhoitettu tai liiketoimintaohjelmistotoimittajan itsensä tekemä E2E-tyyppinen tai BPM-tyyppinen valvontamekanismi ja se suorittaa valvottavaan kohteeseen tapahtuman tai tapahtumaketjun, jonka vasteaikaa seuraamalla saadaan informaatiota mitattavan kohteen tilasta.

End-to-End, e2e-valvonta on valvontaa, jossa järjestelmän loppukäyttäjien toimintaa simuloidaan jatkuvalla, ajastetulla syklillä virtuaalikäyttäjien avulla. Näin saadaan loppukäyttäjän näkökulmasta kuva järjestelmän toiminnasta sekä mahdollisista viiveistä tai häiriöistä tietojärjestelmässä. Toiminta perustuu käyttäjän toiminnasta, järjestelmän keskeisistä toiminnoista nauhoitettujen ja skriptattujen käyttötapauksien ajastettuun toistamiseen mittauspisteiltä käsin, joita voidaan sijoittaa asiakkaan infrastruktuuriin haluttuihin kohteisiin asiakkaan

sisäverkossa, internetissä tai kapasiteetti- ja konesalipalveluiden toimittajan konesaliin. Varsinaista yhtenäistä hyväksyttyä määritelmää e2e-monitoroinnille ei ole, mutta yleisen ymmärryksen asiasta saa palvelua tuottavien yritysten markkinointimateriaaleista tai Wikipediasta.

Real user monitoring, RUM, tarkoittaa käyttäjän toiminnan tallentamista web-sivuilla tai tietojärjestelmässä ja tämän tallennetun datan myöhempää analysointia loppukäyttäjäkokeman, laadun sekä häiriöiden juurisyyn etsintää varten (Stackify 2019).

Sovelluksen toiminnan oma analysointi ja sisäänrakennettu "sovelluksen itsevalvonta". Sovelluksen sisään rakennetut ajonaikaisen eli tuotannon operatiivisen ylläpitotyöskentelyn työkaluilla voidaan seurata yksittäisen sovelluksen toimintaa sen keskeisten toiminnallisuuksien osalta. Useissa tietojärjestelmissä on sisäänrakennettuja työkaluja sovelluksen toiminnan seurantaa varten. Nämä työkalut ovat usein roolitettu pääkäyttäjä, admin oikeuksin varustetuille käyttäjille ja työkalujen käyttö sekä ymmärtäminen syyseuraus suhteista vaatii yleensä spesifioituneempaa osaamista ko. sovelluksen toiminnasta.

Business Process management, BPM, eli liiketoimintasovellusten monitoroinnilla viitataan sovellusten valvontaan ja tarkemmin ottaen liiketoimintaprosessien ja ketjujen mittaamiseen (Gartner, BPM 2019). Näitä arvoketjuja voidaan havainnollistaa vaikkapa lipunmyyntijärjestelmän ja sen vaatimien sovellus - sovellus yhteyksien sekä käyttäjän käynnistämien toimintoketjujen valvonnan kautta. Liiketoimintasovellusten monitoroinnilla ja valvonnalla pyritään ennakoimaan ja estämään liiketoiminnan potentiaalisia häiriökohteita sovelluksissa. Useat toimittajat, mm. HP, SAP, IBM tarjoavat omia ratkaisuja tähän käyttöön.

Palvelin ja Komponenttitason valvonta, ovat valvontamekaniikkaa, joita mm. käyttöpalvelutoimittajat käyttävät laitteistonhallinnan ja valvonnan työkalujen avulla monien tuhansien palvelinten yhtäaikaiseen monitorointiin ja valvontaan. Komponenttitason valvonnalla rakennetaan usein asiakkaan liiketoiminnan järjestelmien käyttämistä komponenteista looginen kokonaisuus relaatioiden avulla, jonka jokaista yksittäistä komponenttia valvotaan valvontasovelluksen avulla. Nämä valvonnat perustuvat useimmiten valvottavalle laitteelle asennettavaan sovellukseen, joka valvoo laitteen tilaa ja tuottaa monitorointidataa keskitettyyn tieto-

kantaan sekä raja-arvojen ylittyessä lähettää hälytyksen operatiiviselle henkilökunnalle. Valvonta- ja monitorointityökaluilla voidaan mitata laitteen fyysistä tilaa sekä laitteella toimivien sovellusten tilaa.

3.3 Sovelluksenvalvontajärjestelmä (APM)

APM, eli applikaation suorituskyvyn hallinnalla tarkoitetaan järjestelmän ja tai applikaation suorituskyvyn ja saavutettavuuden monitorointia ja hallintaa. APM:n avulla käännetään IT -metriikat liiketoiminnan arvoiksi. Taulukossa 3. esitellään APM konsepti esimerkin avulla.

Sovelluksenvalvontajärjestelmän ulottuvuudet on kuvattu vuonna 2012 seuraavasti; käyttäjäkokemuksen mittaaminen, EUE, (End User Experience), Ajonaikainen applikaatio arkkitehtuuri, jolla tarkoitetaan järjestelmässä tapahtuvien siirtymien ja riippuvuuksien monitorointia. Liiketoiminta transaktiot, joilla monitoroidaan nimenmukaisesti liiketoiminnalle merkittävien tapahtumien toimintaa. Syväluotaava komponenttien monitorointi, jolla taas tarkoitetaan kooditason suorituksen monitorointia komponenttitasolla sekä Analysointi ja raportointi, jolla tarkoitetaan esim. palvelutason raportointia.

Ulottuvuudet	Fokusalueet	Mahdolliset hyödyt
1. EUE, End User Experience, loppukäyttäjäkokemus	Agentiton (RUM) Usean protokollan analysointi Keinotekoisia luotauksia ja robotteja	APM arvo/hyöty; 80% saavutetaan EUE monitoroinnilla Agentiton on pieniriskinen (Porttien peilausta) • Nopea implementointi < 2 päivää Robotit = saavutettavuus & matalat volyymit, trendit
2. Ajonaikainen applikaatio arkkitehtuuri	Polkujen analysointi Alhaalta ylös – ylhäältä alas Pilvi applikaatioidenmonitorointi	Parempi riippuvuuksien kartoitus • Ymmärrys siitä, miten tietoliikenne topologia vaikuttaa applikaatioarkkitehtuurin kanssa • Muutosten vaikutusten arviointi
3. Liiketoiminta transaktio	Käyttäjän määrittelemät transaktiot URL / Sivu määrittelyt 8:sta 12:staylätason ryhmää	Tarkoituksenmukaiset SLA:t liiketoiminnan tueksi Liiketoiminnan luottamuksen vahvistaminen Tarjoaa ennakoivia varoitusraportteja
4. Syväluotaava komponentti monitorointi	Väliohjelmisto (Applikaatio & Viestin välitys) Ajonaikainen (J2EE & .NET) Toisen tason laitteiston automaattinen komponenttitietojen ja riippuvuuksien keruu	Paremmat koodin katselmukset ja tarkkuus. Laatu testauksen tarkkuuden paraneminen Nopeampi juurisyyn löytyminen suorituskyvyn hidastumistilanteissa
5. Analysointi ja raportointi	Raaka-datan keruu Yhteinen metriikka kokoelma Keskiarvot ja yhteydet	Palvelutasonhallinta applikaation profilointi (vertailuarvojen rakennus) Kapasiteetin suunnittelu / trendien analysointi

Taulukko 1: Application Performance Management kehikko (Dragich 2012), käännös kirjoittajan

Nykyisin käytetään myös termejä ”Digital experience monitoring (DEM)” eli digitaalisen käyttökokemuksen monitorointi, ”Application discovery, tracing and diagnostics (ADTD)” eli applikaation infrastruktuurin automaattinen havaitseminen ja diagnostiikka sekä ”Artificial intelligence for IT operations (AIOps)” jolla puolestaan tarkoitetaan operaatioiden alustaa, jotka yhdistävät Big Datan ja koneoppimisen keinoja avustaa IT-operaatioita.

4 ITIL Viitekehys ja monitorointi

ITIL, IT infrastructure library, on kokoelma parhaita IT-alan käytäntöjä. Viitekehys on peräisin 1980-luvulta, Ison Britannian hallituksen kehittämä sekä nykyisin itSMF – IT Service Management Forumin –käyttäjäyhdistys- hallinnoima kokonaisuus. ITILin edeltäjän nimi oli GITIM; Government Information Technology Infrastructure Management (ITIL Central 2019).

ITIL on laajasti IT-alalla käytetty, yleismaailmallisesti tunnustettu viitekehys, joka määrittelee itsensä seuraavasti:

”Joukko IT-palvelunhallinnan parhaiden käytäntöjen julkaisuja. ITILin omistaa Cabinet Office (osa Britannian hallitusta). ITIL ohjaa laadukkaiden IT-palvelujen ja prosessien, toimintojen ja muiden kyvykkyyksien tuottamista. ITIL-viitekehys perustuu palvelun elinkaareen, ja muodos-

tuu viidestä elinkaaren osasta (palvelustrategia, palvelusuunnittelu, palvelutransitio, palvelutuotanto ja jatkuva palvelun parantaminen), joista kustakin on oma julkaisunsa" (itSMF Finland 2011).

4.1 Tietojärjestelmän monitoroinnin ja valvonnan tarkoitus

Kontrolli ITIL Service Operation kirjassa määritellään "keinoksi riskienhallinnalle; liiketoimintatavoitteen saavuttamisen varmistamiseksi tai prosessin seurannan varmistamiseksi". Kontrollilla tarkoitetaan myös konfiguraation, konfiguraation osan, systeemin tai IT-palvelun käyttöasteen tai käyttäytymisen hallintaa (ITIL SO 2010, 229).

ITIL, Service Operation kirjassa määritellään valvonnan ja monitorointi lisäksi seuraavasti: "Valvonta, monitorointi (ITIL Palvelutuotanto), Konfiguraation rakenneosan, IT-palvelun tai prosessin toistuva havainnoiminen herätteiden havaitsemiseksi ja sen varmistamiseksi, että vallitseva tila on tiedossa" (ITIL SO 2010, 238).

Monitoroinnilla mahdollistetaan ja luodaan perustat strategialle, palvelun jatkuvalle parantamiselle, palvelutasojen mittaamiselle sekä testaamiselle. Vaikka ITIL asettaa monitoroinnin palvelun operaatioiden osaksi, monitoroinnin tuloksia käytetään kaikkien IT-palvelunhallintaprosessien laadullisen tarkkailun lähtökohtana sekä perustana.

4.2 Raportointi, monitorointi ja kontrolli

Raportoinnilla viitataan monitoroinnin yhteydessä monitoroinnista syntyviin analyyseihin sekä monitoroinnin tuloksena syntyvän datan tuottamisen sekä julkaisun oikeille henkilöille, ryhmille tai työkaluun (ITIL SO 2010, 82).

Kontrollilla tarkoitetaan IT-operaatioissa, tuotannonhoidossa ja operatiivisessa tehtävissä prosesseja ja työkaluja, joilla hallitaan laitteen, järjestelmän tai palvelun käyttöä tai käytöstä. Kontrollin avulla operaatiot määrittelevät, mikä on normaalia tuotannon tilaa ja mikä epänormaalia, sääntelevät laitteiston, palveluiden tai järjestelmien tilaa sekä käynnistävät tarvittaessa korjaavat toimenpiteet, jotka voivat olla joko manuaalisia tai automatisoituja (ITIL SO 2010, 83). Yleisesti ottaen ja laajemmassa merkityksessä sana kontrolli merkitsee kielitoimiston sanakirjan mukaisesti valvontaa, silmälläpitoa, tarkkailua sekä tarkistusta (Kotimaisten kielten keskus 2018).

Keskeisenä osana monitorointiin ja kontrolliin kuuluvat monitoroinnin kontrolli luupit, joita on kahdentyyppisiä; suljettuja ja avoimia (ITIL SO 2010, 83). Avoimen luupin kontrollilla tarkoitetaan esim. tilannetta, jossa varmistus ajetaan ennalta määritettynä ajankohtana – välittämättä sen kummemmin ympäristön kulloisestakin tilasta. Suljetun luupin kontrollilla taas tarkoitetaan esimerkiksi tilannetta, jossa tietoliikenteen kasvaessa tietyn raja-arvon yli, kontrollijärjestelmä alkaa ohjaamaan tai jakamaan liikennettä varayhteyden kautta (ITIL SO 2010,

83). IT-palvelunhallinnassa monitoroinnilla ja kontrollilla tarkoitetaan jokaisen palvelua tuottavan asiantuntijaryhmän tai komponenttien aktiviteettien monitorointia. Jokainen ryhmä asettaa monitoroinnin kontrolli luupit oman palvelusuunnitelman mukaisesti. Toinen keskeinen toiminto, joka hyödyntää näistä syntyvää dataa, asiantuntijaryhmien lisäksi, on jatkuvan palvelun parantamisen prosessi, CSI (ITIL SO 2010, 86 - 87).

4.3 Monitorointi ja valvonta ITIL Viitekehyksessä

Taulukossa 2 on kuvattu ITIL viitekehyksen mukaisesti monitorointi aktiiviseen, passiiviseen, reaktiiviseen ja ennakoivaan monitorointiin. Jaolla on pyritty eriyttämään erityyppisiä monitoroinnin alalajeja niiden käyttötarpeen ja käyttökohteen mukaan.

Monitorointityyppi	Kuvaus
Valvonta (monitorointi)	Konfiguraation rakenneosan, IT-palvelun tai prosessin toistuva havainnoiminen herätteiden havaitsemiseksi ja sen varmistamiseksi, että vallitseva tila on tiedossa
Aktiivinen monitorointi (valvonta)	Konfiguraation rakenneosan tai IT-palvelun valvonta, joka käyttää automaattisia ja säännöllisiä tarkistuksia havaitakseen kulloisenkin tilan. Ks. myös passiivinen monitorointi
Passiivinen monitorointi (valvonta)	Konfiguraation rakenneosan, IT-palvelun tai prosessin, joka on hälytyksen tai ilmoituksen varassa, valvonta nykytilan selvittämiseksi.
Reaktiivinen valvonta (monitorointi)	Valvonta, joka tapahtuu vastauksena herätteeseen; esimerkiksi käynnistää eräajon, kun edellinen ajo on valmis, tai häiriön kirjaaminen, kun virhe tapahtuu.
Ennakoiva valvonta (monitorointi), proaktiivinen valvonta (monitorointi)	Valvonta, joka etsii herätteiden toimintamalleja ennustaakseen mahdollisia tulevia toimintahäiriöitä. Ks. myös reaktiivinen valvonta

Taulukko 2: Monitorointi ITIL viitekehyksen mukaisesti

ITIL kirjastossa kuvatuista prosesseista monitorointiin ja valvontaan erityisesti liittyviä alueita ovat mm. Palvelusuunnittelu; Palveluntasonhallinta, Saatavuudenhallinta, Kapasiteetinhallinta ja Palvelun siirto; Muutoksenhallinta, Julkaisunhallinta sekä Palvelu operaatiot; Herätteidenhallinta, Häiriönhallinta ja Ongelmanhallinta (APM Digest 2018).

4.4 Herätteidenhallinta

Herätteidenhallinnan prosessi on kokonaisuudessaan kuvattu ITIL Service Operation kirjassa. Tietojärjestelmän monitorointi ja valvonta synnyttää herätteitä ja yksittäiset herätteet kertovat raja-arvon ylittämisestä monitoroitavassa tai valvottavassa infrastruktuurin tai sovelluksen osassa. Tyypillisesti valvontakohteita ovat esim. palvelintenlämpötila, levytila, laskentateho, lokitiedostot, hakemistot, eräajot, sovelluksen häiriötilanteet jne. Syntyvät herätteet ohjataan ennalta sovittua viestintäkanavaa pitkin esimerkiksi toiminnanohjausjärjestelmään, valvontatyökaluun, sähköpostiin tai SMS-viestinä halutulle vastaanottaja ryhmälle. Herätteitä on monen tyyppisiä, esimerkiksi: hälytys, poikkeus, ilmoitus tai virhe (ITIL SO 2010, 40) ja hälytyksiin reagoivat yleensä tietojärjestelmän kunkin kerroksen palvelua tuottava asiantuntijataho. Heräteviestit muotoillaan selkeästi, jotta vastaanottavalla taholle välittyy hälyttävän

kohteen tunnistetiedot, hälytyksen raja-arvon eksakti arvo ja raja-arvon ylitys sekä ohjeistus toimintaan tai viittaus tuotannolliseen ohjeeseen ko. tilanteessa.

Alan Cooper (Cooper 2003, 436)kirjoittaa klassikkoteoksessaan ”About Face, 2.0” loppukäyttäjille sovelluksissa suunnatuissa häiriöviesteistä, että ihmiset eivät yksinkertaisesti halua nähdä virhedialogeja ja että sovellukset tulisi lähtökohtaisesti kirjoittaa niin, että ne ehkäisevät häiriötilanteiden synnyn. Cooper kirjoittaa tätä kirjassaan epäilemättä koskemaan järjestelmän käyttäjää, mutta vastaavasti järjestelmän käyttäjiä ovat myös pääkäyttäjät sekä ylläpitohenkilöstä ja täten tulisi samaa ajatusta noudattaa koko tietojärjestelmän kerroksellisen infrastruktuurin osalta. Lisäksi Cooper kirjoittaa sovellusten virhedialogeista; ”ole kohtelias, ole valaiseva, ole avustava” (Cooper 2003, 443). Samat periaatteet ovat yhtä lailla sovellettavissa, kun kirjoitetaan heräteviestejä, varsinkin kun osa herätteistä suunnataan järjestelmän tukeman liiketoiminnan edustajille, joilla ei välttämättä ole muuta ymmärrystä teknisestä häiriötilanteesta, kuin se, että tilanne jo parhaillaan pysäyttää, häiritsee tai riskeeraa liiketoimintaa. Isompi osa syntyvistä häiriöviesteistä on kohdennettu joko toimittajan Control Deskiin tai tietojärjestelmien osakokonaisuuksien toiminnasta vastaavalle asiantuntijaryhmälle varsinaista häiriötilannetta ennakoivana informaationa.

4.5 Palveluomaisuuden hallinta ja konfiguraationhallinta

ITIL viitekehyksessä Konfiguraationhallinta viittaa tapaan säilyttää ja hallinnoida tietoteknisen ympäristön eri komponenttien keskeisiä informaatioita niiden elinkaaren ajan.

”Prosessi, jonka vastuulla on varmistaa, että palvelujen tuottamiseen tarvittavaa palveluomaisuutta hallitaan oikealla tavalla, ja että omaisuudesta on saatavilla tarkkaa ja luotettavaa tietoa, milloin ja missä sitä tarvitaankin. Tämä tieto sisältää yksityiskohtia siitä, miten omaisuuserät on konfiguroitu, ja mitkä ovat omaisuuserien väliset suhteet” (itSMF Finland 2011.)

Konfiguraationhallinnan prosessin keskeinen tukijärjestelmä on CSM (Configuration Management System) ja sen keskeinen tietokanta on CMDB (Configuration Management Database) (ITIL SO 2010, 229). Tässä tietokannassa säilytetään ja ylläpidetään ajantasaista tietoa infrastruktuurin keskeisten laiteosista; ”Configuration Item, CI”. Yleisesti ottaen tiedot laitteesta sisältävät yksityiskohtaista tietoa CI:n palveluajoista, palveluista, omistajuudesta, palveluiden tarjoajista, relaatioista toisiin laitteisiin ja niin edelleen. Esimerkki rakenneosan sisältämistä tiedoista on kuvattuna taulukkoon 3. Asiakkaan CI kokonaisuus CMDB:ssä muodostaa kokonaisuuden infrastruktuuriarkkitehtuurista sekä liiketoimintajärjestelmien relaatioista infraan ja toisiin sovelluksiin. Monitoroinnin ja valvonnan näkökulmasta tämä tietokanta on hyvin keskeinen, sillä sinne piirtyy rakenne valvottavasta ja monitoroitavasta kokonaisuudesta. Useimmissa nykyisissä toiminnanohjausjärjestelmissä on konfiguraationhallinnan tietokanta,

CMDB, Configuration management database, keskeisessä roolissa ja tämä mahdollistaa palvelutuotannon systemaattisen dokumentoinnin ja palvelupyyntöjen ohjauksen oikealle taholle. CMDB:n ajantasaiset tiedot mahdollistavat myös valvonnan ja monitoroinnin automatisointia. Sovelluspuolen konfiguraatiohallinta rakentuu yleensä sovelluskehityksen kehittäjien yhteisesti sopimissa versionhallintatyökaluissa ja ovat tyypillisesti irrallaan konesali- ja kapasiteettipalveluiden tuottajan vastaavasta.

Kenttä	Kuvaus	Esimerkkiarvo
Name	Nimike	xxssxxssxx
Priority flag	Rakenneosan kriittisyys	Critical High Moderate Low Basic
Lifecycle	Elinkaaren vaihe	In transit Installed Retired
Company	Rakenneosan asiakkuus	
Owning company	Rakenneosan omistaja	
Subcategory	Luokittelu	Oracle
Environment	Ympäristö	Development Test Production
Installed	Asennusaika	2017-04-09
Description	Vapaa_kuvaus	
Security level	Tietoturvataso	Base Increased High

Taulukko 3: Esimerkki laitteistotiedosta konesali- ja käyttöpalvelun toimittajan laitteistonhallinnasta

4.6 Jatkuva palveluiden parantaminen

Jatkuva palveluiden parantaminen, Continual Service Improvement (CSI), on yksi ITIL v3, 2011, pääprosesseista. Jatkuva palvelun parantaminen varmistaa, että palvelut vastaavat liiketoiminnan muuttuva tarpeita tunnistamalla ja tekemällä parannuksia liiketoimintaprosesseja tukeviin IT-palveluihin. IT-palvelutuottajan suorituskykyä mitataan jatkuvasti, ja prosesseja, IT-palveluja ja IT-infrastruktuuria parannetaan tehokkuuden, vaikuttavuuden ja kustannustehokkuuden parantamiseksi.” (ITIL SO 2010, 229.) Tietojärjestelmän kaikista osakokonai-

suuksista voidaan tuottaa tilainformaatiota, jota seuraamalla voidaan ennakoida mm. kapasiteetin lisäystarpeita tai laitteiston korjaustarpeita ennen kuin ko. laitteen resurssit loppuvat ja aiheuttavat ennakoimattoman katkon liiketoimintajärjestelmälle.

4.7 Tilannekuva ja Perustason/Lähtötason mittaaminen

Tilannekuva (dashboard) ja viitearvon (baseline) mittaaminen. Vanhakantainen Suomenkielinen käännös dashboardista, ”kojetaulu”, antaa varsin hyvän käsityksen siitä, mistä tässä on kyse; kojetaulun merkityksen ymmärtää jokainen, joka on auton ratin takana istunut. Kojetaulusta tarkistetaan nopeus, moottorin lämpötila, kierrosluku, polttoaineen määrä ja hallitaan, kontrolloidaan auton toimintaa. Kojelaudan tiedot ovat auton operoijalle, kuljettajalle, edellytys koneen operointiin. Vastaavasti tietojärjestelmän operoija, pääkäyttäjä, tarvitsee työssään kojetaulun tai tässä yhteydessä kuvaavammalla termillä, valvontanäytön tai tilannekuvan, vastuullaan olevan kokonaisuuden toiminnasta. Vastaavasti myös valvontanäytön mittaristojen arvojen tulee antaa operoijalle ymmärrys siitä, mikä on tietojärjestelmän yleinen tilanne, perustaso ja operoijalla tulee olla käsitys siitä, miten valvontanäkymän arvot korreloivat tietojärjestelmän toimintaan, liiketoimintaan ja loppukäyttäjän palvelukokemaan.

Jatkuvan palveluiden parantamisen lähtötasoksi tarvitaan viitearvot, joita vasten kehitystä voidaan mitata. On sitten kyse prosesseista, kapasiteetista tai loppukäyttäjän palvelukokemasta järjestelmän käytön kanssa; tarvitaan viitearvo, jonka vaihtelua seuraamalla saadaan informaatiota esimerkiksi muutosten vaikutuksesta tietojärjestelmään. Näiden viitearvojen seuranta antaa mahdollisuuden toimittajalle reagoida tilanteisiin niiden vaatimalla tavalla sekä perustason datan pidempiaikainen seuranta rakentaa toimittajalle kyvykkyyttä proaktiivisuuteen reaktiivisuuden sijasta. Viitearvoon viitataan usein myös sanalla ”Baseline”.

Viitearvon seurannan kannalta on oleellista ymmärtää, mikä on ”normaalia” järjestelmän toimintaa ja mikä taas epänormaalia. Raja-arvojen asettaminen antaa tämän mahdollisuuden ja käytäntönä on raja-arvojen ylittämisestä syntyvä hälytys, joka ohjataan ko. mittauskohteen jatkuvasta palvelusta vastaavalle taholle; useimmiten Control Deskiin tai Service Deskiin. Lisäksi on mahdollista automatisoida hälytyksestä seuraavat vastineet tai toiminnot.

ITIL jäsentää saman asian seuraavasti:

”takaisinkytketty kontrolli: Tehtävän, prosessin, IT-palvelun tai muun konfiguraation rakenneosan tuotoksen valvonta; tuotoksen vertaaminen ennalta määriteltyyn normiin; ja toimiminen soveltuvalla tavalla tämän vertailun pohjalta” (itSMF Finland).

Järjestelmän teknisen datan vaihteluvälien seuranta mahdollistaa mm. kapasiteetin tarpeen ennakoinnin kanssa tai esimerkki tarkemmin; järjestelmän käyttäjämäärän tai datamäärän

kasvun aiheuttaman kuormituksen vaikutukset tietojärjestelmä infrastruktuurin suorituskykyyn. Laajemmassa perspektiivissä katsottuna Juhta (JUHTA 2012) viittaa samaan käsitteeseen yleisemmällä tasolla ”nykytilan analyysi”.

” ICT-palvelujen kehittämisen näkökulmasta kehittämisellä on kolme päävaihetta: nykytilan analyysi, tavoitetilan suunnittelu, toimeenpanon suunnittelu” (JUHTA 2012).

5 EA-näkökulma valvontaan ja monitorointiin

Kokonaisarkkitehtuuri, EA, on käsitteenä moniulotteinen, ilman selkeää yleismaailmallisesti hyväksyttyä määrittelyä. Monissa organisaatioissa kuitenkin laaditaan kattavaa kokonaisarkkitehtuuria jäsentämään sekä tukemaan liiketoimintapalveluiden, prosessien, tietojärjestelmien johtamista ja jatkuvaa kehittämistä. Kokonaisarkkitehtuurille löytyy useita erityyppisiä määrittelyitä, mm. Jyväskylän yliopiston väliraportissa 2012, on kirjattu kokonaisarkkitehtuurista seuraavasti:

> ”Kokonaisarkkitehtuuri on johtamisen ja yhteistyön väline, jonka avulla voidaan edistää organisaation strategisten tavoitteiden saavuttamista. Toimintaprosessien, tietojen, tietojärjestelmien ja teknologian sekä näiden keskinäisten riippuvuuksin systemaattisella tarkastelulla on mahdollista lisätä päätöksenteon laatua ja nopeutta, parantaa muutoksenhallintaa ja resurssien kohdentamista sekä kehittämishankkeiden ohjausta” (Jyväskylän yliopisto 2012.)

Vastaavasti The Open Group Architecture Framework (TOGAF), kuvaa arkkitehtuurin hallintamallin kokonaisarkkitehtuurin johtamismenetelmänä, jolla arkkitehtuurikehitystä tarkastellaan koko yrityksen laajuisena aktiviteettina ja jonka tehtävänä on luoda käytännöt ja kontrollit arkkitehtonisten komponenttien luonnille, monitoroinnille, implementoinnille, kehitykselle, yhteensopivuudelle sekä näitä tukevien prosessien kehittämiselle (Togaf 2019).

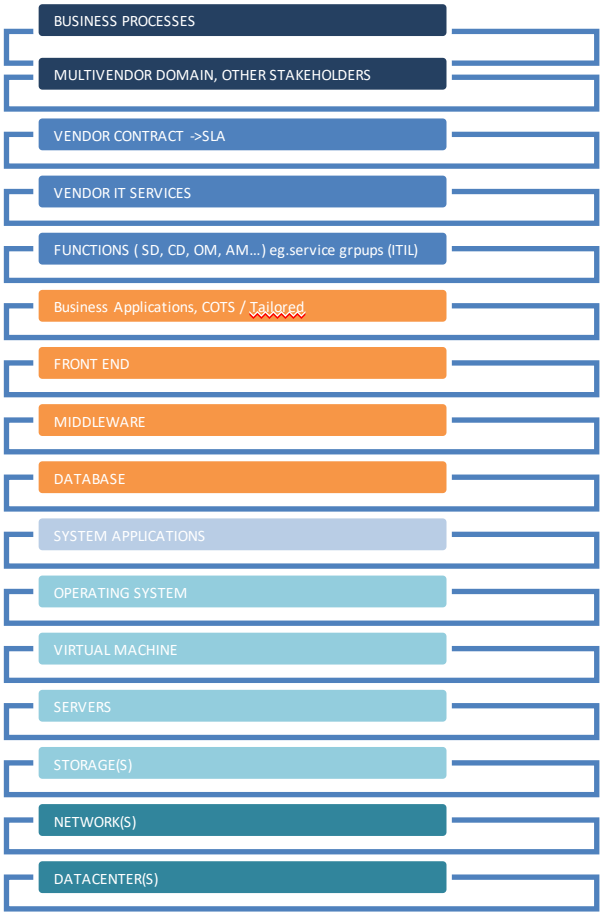
Juhta, Julkisen Hallinnon tietohallinnon neuvottelukunnan, suositus JHS 171 ICT Palvelujen kehittäminen puolestaan määrittelee seuraavasti: ”Kokonaisarkkitehtuuri on toiminnan prosessien ja palvelujen, tietojen, tietojärjestelmien ja niiden tuottamien palvelujen muodostaman kokonaisuuden rakenne. Kokonaisarkkitehtuuri pitää sisällään arkkitehtuurilinjaukset ja kuvaukset, arkkitehtuurin hallintamallin sekä arkkitehtuurimenetelmän” (JUHTA 2012).

Kokonaisarkkitehtuuri määrittyy myös ”Yritysarkkitehtuuri” termin kautta: ” Yritysarkkitehtuurit (Enterprise architecture) mahdollistavat liiketoiminnan ja ICT-teknologian yhtäaikaisen jatkuvan kehittämisen ja hallinnan. Yritysarkkitehtuurin tavoitteena on luoda muokkautuva ja tehokas hallintaväline sekä liiketoiminta, että ICT-muutoksia varten” ja ” Englanninkielisen

Enterprise architecture – termin käännöksenä käytetään myös kokonaisarkkitehtuuri termiä" (Isokallio 2005).

5.1 Kokonaisarkkitehtuurin ajonaikainen monitorointi

Monet hyvin tunnetut kehikot kuten Togaf ja ITIL luovat kerroksellisen näkymän, abstraktion kokonaisarkkitehtuurista; It-infrastruktuuri, sovellukset ja liiketoiminnalliset prosessit. Vaikka markkinoilla on olemassa runsaastikin erityyppisiä ja tasoisia monitorointiohjelmistoja ja näistä laadullisia vertailuja on olemassa, holistisen kuvan muodostaminen kokonaisarkkitehtuurin tilasta on hankalaa. Koska em. kaltainen linkitys EA:n ja monitoroinnin on todettu puuttuvan, ehdottavat Kleehaus, Uludag ja Matthes palveluväylän lisäämistä EA-tuotteeseen (Kleehaus;Uludag ja Matthes 2017), jonka tehtävänä on yhdistää kokonaisarkkitehtuuria ja monitorointia tekevät sovellukset kokonaisvaltaisen ja reaaliaikaisen ajonaikaisen näkymän muodostamiseksi. Tässä tutkimuksessa asiantuntijoiden teemahaastatteluista saatu kokemusperäinen informaatio tukee tätä näkemystä kokonaisnäkökulman puutteen osalta, kuviossa 1 on kuvattuna esimerkki kerroksellisuudesta, joihin monitorointia eri työkaluin tyypillisesti kohdistuu.



Kuvio 1: Kokonaisarkkitehtuuri esimerkki, Palveluiden kerroksellisuus

5.2 Palveluiden käyttäjien kategorisointi

Kokonaisarkkitehtuurin sidosryhmät voidaan luokitella 3 eri ryhmään; Tuottajat, Fasilitaattorit ja käyttäjät (Niemi 2007). Käyttäjillä tarkoitetaan tässä kontekstissa kaikkia niitä työrooleja, joilla on vaatimuksia EA:ta kohden. Käyttäjällä on työtehtävä tai liiketoiminnallinen syy järjestelmällä tehtävään toimenpiteeseen.

Alan Cooper esitteli sovelluskehityksen työkaluksi ”personan” käsitteen, loppukäyttäjän/ryhmän geneerisen arkkityypin. Kirjassaan ”Inmates are running the asylum” Cooper hahmotteli eri tyyppisiä ”persona”, suom. persoonia ja suunnitteluperiaatteita näiden luomiselle. Yksinkertaisimmillaan siinä luodaan tarkka kuvaus käyttäjästä ja mitä käyttäjä haluaa järjestelmässä suorittaa (Cooper 2004, 123-124). Monitoroinnin ja käyttäjäkokemuksen seurannassa voidaan hyödyntää näitä arkkityyppejä monitorointikohteita suunniteltaessa. Järjestelmään voidaan mm. rakentaa keinotekoisia käyttäjiä suorittamaan ajastetusti arkkityypille tyypillisiä tehtäviä ja näin voidaan todentaa järjestelmän käytön toimivuutta.

5.3 Yleisimmät pilvipalveluiden palvelumallit

SAAS, Software as a Service Ohjelmisto, jonka omistaa, toimittaa ja hallinnoi yksi tai useampi palveluntuottaja etäyhteyksien kautta (Gartner, SAAS 2019). Sovellus palveluna -palvelukonseptissa, kuluttaja ostaa infra, ja alustapalveluiden lisäksi näiden päällä toimivan omaa liiketoimintaansa tukevan sovelluksen toiminnan kokonaispalveluna. Sovelluksen omistajuus on palvelun toimittajalla. Asiakaskohtaisia infrastruktuuriympäristöjä ei ole, vaan sama ympäristö ja kapasiteetti palvelee kaikkia asiakkaita ja käytöstä veloitetaan käytön määrän perusteella.

PAAS, Sovellusten alustapalvelut, Platform as a service. Fyysisen, käsin kosketeltavan laitteiston ja infrastruktuurin yläpuolella olevat, sovellusten tarvitsemat varusohjelmistot muodostavat pilvi palveluna palvelukokonaisuuden, josta kuluttaja voi ostaa infrapalvelun lisäksi myös tämän osakokonaisuuden applikaatiotansa varten palveluna – ilman fyysisen infrastruktuurin mukanaan tuomaa kompleksisuutta (Gartner, PAAS 2019).

IAAS, Infrastructure as a Service, infrastruktuuri palveluna. Sovelluksen tarvitsema infrastruktuuri – laskentateho ja tallennustila ostetaan palveluna. Tässä palvelumallissa ei järjestelmän omistajalle tule kuluja infrastruktuurin laitteiston ylläpidosta tai laitteiston omistamisesta. Palvelusta maksetaan käytön mukaisesti ja yleisesti siihen sisältyy itsepalvelurajapintojen kautta hankittavat tallennustila, palvelimet, verkkoyhteydet sekä näiden ylläpito (Gartner, IAAS 2019).

6 Menetelmäosuus

Tässä tapaustutkimuksessa käytettiin laadullista, eli kvalitatiivista tutkimusmenetelmää, pyrkien saavuttamaan kokonaisymmärrystä monitoroinnin ja valvonnan haasteista kohdeyrityksen

asiantuntijaryhmien kokemuksia tutkien. Lisäksi tutkimuksessa käytettiin fenomenologista lähestymistä, jossa tutkija itse peilaa omaa kokemustaan, teoreettista kehystä ja kuvaa aihealueesta saavutetun käsityksen muotoutumista haastateltavilta saatuun tietoon.

Tutkin työssä tietojärjestelmien valvontaa kokonaisuutena ja pyrin esittämään mallirakenteita, joita voidaan hyödyntää valvonnan ja monitoroinnin suunnittelun yhteydessä kohdeyrityksessä myöhemmin. Pyrin lopputyössä kaikuluotaamaan työyhteisöstä pidemmältä aikaväliltä kummunneita teemoja, selkeästi toisistaan eroavia käsityksiä aihepiiristä, haastatteluiden teemana sekä alan kirjallisuutta ja alueen eri toimittajien palvelutarjontaa kartoittaen.

6.1 Laadullinen eli kvalitatiivinen tutkimus

”Lähtökohtana kvalitatiivisessa eli laadullisessa tutkimuksessa on todellisen elämän kuvaaminen. Tähän sisältyy ajatus että, todellisuus on moninainen.” ja ” Kvalitatiivisessa tutkimuksessa kohdetta pyritään tutkimaan mahdollisimman kokonaisvaltaisesti.” (Hirsjärvi;Remes ja Sajavaara 2000, 161) Tesch on todennut, että kvalitatiivisten tutkimuksen lajeja on runsaasti ja että usein erottavana tekijänä on lähinnä käytetty aineisto tai metodologia. (Tesch 1991, 16-17, Hirsjärvi, ym., 2000, 163) mukaan.

6.2 Fenomenologinen tutkimus

Fenomenologia on filosofinen suuntaus, jolla tarkoitetaan ilmiöiden olemuksen tutkimista henkilön oman kokemuksen näkökulmasta (Smith 2018).

Valitussa tutkimusstrategiassa tämä näkyy kvalitatiivisen tutkimuksen lähtökohdan valinnassa ja tämän rinnalle täydentävänä lähestymisenä fenomenologista strategiaa ja fenomenografista lähestymistä, joka korostaa asiantuntijoiden omaa kokemusta aiheesta ja näihin perustuvaa ymmärryksen muodostumista tutkimuskohteesta. Pyrkimyksenä on löytää aiheesta/ilmiöstä eroavuuksia sekä erityisesti yhtäläisyyksiä asiantuntijoiden kokemuksien ja käsitysten kautta, teemahaastatteluiden kautta saavutettavasta informaatiosta.

Fenomenografian nimi muodostuu sanoista ”ilmiö” ja ”kuvata”. Fenomenografinen tutkimuksen ensimmäisessä vaiheessa tutkija kiinnittää huomionsa asiaan ja/tai käsitteeseen, josta tuntuu olevan monentyyppisiä käsityksiä. Toisessa vaiheessa tutkija perehtyy aihealueeseen jäsentäen alustavasti näkökohdat, kolmannessa vaiheessa haastatellaan henkilöitä, jotka ilmaisevat erilaisia käsityksiä asiaan liittyen ja neljännessä vaiheessa tutkija luokittelee käsitykset niiden merkityksen perusteella. (Syrjälä, Ahonen, Syrjäläinen & Saari 1994, 114-115.)

6.3 Aineistonhankintamenetelmät

Aineistonhankintamenetelmistä puolistrukturoitu haastattelumenetelmä, eli teemahaastattelu, on soveltuva metodi kvalitatiivisen tutkimuksen aineistonkeruuseen. Teemahaastatte-

lussa haastattelun aihealue on tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat. Haastattelija pyrkii saamaan tarkentavien kysymysten avulla laajemmin tietoa aiheesta (Hirsjärvi, Remes ja Sajavaara 2000, 204-205.)

Haastattelu on tavallisin fenomenografisen aineiston keruumenetelmä, jossa toteutuu fenomenografian tiedonkäsitykseen kuuluva intersubjektiivisuus. Haastattelijalta tämä edellyttää oman lähtökohdan tiedostamista, aktiivisen kuuntelijan roolia, sekä haastateltavan luottamusta tutkijaan. Haastattelussa pyritään keskustelevaan otteeseen ja menetelmä edellyttää tutkijalta tutkittavan aihealueen suvereenia teoreettista hallintaa sekä harjaantunutta otetta kysymysten muotoiluun haastattelutilanteessa. Ihanteellisessa tilanteessa haastateltavalla ja haastattelijalla on mahdollisuus jatkaa haastattelua aiheesta useina eri päivinä. Syvähaastattelulla pyritään spiraalinomaisesti työntymään kulloisenkin aiheen sisältöön. (Syrjälä ym., 1994, 136-137.)

Lopputyön kirjallinen pohja perustuu alan vallitseviin käytäntöihin, aihealueelta valikoituihin kirjallisiin lähteisiin sekä suoritettuihin syväasiantuntija haastatteluihin. Haastattelutilanteista kirjoitetut yhteenvedot esitellään liitteissä 1-3.

6.4 Reliabiliteetti ja validiteetti

Laadullisen aineiston luotettavuus ja tulkinnat riippuvat, siitä miten ne vastaavat haastateltavien tarkoittamia merkityksiä sekä siitä, missä määrin ne vastaavat teoreettisia lähtökohtia. Aineiston kohdalla validiteetti merkitsee aitoutta ja relevanssia. (Syrjälä ym. 1994, 129.)

Tämän tutkimuksen luotettavuus ja validiteetti rajautuu, tiedostetusti kontekstiin, jossa haastattelut suoritettiin ja vastaakin lähinnä kysymyksiin kohdeyrityksen ja asiantuntijoiden kokemuksen ja kokeman näkökulmasta. Tulokset eivät siten ole kovin hyvin yleistettävissä tai laadullisesta näkökulmasta luotettavuuden osalta toistettavissa. Tutkimus vastaa esitettyihin kysymyksiin juurikin kohdeyrityksen sekä haastateltujen asiantuntijaryhmien käytännön työn kehittämistarpeiden ja kohdeyrityksen näkökulmasta. Muiden asiantuntijaryhmien näkökulma antaisi todennäköisesti kattavamman, erilaisen tai ainakin eri tavalla painotetun näkökulman aiheeseen.

7 Haastattelututkimus

Haastattelut suoritettiin kolmena varsinaisena erillisenä haastattelutilanteena kohdeyrityksen tiloissa. Haastattelutyyppinä käytettiin tilanteeseen parhaiten soveltuvana teemahaastattelua, jossa pääteemoina oli haastateltavana kunkin asiantuntija-alueen edustajalle häiriötilanteista toivuttamisen haasteet ja valvontanäkymien hyödyllisyys/hyödyttömyys haastateltavan asiantuntijan työssä, asiantuntijan käytössä olevat informaatiolähteet, nykyiset kullakin haastatellulla käytössä olevat monitorointi- ja valvontatyökalut sekä asiantuntijan työtä tukevan

ihanteellisen valvontaratkaisun kuvailu. Haastateltavaksi valittiin kerroksellisesti tarkasteltuna kolmen eri asiantuntija-alueen hyvin tunteva asiantuntija yli 10 vuoden työkokemuksella. Haastattelutilanteet olivat irrotettuna ulkopuolisista häiriötekijöistä sekä keskustelun kulu oli luontevaa, sillä keskustelijoilla oli entuudestaan luottamuksellinen työsuhde, samankaltainen tietopohja ja termistö hallinnassaan sekä suoritetut haastattelut limittyivät yhteisiin työtehtäviin sekä työnkehittämisen tarpeeseen. Varsinaisten työtilanteiden ulkopuolella tapahtuneissa vapaamuotoisemmassa haastattelutilanteessa keskustelu tuotti laaja-alaisesti informaatiota kunkin haastateltavan näkökulmasta.

Haasteiksi haastatteluissa nousi esiin teemasta lipsuminen ja sovittujen haastatteluaikojen noudattaminen sekä haastatteluiden edetessä oli haastattelijalla haasteena pidättäytyä haastatteluissa neutraalina, vaikkakin aiemmista haastatteluista alkoi muodostua yhteisiä teemoja ja rakennetta. Haastatteluissa aluksi aiheeseen ja teemaan pääseminen oli hidasta, mutta keskustelun käynnistyttyä huomasimme usein ajan päättyvän kesken. Keskustelua ja haastattelua jatkettiin myös useassa eri tilanteessa varsinaisten haastatteluiden jälkeenkin, täydentäen sekä kommentoiden eri näkökulmia. Dokumentoin varsinaiset muistiinpanot jokaisen haastattelun sekä sitä seuranneiden keskusteluiden jälkeen sekä toimitin muistiinpanoni käydyistä keskusteluista vielä haastateltaville sähköisesti kommentoitavaksi ja jatkokeskustelun pohjaksi.

7.1 Haastatteluiden tulokset

Haastatteluista sekä käydyistä keskusteluista saatiin tuloksena kolmesta palvelutuotannon asiantuntijaryhmästä tyypilliset vastaukset ja näkökulmat kunkin asiantuntijaryhmän kehittämistarpeisiin monitorointiin ja valvontaan liittyen. Haastatteluista syntyneistä aineistoista löytyi ns. punainen lanka kaikille tuotannon hoitamiseen liittyville asiantuntijoille, sekä tunnistettiin erityyppisiä ennakointiin, reagointiin sekä häiriönhallintaan liittyviin tilanteisiin sekä tarpeisiin, jotka on kuvattu kuviossa 3 ja 4.

7.2 Haastatteluiden yhteenveto

Kaikissa haastatteluissa nousi esiin tarve ennakoivaan häiriöntunnistamiseen sekä kokonaisvaltaisempaan – mutta toisaalta myös yksityiskohtaisempiin tietosisältöihin häiriötilanteeseen liittyen. Yhtenä suurena haasteena tietotekniikka toimittajilla on asiakkaiden ja järjestelmien lukumäärä, teknologiakirjo sekä hajautetut palvelutuotantomallit. (Liite 2: haastattelu 2, monitorointi- ja valvonta-alueen arkkitehti) Monitorointi- ja valvontatyökalut ovat usein raken-

nettu hyvin spesifeiksi tuotteiksi tuottamaan informaatiota kunkin tekniikan tai vaikkapa palvelintyypin tai tietokannan tilasta kunkin teknologian asiantuntijoiden analysoitavaksi ja tutkittavaksi.

Tietoturvan kannalta monitoroitavia asioita ovat mm. tietoliikenne, sisään- ja uloskirjautumisten määrä, työasemien / palvelinten määrä sekä jatkuvuuden varmistamiseksi rakennettavat toiminteet, kuten varmistukset, seurantaraportit sekä spesifit jäljitettävyyden valvontakohteet tietojärjestelmissä. Center for Internet Security, CIS, on kehittänyt sarjan parhaita käytäntöjä, benchmarkkeja arkkitehtuurin eri kerroksia varten, esim. applikaatiot, käyttöjärjestelmät, palvelimet, tietokannat. Benchmarkit sisältävät suositeltuja tietoturvakovennuksia (CIS 2018).

Keskustelussa Tietoturva-alueen asiantuntijan kanssa (Liite 3, haastattelu 3) nousi esiin valvonnan ja monitoroinnin näkökulma tietoturvan ja jatkuvuudenhallinnan osalta. Jatkuvuudenhallinnasta hyvän esimerkin hän asettaa mm. Valtionvarainministeriön ylläpitämä VAHTI-ohjeistus tilannekuvalle seuraavia vaateita tietojärjestelmien toimittajille ja palvelutuotannosta vastuullisille tahoille:

> “Tilannekuva muodostuu kaikesta toiminnan kannalta relevantista informaatiosta. Sitä tulee ylläpitää ja seurata, jotta voidaan ennakoida ja pienentää mahdollisten häiriöiden vaikutuksia. Esimerkkejä toimintaan mahdollisesti vaikuttavista tekijöistä ovat ulkoiseen toimintaympäristöön kohdistuvat myrskyt, lakot, epidemiat ja mielenosoitukset.
>
> Häiriötilanteessa teknisen tilannekuvan muodostamiselle hyödyllisiä tietoja ovat esimerkiksi seuraavat, verkon tilannetieto, palveluiden käytettävyyden tilannetieto, suunnitellut huoltokatkot, havainnot kyberuhkista ja niiden mahdollisista vaikutuksista, tilannetieto käyttö- ja palvelukeskusten sekä kenttätoiminnan valmiustason muutoksista, muu merkittävä, palvelun tuottamiseen vaikuttava tapahtuma, esim. jakeluhäiriö sähköverkossa.” (Valtionvarainministeriö 2016.)

Tietoturvan kovennuksia ovat infrastruktuurin jatkuvan seurannan ja tietoturva raportoinnin seurantakohteena. Nämä seurattavat kohteet muodostavat tietoturvan ohjauspaneelin, valvontanäkymän. Monet tietoturva- sekä ICT-toimittajat ovat rakentaneet omat työkalunsa tai asiakkaille tarjottavat palvelut tietoturvan jatkuvaan seurantaan. Tietoturvan monitorointi, kuten muutkin monitoroinnit, ovat usein osin päällekkäisiä toisten alueiden seurannan kanssa, mutta näkökulma ja seurattavat asiat; esim. syklit, kyselyvolyymit, datamäärät ja protokollat

eroavat muusta monitoroinnista. Tietoturvan näkökulmasta haetaan poikkeavuuksia normaaliin toimintaan, kun taas muussa monitoroinnissa usein todennetaan, että järjestelmät toimivat odotetulla tavalla tai ennustetaan tulevaa toimintaa.

Tietoliikennettä monitoroidaan useilla eri työkaluilla ja seurattavia kohteita ovat mm. IP osoitteet, portit, tietoliikenteen määrä, protokollat, verkot. Vastaavasti tietoliikenteen seurantaan on monimutkaisissa infrastruktuureissa käytettäviä kehittyneitä työkaluja ja valvontanäkymiä.

Ohjelmoitava logiikka on kasvavissa määrin tulossa myös kuluttajapuolen tietojärjestelmien valvontamekanismien osaksi IOT-(Internet-Of-Things) teknologian kehityksen myötä. Ohjelmoitavalla logiikalla tarkoitetaan käytännössä pientä tietokonetta tai komponenttia, jota yleensä käytetään tosiaikaisten teollisen tuotannon automaatioprosessien ohjauksessa. Alkujaan teollisuuden käytöstä sittemmin myös kasvavissa määrin kuluttajapuolelle siirtyvää teknologiaa, osana jo vaikkapa kodin pesukonetta, jääkaappia tai liikkeentunnistimia. Haastatellessa monitorointi- ja valvonta-alueen arkkitehtia (Liite 2) nousi tämä monitoroinnin ja valvonnan osa-alue yhtenä keskeisenä monitoroinnin tulevaisuuden kehitysalueena esiin.

Haastatteluiden tuloksina kyettiin antamaan suosituksia nykyisen monitoroinnin sekä työkalujen kehittämiseksi, jotka puolestaan ovat jo edenneet tätä kirjoittaessa tuote-evaluointeihin, toimittaja-arviointeihin ja osaksi yrityksen palveluvalikoimaa. Lisäksi haastatteluissa nousi esiin monia uusia mahdollisuuksia monitoroinnin ja valvonnan yleisen tason kehittämiselle sekä myös uudentyyppisille liiketoimintamahdollisuuksille.

8 Näkökulmia monitoroinnin kehittämiseksi

Teollisen kehityksen historiassa on aina ollut työn suorittajia sekä työn valvojia. Kaleereissa oli rummunhakkaaja kertomassa suoritettavan työn ajallista ulottuvuutta ja vastaavasti työn suorittajia melan kanssa liikuttamassa kaleeria yhteisvoimin eteenpäin. Komentosillalla seisoi hyödyn saajana ja työsuoritteen tilaajana kapteeni antamassa suuntaa kaleerille. Komentosillalta pystyi myös kontrolloimaan työsuoritetta kokonaisuutena.

Nykyisin laivojen komentosillat on pääsääntöisesti suunniteltu toimimaan selkä tehtävään työsuoritteeseen päin, näyttöpaneelien korvatessa työn suoritteen seurannan sekä koneiden suorittaessa fyysisen työn. Tätä aikakauden muutosta kuvaa hyvin laivassa palvelleen johtajan kommentti:

> ” Olen ollut vuosia laivan komentosillalla tähyten horisonttiin ja antanut ohjeita silmilläni hankkimani informaation perusteella. Tietokoneteknologian tultua ei laivan komentaja ole enää komentosillalla. Hän on tietokoneita täynnä olevassa huoneessa. Nyt hän katselee täynnä informaatiota olevia ruutuja ja

> tekee päätöksiä niiden perusteella. Hänellä täytyy olla uusia keinoja niiden ymmärtämiseksi. Hänen täytyy ymmärtää numerot, trendit ja kaaviot ja verrata niitä ympäristön todellisiin tapahtumiin. Hänen täytyy muodostaa päässään tulevaisuudenkuva ruudussa olevan informaation perusteella. Uskon, että pankissa on nyt tapahtumassa samaa – pankkiirilla on samanlainen ongelma." (Zuboff 1990, 195.)

Teollistumisen aikakaudella työn kontrolli perustui pitkälti esimiehen rooliin työn jakajana ja kontrolloijana. Yhteiskunnassa on tapahtunut muutamassa vuosikymmenessä voimakas murros liukuhihnatyöskentelystä aivotyöläisten suorittamaksi tietotyöksi, jossa johdolla ei välttämättä ole täydellistä informaatiota toiminnan ohjaamiseksi (Teittinen ja Auvinen 2014).

Teollistumisen myötä, koneiden korvatessa ihmisen työnsuorittajana, tämä työn suorittamisen sekä seurannan malli on ensin koneellistunut ja sittemmin automatisoitunut informaatioteknologian avulla. Tehtaissa "komentosillat" ovat saaneet oman mallinsa valvomoista sekä kontrollihuoneista, joissa työskentelevät seuraavat työn ts. prosessien toimintaa reagoiden poikkeamiin tarkoin ennalta määriteltyjen ohjeiden perusteella tai kokemusperäisesti. Datakeskusten valvomot eivät juurikaan luonteeltaan eroa valmistavan teollisuuden vastaavista, valvonnan kohteet vain ovat muuttuneet koneiden, sovellusten ja näiden prosessien tai näiden tuottamien prosessien seurantaan. Siirryttäessä poispäin mekaanisesta, valmistavasta teollisuudesta kohti informaatioteknologian kyllästämää yhteiskuntaa, on ajatus komentosillasta tai kontrollihuoneesta kuitenkin taas ajankohtainen. Useat globaalit, eri toimialoja edustavat, yritykset tarjoavat kuluttajille suoraan suunnattua uuden teknologian mahdollistamaa help desk palvelua, esim. ”Opel On Star, henkilökohtainen avustaja” (OPEL 2018) tai ”Apple SIRI, henkilökohtainen puhetunnistukseen perustuva avustaja” (Apple 2018). Vastaavasti useat sovellustoimittajat; mm. BMC, IBM, Oracle, Microsoft, Cisco, jne. tarjoavat omaa holistista kokonaisratkaisua tietojärjestelmien monitorointiin ja valvontaan IT-toimittajille; tosin usein vain omaan teknologia-alueeseensa rajautuen. Tietojärjestelmien valvonnan kannalta haastavaksi muuttuu se, ettei kokonaisarkkitehtuurit koostu juuri koskaan yhden yksittäisen toimittajan teknologiasta per valvottava kokonaisuus, vaan toimittajia, teknologioita sekä loppukäyttäjän kokemaan vaikuttavia tekijöitä on useita.

Miten sitten rakennetaan kokonaisvaltainen seuranta ja kontrollikeskus useista eri teknologioista, toimittajista, tietojärjestelmistä ja arkkitehtuureista koostuvaan kokonaisuuteen? Tulisiko asiakkaalla tai valitulla "päätoimittajalla" olla oma komentosiltansa tai kontrollihuoneensa? Informaatioteknologian maailmassa Pilvi (Pilvi) palvelun tarjoajan tai runkoverkon häiriön ollessa sovellustoimittajan palvelupäällikölle näkymätön, on palvelupäällikkö haasteen

edessä ongelmanratkaisun kanssa, ja ajatellen vielä tietojärjestelmän tuottaman palvelun loppukäyttäjää; jonka oma päätelaite/verkko saattaa olla syynä huonoon palvelukokemaan.

Minkälainen on siis komentosilta tai kontrollihuone vuonna 2025? Jos muinoin orjakaleeri tahdin säilyessä samana alkoi kaartamaan tyyrpuuriin ja kapteeni näki komentosillalta käsin kolme tyhjää soutupenkkiä: oli syy-yhteys selkeä ja hän osasi reagoida asiaan tämän vaatimalla tavalla. Mitkä ovat ne tietosyötteet, impulssit ja miten tulisi valita nämä seurattavat kohteet erilaisista tieto-järjestelmäkokonaisuuksista, jotka palveluvastuullisen tahon tulisi kerätä virtuaaliselle ”komentosillalleen” ja tulevatko ”komentosillat” edelleen säilymään työn kontrollirakenteena ja minkälaisessa formaatissa?

Työn luonne on muuttumassa tai jo muuttunut. Työn tekeminen tietojärjestelmien kanssa ei ole enää välttämättä sidottuna konttoriaikaan tai paikkaan, työ ja työpaikka ovat eriytyneet käsitteinä toisistaan (Demos Helsinki 2017). Työsuorite valvontaan liittyen voidaan tehdä vaikkapa kesämökin laiturilta mobiililaitetta käyttäen ja samalla erilaisiin kansainvälisiin ITSM-hallintaryhmiin kuuluen.

Tietoteknisten kokonaisuuksien rakentuessa kattamaan yhä laajempia kokonaisuuksia Valvonnan ja monitoroinnin muuttuminen yksittäisten komponenttien valvonnasta prosessien ja loppukäyttäjäkokeman mittaamiseen ja edelleen virhetilanteista automaattiseen toipumiseen on syytä pitää mielessä. Tietojärjestelmien Infrastruktuurin hallinnan puolella tämä tarkoittaa vanhakantaisesti kahdennusten ja modernimmin Pilvipalveluiden kasvua ja sekä myös valmistavan teollisuuden puolella käytössä olevan häiriö/kontrolli-automaation lisäämistä häiriötilanteiden korjaamiseksi automatisoidusti myös kuluttajapalveluissa sekä pilvipalveluvalikoiman kasvattamista myös tälle alueelle. Applikaatiopuolella vastaavasti automaattista lokienseurantaa ja häiriötilanteista toipumiseen varautumista prosessiseurannan automatiikan avulla.

Traditionaalisen IT-infrastruktuuriin tottuneet käyttäjät ja hallintatyöntekijät kokevat kontrollin heikentyvän tietojärjestelmien siirtyessä pilvipalveluiden osaksi eri tyyppisin palvelumallein. Tämä asettaa muutoksena valvonnan ja monitoroinnin osalta BCM, APM ja E2E tyyppisten valvontojen tarpeen kasvua, koska nämä kykenevät tarkemmin kohdentamaan ja myös poimimaan häiriötilanteet loppukäyttäjän tai liiketoimintaprosessin näkökulmasta. DevOps-työskentelymalli nopeuttaa huomattavasti sovellusversioiden siirtoa tuotantoon ja sovellushäiriön ilmetessä tämä malli nopeuttaa myös korjaavaa toimenpidettä. Häiriön tapahtuessa vaikkapa asiakkaan joulumyynnin tai muun liiketoimintasesongin aikaan, on vahinko liiketoimintamielessä jo tapahtunut. Tällaisten liiketoimintakriittisten häiriöiden ennaltaehkäisemiseksi tai niistä toipumiseksi tarvitaan siis teollisuuden tuotantolinjoista tuttua häiriönkohdentamisen ja

korjaamisen automatisoitua toimintamallia ja kokonaisvaltaista automatiikkaa samalla vähentäen kaikilta osin tällaisissa häiriötilanteissa toivuttamiseen tarvittavaa manuaalista henkilötyötä.

8.1 Tilaajan ja toimittajan välinen yhteistyö

Tilaajan ja toimittajan välille on syytä rakentaa hallinta- ja toimintamalli, jossa yhteistyössä sovitaan mm. eri palvelunhallintakerrosten; tyypillisesti operatiivinen, taktinen ja strategiset tasot; palaverikäytännöistä ja vuosikellon mukaisesta toiminnasta sekä palvelun avainhenkilöstön yhteistyöstä. Yleensä palveluyhteistyöstä yhteisesti sovitut asiat kuvataan palvelusopimukseen ja tarkemmin tilaajalle toimitettavaan palveluoppaaseen.

> ”Palveluyhteistyöllä tarkoitetaan toimittajan ja asiakkaan tilaajien sekä ICT-avainhenkilöiden palvelun hallintaan liittyvää yhteistyötä. Tämän palveluyhteistyön sujuvuus on olennaista kokonaislaadun kannalta. Palveluyhteistyön ongelmat tai haasteet voivat joskus näkyä vasta myöhemmin loppukäyttäjien palvelussa. Palveluyhteistyön sujuvuus onkin yksi tyypillisistä ennakoivista palvelun laadun mittareista. Palveluyhteistyö on hyvä dokumentoida palvelusopimukseen heti sopimuksen alusta asti.” (JUHTA 2009.)

Palveluyhteistyön kuvaamiselle on formaattina usein liite varsinaisessa sopimuksessa, jossa kuvataan yhteisesti sovittuna tilaajan ja toimittajan välinen hallinta ja toimintamalli. Hallinta ja toimintamallissa kuvataan yhteistyön hallintaan tarvittavat tasot, jotka ovat tyypillisesti Strateginen, Taktinen ja Operatiivinen taso. Lisäksi sovitaan eri ryhmistä, jotka näillä tasoilla toimivat; johtoryhmä, ohjausryhmä, tuotantoryhmä, muutoshallintaryhmä jne. Asiakassuhteen hoitamiseen liittyvät ryhmien päätäntävalta, eskalaatiomenettelyt, avainhenkilöt, tilausmenettelyt ja toimitusten hyväksynnät sekä prosessien rajapinnat ja hallinta. Vastaavasti nämä, kuten kaikki palveluiden käyttämiseen, hallintaan sekä tilaamiseen liittyvät tiedot kuvataan palveluoppaaseen.

8.2 Monitoimittajaympäristöt

Monitoimittajaympäristöt syntyvät tilaajan kilpailutus- ja ostokäyttäytymisen tuloksena ja näillä tilaaja pyrkii saavuttamaan kustannusetuja. Erityyppiset ulkoistusmallit vaativat kuitenkin erityyppisiä hallintamekanismeja ja osaamista tilaajalta tuotannon aikaiseen toimintaan, jos ja kun Tilaajan pilkkoo kokonaisvastuuta palvelukerroksittain (Kuvio 2 ja 3) ja ostaa yksittäisiä palveluita yksittäisiin palveluihin erikoistuneilta toimittajilta yksittäiseen liiketoiminnallisen järjestelmäkokonaisuuteen. Kaikille toimittajille kerroksellista vastuukokonaisuutta ei ole useinkaan esitelty ja kokonaisymmärryksen puutteen vuoksi tilaajalla ja toimittajilla ei välttämättä ole yhteistä visiota, ammatillista kieltä tai selkeästi kommunikoitua päämäärää. Traditionaalisesti tätä kontrollia, palveluiden johtamista ja hallintaa on edustanut tilaajan

oma IT-osasto ja nykyisin nousevassa trendissä oleva SIAM, Service Integration and Management eli Palveluintegraatio-palvelut.

Tekninen kehitys ei ole poistanut kokonaisvalvonnan ja monitoroinnin tarvetta. Palveluiden ostokäytöksen muutos ohjaa myös tilaajan tarvetta valvonnalle ja monitoroinnille. Seuranta ja reagointivastuu häiriötilanteessa jää palveluita ostavalle taholle itselleen tai hajautuu yhtäaikaisesti usealle eri palvelutoimittajalle esim. seuraavalla tavalla; Liiketoimintajärjestelmien seuranta ja valvonta asiakkaalla tai sovellustoimittajalla. Sovellustoimittajan sovellushallintapalveluiden suorittama monitorointi, ja valvonta sekä Konesali, ja kapasiteettipalvelun toimittajan suorittama monitorointi, ja valvonta, tietoliikenne runkoverkkojen seuranta tietoliikennetoimittajan suorittamana sekä tietoturvan seuranta, tilannekuva erillisesti ostettuna palveluntuottajalta. Rakentaessa valvontahuonetta tai valvontanäkymiä mm. yhteiskunnallisesti merkittävien kokonaisuuksien ja tietojärjestelmien seurantaan tulisi em. jaottelun mukaisesti kyetä seuraamaan tietojärjestelmien toimintaa näytöiltä.

Nykyistä vallitsevaa tietojärjestelmien ylläpitovaiheen ostokäyttäytymistä ja palveluiden tahtotilaa onkin usein keskusteluissa verrattu sähkön kuluttamiseen kuluttajana. Vastaavan tyyppinen palvelumalli on nyt teknologian kehityksen myötä siirtynyt IT-Infrastruktuurissa kerroksia ylöspäin kapasiteetin kuluttamiseen. Sähkönsyötön ja tuoton osalta, on olemassa yleismaailmallinen palvelumalli, jossa kuluttaja ostaa sähkön kulutuksensa mukaan ja tietojärjestelmien ylläpidosta taas tyypillisesti SAAS, PAAS, IAAS jne. palvelumallien mukaista palvelupakettien maksua käytön mukaan tai käyttäjämäärän mukaan. Näissä malleissa korostuvat liiketoimintaa tukevien ja tuottavien järjestelmien seurannan vastuut sekä kontrollia varten rakennetut monitorointi, ja valvontajärjestelmät, varsinkin prosessiseurantaan keskittyvät järjestelmät.

Toinen vaikuttava asia ostokäytöksen muutoksen lisäksi on yleismaailmallinen informaation määrän kasvu. Kotikoneiden siirtyminen osaksi tietoverkkoa avaa mielenkiintoisia näkökulmia ja myös liiketoiminnan optimointimahdollisuuksia; esim. jääkaapin kylmätuotteiden kulutuksen seuranta ja monitorointitiedon välittäminen automaattisesti verkon välityksellä myyjälle ja/tai tuottajalle. Tieto kulutuksesta reaaliaikaisesti luo selkeää liiketoiminta etua tämän tyyppisen kulutustiedon haltijalle. Kun tietojärjestelmien ulottuvuus kasvaa edellisen esimerkin mukaisesti meijeristä kaupan lisäksi myös kuluttajan jääkaappiin, se aiheuttaa muutoksia myös monitorointi, ja valvontatarpeille. Liiketoiminnan optimointi kulutustiedon avulla mahdollistuu, mutta järjestelmien ja informaation kasvun myötä myös tämän tyyppisten liiketoimintaa tukevien, fyysisten laitteiden valvontatarpeet lisääntyvät. Kaikkien IoT-laitteiden tu-

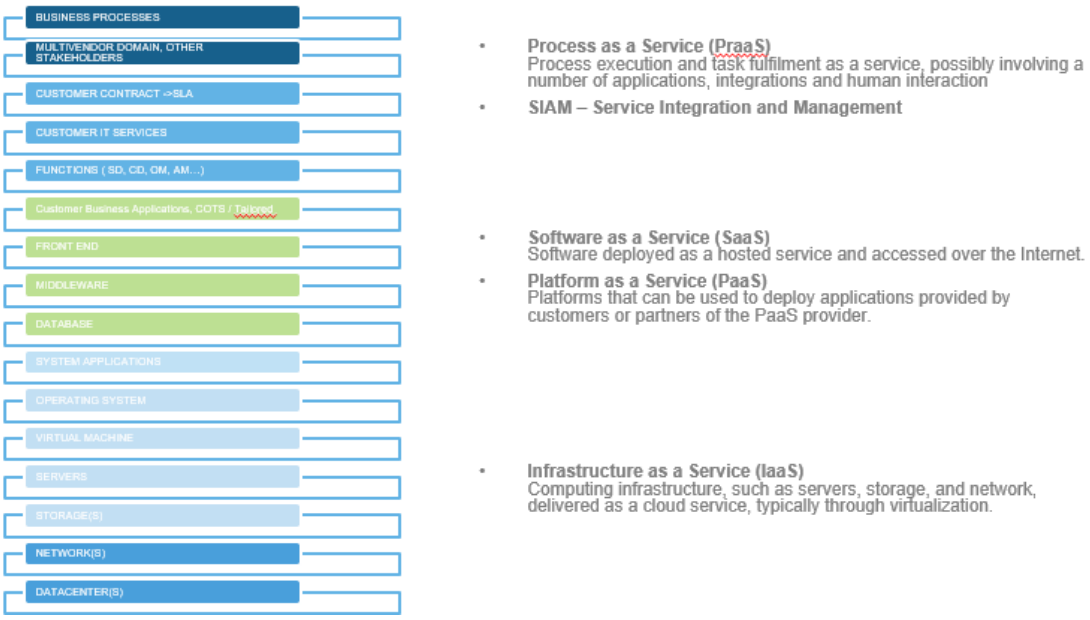
lisi kyetä monitoroimaan omaa statustaan sekä myös ilmoittamaan mahdollisista häiriötilanteistaan. Lisäksi näiden laitteiden tulisi mahdollistaa ulkopuolinen, etähallinta ja valvonta vikatilanteiden hallintaa varten.

8.3 Monitorointi ja valvonta kehikon hahmottelua

Monitorointi, ja valvontaratkaisut tulee rakentaa tietojärjestelmään kokonaisuudessaan; käyttäjien työsuoritteisiin, applikaatioihin, varusohjelmistoihin, teknologiaan sekä infrastruktuuriin. Palvelutaloille on tärkeää valvoa ja seurata useiden asiakkaiden tietojärjestelmien tilannetta ja tarvittaessa puuttua joko valvonnan tuottamaan häiriöön tai raja-arvo muutokseen. Palvelutalot edustavat palvelutarjonnaltaan useita eri teknologioita ja ovat usein kyvykkäitä myös toimittamaan palveluita asiakkaan tarpeiden mukaisesti ympäri vuorokauden. Tämä myös edellyttää palvelutaloilta kykyä reagoida häiriötilanteisiin ja informaatio, sekä järjestelmämäärän kasvaessa myös kykyä vastaanottaa ja hallita automaattisesti erityyppisiä valvontailmoituksia raja-arvojen ylityksistä omalta vastuualueeltaan sekä muilta toimittajilta. Kyvykkyys holistiseen seurantaan ja valvontaan on liiketoiminnallinen etu sekä hyvän palvelu, ja käyttäjäkokemuksen edellytys. Monitoroinnin ja valvonnan kohteiden kasvaessa holistisen näkökulman omaksuminen on tärkeää. Onnistuneesti rakennettuna se vähentää häiriötilanteiden syntyä, häiriökohdennuksen kestoa sekä häiriötilanteesta toipumista.

Traditionaalisessa, kiinteään laitteistokantaan keskittyvässä infrastruktuurissa on valvonnan ja monitoroinnin rakentaminen selkeää. Kyse on pitkälti fyysisen kokoonpanon, lokien, prosessien sekä applikaatioiden toiminnan, raja-arvojen/viitearvojen, seurannasta. Siirryttäessä Pilvipalveluihin muuttuu seuranta asteittain haastavammaksi kokonaisvalvonnan näkökulmasta, sekä samalla siirtyy monitoroinnin ja valvonnan painopiste astetta lähemmäksi liiketoimintaprosessien seurantaa. Palveluiden yleisimpien ostomallin mukaisesti - IAAS, PAAS, SAAS – tulee seurantavastuu vastaavasti kerroksittain lähemmäksi liiketoimintasovellusten valvontaa, palvelutuottajien vastatessa tuottamistaan palveluista. Kokonaisuuden kannalta, vaikka hajautettua ostamista tehtäisiin hallitustikin, vastuuta oman liiketoimintajärjestelmän toimin-

nasta ei viimekädessä kuitenkaan voi täysin ulkoistaa sekä jäännösvastuun mukainen monitorointi ja valvonta tulee järjestää.



Kuvio 2: Kokonaisarkkitehtuuri esimerkki, palvelun osto, ja ulkoistusmalleista; PRAAS, SIAM, SAAS, IAAS

8.4 Goal Directed Design, ”Personat”

Konesali, ja kapasiteettipalveluilla (käyttöpalvelut) on historiallisesti ollut eronsa sovelluspuolen kanssa. Jo Ylen tuottamassa dokumentissa vuodelta 1973 ”Kaikkialla ATK - ammattina ATK” (Arkisto 1973) on nähtävissä ero sovelluspuolen sekä laitteistopuolen välillä. Alan Cooper kirjoittaa vastaavasta erosta kirjassaan ”Inmates are running the asylum” (Cooper 2004, 198) käytettävyyden näkökulmasta: On olemassa laitteistoinsinöörejä, jotka luovat emolevyjä ja mikroprosessoreita ja sitten on olemassa sovellusinsinöörejä, jotka luovat ohjelmakoodia. Vaikka heidän työnsä päämäärä on yhteinen -tai hybrituote, nämä kaksi ryhmittymää eivät tyypillisesti työskentele yhteistyössä.

Sama kahtiajako on edelleen voimassa IT-alalla, on kyse sitten liukuhihnateknologiasta tai sitten palvelutuotannosta. On asiantuntijoita, jotka ovat keskittyneet laitteistopuolen ja/tai näiden käyttöjärjestelmä ja varusohjelmistojen haasteisiin ja asiantuntijoita, jotka kirjoittavat, ylläpitävät ja suunnittelevat sovelluksia.

Cooper myös hahmottelee ”Goal Directed Design” -mallin (Cooper 2004, 151), joka tähtää käytettävyyden sekä ihmisen ja koneen interaktion helppouden maksimoimiseen. Cooper keskittyy kirjassa esimerkein kuluttajaelektroniikan käyttöliittymien vaikeaselkoisuuteen, hän toteaa, että laitteistopuolen yritykset ovat usein kokeneempia hankkimaan ulkopuolista apua teollisen suunnittelun yrityksiltä tehdäkseen tuotteistaan haluttavampia käyttäjilleen. Sama

ajatus kantaa siis myös käytettävyyden rakentamisen monitorointi, ja valvontaohjelmistojen ts. operatiivisten hallintasovellusten puolelle – ei ainoastaan kuluttajien. Palvelutaloilla on rahanarvoisia syitä tutkia vastuullaan olevien tietojärjestelmien häiriötilanteita ja ratkaisuja näihin. Vaikkakin Cooper epäilemättä viitoitti ajatustaan kuluttajille suunnattuihin kappalevalmisteisiin tuotteisiin tai käyttöliittymiin yleisesti, tulisi myös monitorointi, ja valvontakehikkoa suunnitellessa toimittajan rakentaa monitorointi, ja valvontakehikkonsa käytettävyys tukemaan palvelua tuottavia teknologia, ja sovellusasiantuntijoita (taulukko 4). Hallintahenkilöstö ovat näistä tuotteista syntyvien herätteiden ensisijaisia käyttäjiä. Mikäli herätteitä on pakko synnyttää ja niiden synnyttämää vastetta ei voi automatisoida, niin herätteiden formaatti sekä tietosisältö tulisi suunnitella mahdollisimman helpoksi asiantuntijalle, joka näistä syntyvän työsuoritteen saa tehtäväkseen. Herätteessä tulisi olla virhetilanteen kuvauksen lisäksi suora linkki helppokäyttöiseen, selkeään toimintaohjeeseen. Tiedostaen kuitenkin herätteiden volyymin, on aina parempi, mikäli syntyvän herätteen pohjalta on mahdollista suorittaa suoraa järjestelmien välistä häiriön korjaavaa automaatiota.

Ensisijaisesti tulisi tutkia mitä mikäkin hallintatyörooli/persoona haluaa saavuttaa järjestelmissä. Esimerkiksi, jos käyttöpalvelutoimittajalta on kapasiteetti lopuillaan asiakkaan tekemän järjestelmän käytön laajennuksen vuoksi, tilanteesta syntyy tällöin asetettujen raja-arvojen rikkoutumisen myötä hälytyksiä, jotka ohjataan valvontatyökalusta puolestaan Control Deskiin. Täällä tilanne analysoidaan ja toimitetaan työtehtävänä vastaavan teknologiatiimin tehtäväksi, jonka asiantuntija lisää tarvittavan määrän kapasiteettia sovelluksen käyttöön. Vastaavasti tämä työnkulku voidaan myös automatisoida. Pilvinatiiveissa sovelluksissa sovellus taas itse allokoi tarvitsemansa pilvikapasiteetin resurssipoolista, mutta vastaava häiriötilanne saattaa edelleen syntyä, vaikkapa Big data sovelluksien yhtäaikaisen ennakoimattoman tietokannan käytön vuoksi. Vastaavanlaiset, eri tyyppiset tilanteet, tulisi dokumentoida työpyyntöjen määrän ja eri työroolien näkökulmasta ja mahdollisuuksien mukaan ratkoa automatiikan tai interaktion kehittämisen avulla. Taulukossa 4 on tyypillisten palvelutuotantokerrosten ja selektiivisesti valiten järjestelmälle palvelua tuottavien arkkitehtuurikerrosten esimerkki persoonat, joilla on toisistaan irralliset valvonta, ja monitorointiohjelmistot käytössään. Vastaavaa taulukkotyökalua voi hyödyntää tietojärjestelmän ajonaikaisen (tuotanto) vaiheen suunnittelussa.

Arkkitehtuurikerros	Persoona	Valvontanäkymä/työkalu
Liiketoimintaprosessit	Liiketoiminnan omistaja	BPM, E2E
Monitoimittaja ympäristöt, Samaa tietojärjestelmäkokonaisuutta ylläpitävät toimijat	SIAM, palvelujohtaja, palvelunhallinta	Tilannehuone, kaikki liiketoimintajärjestelmän monitorointi, ja valvontakohteet
Toimittajasopimukset ja Palvelutasosopimukset	Palvelupäällikkö	E2E, sopimusvastuiden mukaisesti
Asiakkaan tuotantopalvelut	Tuotantopäällikkö	E2E, sopimusvastuiden mukaisesti
Palvelutuotantoon osallistuvat ryhmät, kuten Service Desk, Control Desk, Konesali, ja kapasiteettipalvelut, sovelluspalvelut	Asiakastuen spesialisti	E2E, sopimusvastuiden mukaisesti
Asiakkaan liiketoimintajärjestelmä, räätälöidyt ohjelmistot tai valmisohjelmistot	Sovellusvastuuhenkilö, pääkäyttäjä	BPM, E2E
Internetpalvelin kerros	Teknologia-alue asiantuntija	Komponenttitason teknologian mukaiset monitorointityökalut
Väliohjelmistot	Teknologia-alue asiantuntija	-”-
Applikaatiot	Teknologia-alue asiantuntija	-”-
Käyttöjärjestelmät	Teknologia-alue asiantuntija	-”-
Virtualisointiratkaisut	Teknologia-alue asiantuntija	-”-
Palvelinhallinta	Teknologia-alue asiantuntija	-”-
Tallennusteknologiat	Teknologia-alue asiantuntija	-”-
Tietoliikenne	Tietoliikenne asiantuntija	-”-
Tietokanta	Tietokanta asiantuntija	Tietokannan monitorointityökalut
Konesali	Tilanhallinnan asiantuntija	Tilaan liittyvät monitorointityökalut, tietoturva, pääsynhallinta, lämpötilat jne.

Taulukko 4: Palveluarkkitehtuurikerrosten ”personat”, joille on eri monitorointi, ja valvontatyökalut käytössään

8.5 Hierarkia, rakenneosat ja holistinen näkymä

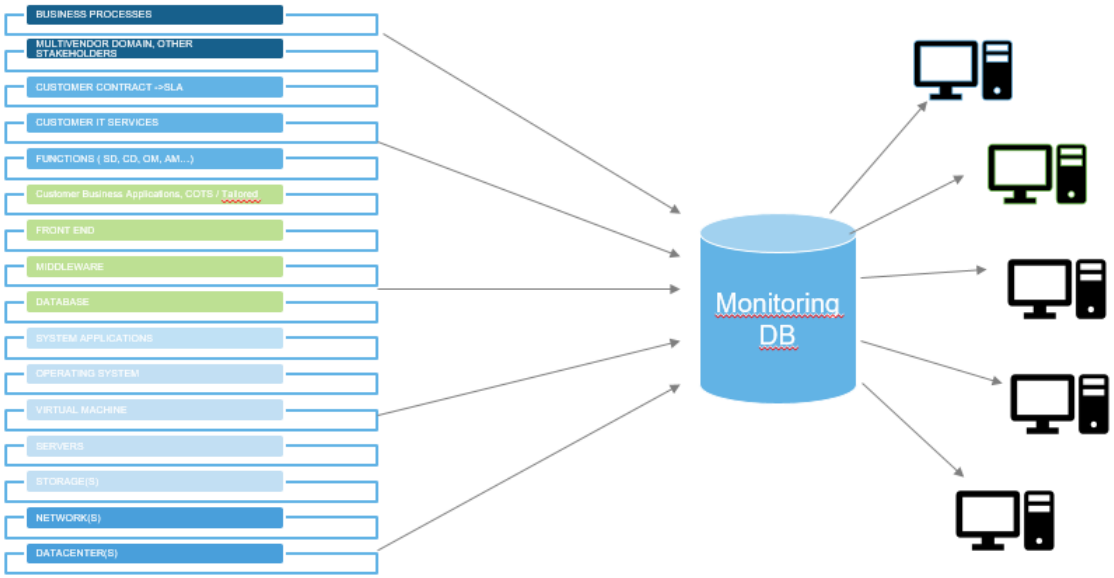
Tietojärjestelmäympäristön komponenttien aiheuttamien, tai riippuvuuksien aiheuttamien häiriöiden tunnistaminen valvontanäkymään voidaan mahdollistaa rakentamalla tietojärjestelmästä hierarkkinen rakennemalli. Yksittäisestä asiakkaan tietojärjestelmästä rakennetaan konfiguraationhallintajärjestelmään rakenneosa (application CI), josta edelleen kuvataan sen loogiset ja tekniset suhteet sekä riippuvuudet muihin arkkitehtuurin kerroksiin, komponentteihin ja järjestelmän hyödyntämiin palveluihin. Liiketoiminnan arvoketjujen tunnistamiseksi on myös hyödyllistä mallintaa eri tietojärjestelmien väliset yhteydet monitorointia ja valvontaa varten. Monilla monitorointi, ja valvontatuotteilla on jo myös sisäänrakennettuna ominaisuutena automatisoitu rakenneosien havainnointi, perustuen tietoliikenteen havainnointiin sekä valvontasovelluksen client-asennuksiin kaikille tietojärjestelmän rakenneosille, joka helpottaa kokonaisuuden rakentamista sekä ajantasaisena pitämistä. ”Tietojärjestelmien välisen

vuorovaikutuskaavion avulla kuvataan prosessien käyttämät tietojärjestelmät ja tietojärjestelmien väliset tietovirrat" (JUHTA 2017).

Valvontaa ja monitorointia varten hierarkia mallinnetaan käyttäjästä, käyttäjäryhmistä ja verkkoteknisestä käyttöpisteestä alkaen edelleen tietojärjestelmään ja järjestelmästä valitaan sen toimintaa parhaiten kuvaavat käyttötapaukset, joiden monitoroinnilla voidaan todentaa järjestelmän haluttu toiminta. Tietojärjestelmän monitorointi ja valvonta sekä eri käyttäjäryhmille suunnatut valvontavastuiden mukaiset näkymät kerätystä monitorointidatasta. (ks. kuvio 3.) Varsinaiset näkymät tulee mallintaa tietojärjestelmän käyttäjä, ja oikeusryhmien avulla – huomioiden käytettävyyden sekä tietoturvan periaatteet, että käyttäjälle näytetään vain ja ainoastaan kunkin työroolin tarvitsemat tiedot. Lisäksi tietojärjestelmien kerroksellisuus edellyttää taas usein eri tyyppisten ja monitorointimekanismien yhdistämistä. (ks. kuvio 4.)

Monitorointi, ja valvontaohjelmistojen valintaa edeltää kuitenkin järjestelmän arkkitehtuurin loogisesta, teknisestä, sekä palvelurakenteesta mallinnettava hierarkia, karkea esimerkki tästä on kuviossa 1. Looginen rakenne kertoo tietojärjestelmän informaatiorakenteen, jota tekninen arkkitehtuuri täydentää seurattavien komponenttien sekä relaatioiden osalta.

Palvelurakenne taas kertoo järjestelmän monitorointiin ja valvontaan osallistuvien toimittajien vastuut sekä hyvin suunniteltuna myös toimittajille yhteiset monitorointitietokannat ja palveluvastuiden mukaiset valvontamekanismit.



Kuvio 3: Tietojärjestelmän monitorointi ja valvonta sekä eri käyttäjäryhmille suunnatut valvontavastuiden mukaiset näkymät kerätystä monitorointidatasta.

Kuviossa 4 on esimerkki ja informaation rakenne-ehdotus valvontarakenteesta ympäristöjen, kerroksellisuuden ja monitorointirakenteen sekä näistä tuotetusta käyttöpalvelutoimittajan valvontanäkymästä, kattaen kuviossa 4 esitetyn informaatiorakenteen mukaisen monitoroinnin ja valvonnan relaatioineen:

Näkymä: Domain ”NN”
- Asiakas 1 _Tuotanto_Ympäristö
    - Asiakkaan liiketoimintajärjestelmä 1
        - E2E monitorointi, transaktiot
        - URL (järjestelmän testisivut, etc.)
        - RUM, Loppukäyttäjä-monitorointi
        - Sovellusalusta(t), transaktiot
            - Tietokanta
            - Microsoft
            - Java
            - Weblogic, WAS, jboss jne.
            - Oracle
        - Palvelimet
        - Tietoliikenne
        - Tietoturva
        - Jaetun infrastruktuurin monitorointi
    - Asiakkaan liiketoimintajärjestelmä 2
        - ...Katso yllä
- Asiakas 1_Testi_Ympäristö
    - ...katso yllä

Asiakas 2
- Asiakkaan 2 liiketoimintajärjestelmä 1
- jne.

Kuvio 4: Tietohierarkia ja rakenne esimerkki asiakkaan ja tietojärjestelmän rakenneosien mukaisesti koostettuna tilannekuvaksi (Dashboard) operoivan henkilöstön käyttöön

8.6 Kontrollihuone

Kontrollihuoneella, Operations Control Center (OCC), tarkoitetaan yhtenäistä tilaa, josta valvotaan tuotantoa tai tarkemmin sanoen tuotannon tilaa monitorien avulla. Kontrollikeskuksissa on tyypillisesti isot monitorit, joista voidaan seurata kaikkia tuotannon toimintaan vaikuttavia tärkeimpiä kohteita. IT-alan toimittajilla tämä tarkoittaa asiakkaiden tietojärjestelmien, palveluiden ja tuotteiden, prosessien, sekä keskeisten muiden olennaisten seurantakohteiden seurantaa. Todennäköisesti historiallisesti tunnetuin kontrollihuone on NASA:n ensimmäisen kuulennon, Apollo11, kontrollikeskus, ”Mission Control Center” (NASA 2014), josta lähetettiin kuvaa miljooniin kotitalouksiin ympäri maailmaa vuonna 1969. Kontrollihuoneet yleistyivät tuottavassa teollisuudessa 1920-luvun lopulla.

8.7 Kontrollihuoneessa seurattavat kohteet

Miltä menestys ja onnistuminen näyttää? Mistä voidaan arvioida, onko tiettyä tarvetta varten rakennettu tietojärjestelmä, palvelu tai komponentit saavutettavissa? Entä toimivatko ne luotettavasti, riittävän nopeasti tai ovatko ne helppokäyttöisiä käyttäjilleen? Saavutetaanko järjestelmän avulla tavoite, mitä varten se on olemassa? Näiden fundamenttikysymysten avulla

on mahdollista rakentaa kontrollihuone, joka palvelee tiettyä tarkoitusta hankkeelle tai organisaatiolle.

Kontrollihuoneessa on yleensä esillä erityyppiset valvontanäkymät, kojetaulut (dashboard) joiden avulla voidaan seurata eri tyyppisiä tavoitteelle painoarvoa omaavia näkökulmia kuten palveluprosessien toimintaa, komponenttien tilaa ja suoriutumista tai odotettujen lopputuotosten syntymistä, tilanteesta riippuen ja tavoitteesta juonnettuna. Valittavien mittareiden tulee noudattaa ”SMART (Specific, Measurable, Achievable, Relevant, Timely)” periaatetta (VanHaren 2006). Jotta mittareista saadaan riittävää informaatiota jatkuvan palvelun parantamisen, ITIL CSI, prosessin mahdollistamiseksi, tulee organisaation kerätä kolmen tyyppistä tietoa: Teknologia, Prosessi, ja Palvelumetriikoita (ITIL SO 2010). Kojetaulujen yleisimpiin epänormaaleihin tilanteisiin tulee varautua mahdollisimman pitkälle selkein toimintaohjein sekä jokaisesta eteen tulleesta tilanteesta tulee edelleen rakentaa operatiivista ohjeistusta. Mitattavien kohteiden tulee pysyä ajantasaisena ja näin ollen näiden tulee olla muutoksenhallintaprosessin piirissä. Mittareiden päivittäminen ja ajantasaisena pitäminen sekä kehittäminen tulee olla osa tietojärjestelmien kehitysprosessia ja huomioitava arkkitehtuurisuunnittelun yhteydessä osana ajonaikaisia menettelyitä sekä hallintatyökaluja.

9 Yhteenveto

Tutkimuksen aluksi esitettyihin kysymyksiin saatiin teoriakatsauksen sekä haastatteluiden avulla selville haasteet, joista suurimpana nousi esiin kontekstin puute; asiantuntija saa hälytyksen häiriöstä, mutta ei sen perusteella tiedä mihin käyttökontekstiin se liittyy eikä häiriötilanteessa ehdi tätä lähteä selvittämään, koska ensisijainen tehtävä on korjata tilanne.

Kokonaisvaltaisesta näkökulmasta, haastatteluiden pohjalta piirretty kokonaisarkkitehtuurinäkymä (Kuvio 3) monitorointiin ratkoisi edellä mainittua ongelmaa. Käytössä olevat tekniikat mahdollistavat pitkälti tahtotilan mukaisen valvontanäkymän ja periaatteet, jotka valvontanäkymä tulisi rakentaa selvisi haastatteluiden ja niitä seuranneiden keskusteluiden avulla. Nämä ovat kuvattuna kuviossa 3 ja 4.

Lisäksi työn tuloksina ja ohella syntyivät kohdeyritykselle tämänhetkisten monitorointityökalujen kyvykkyyksien arviointi, työkaluvalinta, olemassa olleen monitorointipalvelun uudelleenmuotoilua sekä konseptuaalinen arkkitehtuurirakenne sekä Informaatiorakenne ison datan jäsentämiseen monitorointidatasta

Kysymykseen kuinka moniulotteinen tehtävä monitoroinnin ja valvonnan kokonaisuus ylipäätänsä on, löytyi tämän työn kontekstiin riittävä vastaus ja haastatteluiden tuotoksena syntyi

myös pohdiskelua tulevaisuuteen liittyen, joista asiantuntijoilla oli jo tiedossa olevia toteutuksia saman yrityksen sisältä.

Kysymykseen valittavista tietosyötteistä ja impulsseista tietojärjestelmissä, vastaus on moniulotteinen. Varsinaisten haastatteluiden osalta en löytänyt suoraa vastausta kysymykseen, mutta haastatteluiden, keskusteluiden ja teorian törmätessä syntyi paljon uusia ajatuksia sekä käsitteitä ja oppimista, joita olen edelleen kuvannut laajalti pohdintaa kappaleessa.

Erityistä haastetta työlle ja tutkijalle tuli jatkuvasti kehittyvästä alueesta ja alati muuttuvasta sekä päällekkäisistä termistöistä, jotka vaihtuvat toimittajalta toiselle eivätkä myöskään ole sisällöltään yhteismitallisia.

10 Pohdintaa

Työskentelin aiemmin kansainvälisessä yrityksessä systeemisuunnittelijana tarkkaan suunnitellussa tietojärjestelmän uudistushankkeessa, jossa korvattiin asiakkaan aikaisempia, asiakkaan vanhoja ja elinkaarensa loppuvaiheessa olevia järjestelmiä (ns. legacy-järjestelmiä) uudella kolmitasoarkkitehtuurin mutkaisella kokonaisuudella. Yhtenä tehtävänäni oli suunnitella ja käyttöönottaa web-pohjainen käytöntukijärjestelmä, joka integroituisi helposti J2EE-järjestelmiin ja toisaalta tukisi helposti sisällöntuottamista substanssiosaajien toimesta. Myöhemmin, järjestelmän valmistuttua, keskustelin erään kollegan kanssa käytöntuki ja ohjeistusjärjestelmien luonteesta. Kollegallani oli ollut samoihin aikoihin vastaava työtehtävä valmistavan teollisuuden puolella, jossa käytöntuki, ja ohjausjärjestelmän tehtävänä ei ollut ainoastaan olla loppukäyttäjän informointikanava ja ohjekanta, vaan toimia myös aktiivisena järjestelmänä, jonka tehtäviin kuului virhetilanteiden havaitseminen, automaattinen korjaaminen ja tämän jälkeen käyttäjän informointi tapahtuneesta. Kaksi samankaltaiseen tarkoitukseen suunniteltua järjestelmää, joista toinen oli passiivinen informointijärjestelmä ja toinen tiukasti teollisuuteen ja tuotantolinjaan integroitu tuotannonohjauksen virhetilanteiden hallintaan liittyvä tukijärjestelmä. Keskustelu oli mielenkiintoinen ja herätti monia ajatuksia ATK:n, Automaattisen Tietojen Käsittelyn, perimmäisestä tarkoituksesta. Järjestelmiä rakennetaan asiakkaiden liiketoiminnan tukemiseen. Rakentamani web-pohjainen järjestelmä ei korjannut virheitä, muilta osin kuin huomauttaen virheellisestä tietosisällöstä dynaamisilla lomakkeilla; varsinaisen korjaustyön jäädessä edelleen järjestelmän käyttäjän tehtäväksi. Internet-sivujen ja internetjärjestelmien luonteeseen ei ole kuulunut vastaavalla tavalla automatisaation hyödyntäminen kuin valmistavan teollisuuden järjestelmissä on jo historiallisesti ollut. Liiketoiminnan prosessien mallintaminen tukemaan liiketoimintaa ei tarkoita pelkästään manuaalisten tehtävien toistamista helppokäyttöisenä uudessa teknologiassa vaan ensisijaisesti tekniikan käyttöönottoa korvaamaan ihmisen suorittamaa työtä ja näin vähentämään ihmisen suorittaman työn virhealttiutta, epäloogisuutta sekä yleisesti tehostamaan liiketoimintaprosessien kulkua. Vastaava pohdintaa voi sisällyttää myös IT-järjestelmien monitorointiin ja valvontaan kummankin ollessa liiketoiminnalle ratkaisevan tärkeä ominaispiirre. Internetin

aikakaudella tietojärjestelmien kokonaisuuden monitorointi, ja valvontakäytännöt eivät usein ole noudattaneet valmistavalle teollisuudelle ominaista tietojärjestelmien automaatiota tai automaattista virhetilanteiden hallintaa. Tämä edellä kuvattu kokemus on myös toiminut keskeisenä taustahavaintoja ja huomiona lopputyön aiheen valinnalle sekä taustoittanut työtä pitkälti.

10.1 Monitoroinnin ja valvonnan tulevaisuus

Tieteiskirjallisuus usein hahmottelee fantasiamaailmoja tai tulevaisuutta kirjallisin ja elokuvateknisin keinoin. Maailmat, joita kirjailijat ja taiteilijat luovat ovat usein mielikuvituksellisia ja mahdottomia toteuttaa teknisin keinoin. Kuitenkin usein on niin, että tieteiskirjallisuus ruokkii insinöörien mieltä ja toisaalta tekniset innovaatiot taas ruokkivat puolestaan kirjailijoiden mieltä. Ohjauspaneelit ja kontrollit, joita em. elokuvissa järjestelmissä esitellään ovat luonnollisesti mielikuvituksen tuotetta, mutta toisaalta niin ovat myös Powerpoint-esitykset, prototyypit ja demoesitykset, joiden perusteella järjestelmätoimittajat esittelevät tulevia järjestelmiään. Esimerkkejä elokuvista ja kirjallisuudesta on viljalti. Nykyisen Wikipedian kaltaisen konseptin ja samalla älypuhelimen/tabletin perusajatuksen esitteli Douglas Adams kirjassaan Linnunradan käsikirja liftareille (Adams 1979).

Vastaavasti ohjauspaneelien visuaalisia malleja on olemassa viihdeteollisuuden esittelemänä runsaasti, esimerkiksi Tom Cruise, Minority Report, 2002, elokuvassa käytti kontrollihansikasta ohjatakseen läpinäkyvää kosketuspaneelia tai hologrammia (Underkoffler 2017).

Nyt 15 vuotta myöhemmin, Augmented reality tai Mixed reality (MS) sekä aiemmin mielikuvituksellisilta vaikuttaneet käyttöliittymät ovat jo olemassa olevaa teknologiaa useilla toimittajilla, myös Underkofflerin omassa Oblong nimisessä yrityksessä (Oblong 2018).

Modernit sovellutukset kuvantamisen ja 3D-mallinnuksen kanssa avaavat täysin uusia mahdollisuuksia myös työn seurannalle ja valvonnalle, joiden pintaa on tuskin edes raapaistu vielä.

Vaikuttaa jopa siltä, että kaiken minkä ihminen voi kuvitella ja visualisoida – voidaan myös aikanaan rakentaa. Useat nykypäivän monitorointi, ja valvontaratkaisut on suunniteltu tukemaan valvontavaatimuksia, jotka infrastruktuuri, sovellusarkkitehtuuri ja liiketoiminnan luonne ovat asettaneet.

Tietotekninen kehitys 60-70 -luvuilta alkaen on hiljalleen muovannut ja kehittänyt tietoliikenteen, prosessorien, levyratkaisuiden sekä applikaatiotason innovaatioiden kautta infrastruktuuria. Infrastruktuurin rakenne ja sen fyysiset ominaisuudet; palvelimet, reitittimet, konesalit, tietoliikenteen siirtokyky, ovat pitkälti asettaneet reunaehdot sekä vakiinnuttaneet hiljalleen kehittyvät tarpeet monitoroinnille ja valvonnalle. Vasta, ja nyt, kehityksen saavutettua pisteen, jossa yksittäiset infrastruktuurin komponentit ja näiden reunaehdot eivät enää yksin

sanele rajoja ja tarpeita sovellusten valvonnalle – on tarve yksittäisellä järjestelmän omistajalla omalle IT-infrastruktuurin seurannalle pilvipalveluiden yleistymisen myötä selkeästi vähentynyt. Konesali – ja kapasiteettipalveluiden ostomalli on muuttunut ja näitä ostetaan palveluina, kuten majoitusta, sähköä tai vettä. Infrastruktuuripalvelut palveluna, IAAS, on malli, joka mahdollistaa kuluttajalle laitteistopuolen kokonaisuuden ostamisen palveluna, ilman tähän kokonaisuuteen liittyvää, usein mutkikastakin, kerroksellista kustannushallintaa. (Sähkö, Jäähdytys, laitteistot, konesalitilat, Lisenssit, palvelimet, sertifikaatit, versioinnit jne.)

10.2 Monitorointi, koneoppiminen ja tekoäly (Artificial Intelligence, AI)

Monitoroinnille ja valvonnalle on viime aikoina kehittynyt omaa kysyntää myös teko, tai keinoälysovellusten puolella. Markkinoilla on jo nyt usean eri toimittajan tarjoamia järjestelmien tekoälysovelluksia, kuten esimerkiksi Dynatrace Ruxit tai SalesForcen Einstein. Perusajatuksena on ison tietomassan hyödyntäminen datalouhinnan ja koneoppimisen avulla. Tekoäly tai keinoäly termejä käytetään markkinoilla melko villisti ja vapaasti tuotteista, jotka perustuvat koneoppimiseen. Koneoppiminen on tekoälyn osa-alue.

Seuraava suuri kehitysaskel monitoroinnin ja valvonnan alueella tapahtuu eittämättä datan keruun ja koneoppimisen alueella; häiriötilanteisiin reagoinnin automatisoinnin ja tätä tukevan datankeruumekanismin sekä sovellusrakenteiden alueilla. Shoshana Zuboff kirjoittaa 1980-luvulla kirjassaan ”Viisaan koneen aikakausi” seuraavasti:

> ”Eron tekeminen automatisoinnin ja informatisoinnin välillä antaa yhden tavan ymmärtää, kuinka tämä teknologia edustaa sekä jatkuvuutta että epäjatkuvuuskohtaa teollisen historian perinteessä. Niin kauan kuin teknologia käsitetään kapeasti automaattisina tekniikoina, se jatkaa sitä teollisen koneen logiikkaa, joka tämän vuosisadan ajan on tehnyt mahdolliseksi rationalisoida työtä ja vähentää riippuvuutta ihmisen ammattitaidosta.” ja jatkaa: ” Informatisointi johtuu automatisaatiosta ja perustuu siihen. Automatisointi on tarpeellinen, muttei riittävä edellytys informatisoinnille. On aivan mahdollista jatkaa automatisointia välittämättä siitä, kuinka se vaikuttaa teknologian informatisointimahdollisuuksiin. Kun näin tapahtuu, informatisointi on suunnittelematon seuraus automatisaatiosta”. (Zuboff 1990.)

Vastaavasti, edellistä täydentäen, 30 vuotta myöhemmin, voidaan ajatella monitoroinnin ja valvonnan näkökulmasta, ettei automatisaatiosta ja informatisointi mahdollisuuksia ole käytetty riittävällä tasolla sen mahdollisuuksia ole hyödynnetty. Big data -konseptin ajatus on seuraamusta tästä havainnosta ja osin siitä, että koska informatisoinnista on tullut luonteva

lisä tuotteiden ominaisuuksiin – syntyy tietoa hallitsemattomia määriä ja tätä syntyvää tietomassaa hyödynnetään suhteellisen vähän. Kyse on siis pitkälti olemassa olevan tiedon jäsentämisestä ja systemaattisesta analysoinnista automaattisen tietojenkäsittelyn keinoin.

Koneoppimista on puolestaan määritelty esimerkiksi Wikipedian sivuilla seuraavasti: ”Koneoppiminen on tekoälyn osa-alue, jonka tarkoituksena on saada ohjelmisto toimimaan entistä paremmin pohjatiedon ja mahdollisen käyttäjän toiminnan perusteella”

Hoyer puolestaan määrittelee koneoppimisen seuraavasti:

”Koneoppiminen määritelmä:

Kone = Tietokone, tietokoneohjelma

Oppiminen = Ongelmanratkaisukyvyn parantaminen kokemuksen avulla”. (Hoyer 2019.)

Monitoroinnin ja valvonnan näkökulmasta syntyvää dataa tulisi loogisten kokonaisuuksien ja riippuvuuksien osalta systemaattisesti analysoida vasten lähtötilannetta sekä saadusta syötteestä tunnistaa normaali tilanne sekä epänormaalit tilanteet luodun algoritmin toimesta. Tämän lisäksi tulee ohjelmistoista tunnistaa yleisimmät häiriötilanteet ja rakentaa niihin sopiva automaattinen mekanismi kutakin potentiaalista häiriö, tai virhekäyttötilannetta ja tilanteesta toipumista varten. Koneoppiminen perustuu siis tässä yhteydessä ohjelmiston kykyyn tunnistaa normaalit tilanteet ja havaita epänormaalit tilanteet ja ohjelmallisesti oppia laajasta ja alati kasvavasta tietomäärästä. Järjestelmän käytön muuttuessa tämän tehtävän tulisi olla jatkuvaa, automatisoitua toimintaa sekä oppimista järjestelmän tuotannosta ja sen alati muuttuvista tilanteesta. Monitorointi, ja valvontadatasta on mahdollista tunnistaa rajaarvoja, arvioida häiriöiden todennäköisyyksiä, arvioida laitteistojen elinkaaria, havaita käytön ongelmia sekä lukuisia muita trendejä sekä muita ihmisvoimin työmäärältään mahdottomaksi venyviä ennusteita ja analyyseja.

Valvonnan ja monitoroinnin kehitys on ollut pitkään hitaassa kehitysvaiheessa, ja osin pysähtynyt internetin aikakauden alkuvaiheessa. Manuaalinen työstä on siirrytty IT-avusteiseen työhön ja edelleen automatisoituun työhön. Se mitä koneellisen teollisuuden puolella on tapahtunut luontevana askeleena ihmisruumiin avulla tehtävän työn automatisoinnin yhteydessä robotisoinnin ja informatisoinnin seurauksena syntynyt prosessiohjaus ei ole sellaisenaan ja luontevasti tullut käyttöön Internetissä toimivien tietojärjestelmien ylläpitotyön osaksi. Todennäköisenä syynä tähän on se, että kuten teollisuuden järjestelmäkehityksen historiassa;

ensin työ on tehty manuaalisesti ja vasta sitten kun manuaalinen työskentelytapa on pilkottu osakokonaisuuksiin, vakiintunut ja dokumentoitu – on sen automatisointia voitu ajatella.

Internettiin rakennettujen järjestelmien tavoitteena on usein ollut vanhojen tietojärjestelmien toiminnallisuuksien siirto internetin kautta käytettäväksi; selainkäyttöliittymän ja sittemmin mobiilipäätelaitteiden kautta tavoitettavaksi. Näin on ensisijaisesti vapauduttu päätelaitteille suunniteltujen sovelluksien asennuksista, rajatusta työn fyysisestä sijainnista sekä mahdollistettu liikkuvuutta. Internetin kautta toimivien tietojärjestelmien yhä laajempi ja kasvava yhteiskunnallinen kirjo mahdollistaa yli traditionaalisten organisaatio tai toimittaja, tai toimitusketjujen rakentumisen, muokkaa liiketoimintamalleja ja luo kokonaan uusia liiketoimintamahdollisuuksia. Päätelaitteiden määrällinen kasvu ja sensoriteknologian yleistyminen antaa mahdollisuuden mitata yhä erilaisimpia kohteita sekä yhteyksiä.

Tällä hetkellä monet toimittajat tarjoavat erilaisin IT-markkinointiakronyymien avulla myytäviä palveluita IT-alalla tapahtuvaan kokonaisvalvontaan. Näiden valvonta, ja monitorointituotteiden perusongelmana on se, että ne ovat usein itse osa valvottavaa kokonaisuutta ja näin ollen eivät voi koskaan täysin vastata tarpeeseen. Toinen keskeinen haastatteluista havainto on se, että laajimmillaankin nämä tuotteet kattavat käyttöpalvelutoimittajan näkökulmasta edelleenkin vain suppean osan tietojärjestelmään vaikuttavista kokonaistekijöistä. Tietojärjestelmän E2E-valvonnalla saavutetaan loppukäyttäjäkokeman tilannekuva ja yksittäisten tietojärjestelmän operaatioiden tai prosessien vasteajan mittaustulokset. Nykyiset valvonta- ja monitorointimekanismit ovat rakentuneet ja rakennettu tukemaan jo mennyttä maailmaa ja eivät siten vastaa nykyisiin haasteisiin järjestelmien monimutkaistuessa ja järjestelmien määrän kasvaessa. JHS-suositukset huomioivat saman ongelman suosituksessa JHS 174, kpl 8.2.1 Päästä-päähän-valvonta (JUHTA 2009).

Kokonaisvaltaisen seuranta, ja kontrollikeskuksen toiminto vaati toimittajalta kykyä 24/7/365 tyyppiseen palvelukyvykkyyteen, näitä ovat mm. Service Desk & Control Desk sekä kasvavissa määrin suoraan asiakkaan tietojärjestelmiin keskittyvä teknologia ja liiketoimintaosaaminen. Suuri hajonta eri teknologioiden tai asiakaskunnan liiketoimintaan erikoistuneen ”help desk” tai ”on-site” -tyyppisen tuen kanssa aiheuttaa haasteita toimittajille ja uskoakseni johtaa aikaa myöten IT-alan toimialakohtaiseen standardisoitumiseen ja teknologiakirjon keskittymiseen sekä yleisesti IT-yritysten keskittymisen tietyn palvelutarpeen mukaiseen palvelutuotantoon. Palvelutalon kontrollikeskuksen tulee siis kyetä seuraamaan tuottamiansa palveluita lisäksi asiakkaan liiketoimintakokonaisuutta ja ymmärtää tukemansa alueen vaikutus asiakkaan liiketoimintaan kokonaisuudessaan.

Tutkimuskysymykseeni ”Tulisiko asiakkaalla tai valitulla "päätoimittajalla" olla oma komentosiltansa tai kontrollihuoneensa?” vastaus on osittain edellä. Tämä kysymys jää silti siltä osin avoimeksi, miten asiakkaiden ostokäyttäytyminen muokkautuu palvelutarjonnan myötä ja

kuinka paljon asiakkaat itse pyrkivät pitämään kontrollia IT:stä itsellään, omassa IT-palvelutuotantoyksikössään tai vastaavasti hajaannuttamaan palveluita ostaen ne useilta eri tahoilta.

Tietojärjestelmien ollessa kiinteä osa liiketoimintaa, on sen kokonaan ulkoistaminen ajatuksena usein vieras ja ulkoistamisen myötä toimittaja kontrollin tarve kasvaa. Kontrollin tarve materialisoituu sopimustekniikassa SLA-sopimuksin sekä jatkuvuus, sekä raportointivaatein.

Tietojärjestelmien palvelutuotannon kokonaisuuden osienkin hajauttaminen vaatii edelleen IT-osaamista tilaajayritykseen, mm. palveluiden ostamisen, palveluiden hallinnan ja sopimusjuridiikan hallinnan vuoksi sekä palvelutuotannon jatkuva seuranta kustannuksineen vaatii tätä myös. Vaakalaudalla on siis yhden kokonaispalvelutoimittajan loukku vastaan usean eri palvelutoimittajan loukku ja hajautetun kokonaisuuden seuranta, korostuneen valvonta, ja monitorointitarpeen -kontrollin- kera.

IT palveluiden toimittajat ovat tunnistaneet ja reagoineet yllä mainittuun ongelmaan edelleen erilaisin palvelutarjoamin; SIAM, eli Service Integration and Management, jossa yksi toimittaja ottaa kokonaisvastuun asiakkaan tietojärjestelmäympäristöstä tai traditionaalinen kumppaniyritysmalli, jossa tietohallintoyksikkö on yhteinen tilaajalle ja toimittajalle. Palvelumalleissa osittaisina ratkaisuina näitä on teknologia, prosessi tai toiminnekohtaisissa ”As A Service” -malleissa, joiden kirjo on alati kasvavaa.

Sovellusrakentamisen ja ylläpidon sekä toimivien tiimien muodostamisen näkökulmasta DevOps, Development and Operations, ajattelu tai toimintatapa pyrkii osaltaan myös selkeyttämään em. kokonaisuutta. Optimaalisia tiimirakenteita on esitelty maailmalla onnistuneista toteutuksista sekä myös erilaisia antimalleja toimimattomiksi osoittautuneista tiimirakenteista. (devopstopologies.com 2019).

Kaksi yleisesti IT-alalla käytössä olevaa termiä: ”Definition of Done” ja ”End to End, E2E” käsitteiden purkamatta jättäminen aiheuttaa usein kommunikaatiohäiriöitä, kaikkien tahojen ymmärtäessä nämä termit ainoastaan omalta näkökulmaltaan. Toimittajilla, joilla on valmius tiettyjen teknologioiden tai palvelutyyppien tukeen, on usein näitä teknologioita tukeva palveluorganisaatio, joka kykenee massatuottamaan palveluita näillä alueilla yhtäaikaisesti useille eri asiakkaille ja tietojärjestelmille, näille rakennettujen monitorointikontrollien avulla.

Yksittäiselle tietojärjestelmälle rakennettavat, koko infrastruktuurin sekä tietojärjestelmän kattavat monitorointi, ja valvontajärjestelmät, ovat usein hyvin toimivia ja palvelevat yksittäistä asiakasta sekä palvelutuotantoon osallistuvia toimijoita hyvin. Valvottavien kohteiden määrän kasvaessa, niiden tuottaman informaation määrä vastaavasti kasvaa. Ilman tehokasta

automatiikkaa, keskittymistä valittuihin teknologioihin, asiakassegmentteihin ja liiketoiminnallisten ketjujen hallintaan, kasvaa manuaalisen heräte työn määrä palvelutoimittajalle hyvin hajanaiseksi sekä määrältään suureksi.

Keskittyminen valikoitujen arvoketjujen kokonaishallintaan onkin edellytys ja samalla vastaus tutkimukseni toiseen kysymykseen: ”miten rakennetaan seuranta ja kontrollikeskus useista eri teknologioista, toimittajista, tietojärjestelmistä ja arkkitehtuureista koostuvaan kokonaisuuteen?”

Minkälainen on siis komentosilta tai kontrollihuone vuonna 2025? Perusolettamuksena seuraavassa pohdinnassa on tietojärjestelmien määrän kasvu ja ulottuminen myös kuluttajapalveluihin joka kodin sekä kulutuselektroniikan osaksi.

Mikään haastatteluissa saamani tieto ei sinänsä yli kirjoita tai vähennä tarvetta kontrollihuone tyyppiselle funktiolle. Päinvastoin, eri haastatteluissa ja näitä seuranneissa keskusteluissani saamani informaatio antaa ymmärtää, että valvonnan ja monitoroinnin määrä tulevaisuudessa tulee voimakkaasti kasvamaan, (mm. IoT), ja tämän vuoksi tulee nykyisten palveluiden, että kontrollihuoneiden määrä kasvamaan sekä spesifioitumaan seurattavien kohteiden muuttuessa palvelukerroksissa lähemmäs käyttäjää. Kontrollihuoneen muoto tulee muuttumaan ja kontrollihuone itsessään tulee todennäköisesti muuttumaan käsitteenä virtuaalisemmaksi. Eri aihe, ja vastuurakenteiden ympärille rakentuu jo nykyisin virtuaalisia työtiloja, joiden kiinteänä osana on tarvittavat tilannekuvat ja hälytysten seuranta. Ennakoin valmistavasta teollisuudesta tuttujen virhe, ja häiriötilanteiden automaattisten mekanismien yleistymistä myös kuluttajasegmentille sekä näistä syntyvien hallinta, ja tilannenäkymien että ihmisen tekemää päätäntää vaativien tilanteiden keskittymistä selkeämmiksi päätöksentekotilanteiksi eri tyyppisten automaattisten häiriönkorjausvaihtoehtojen valintatilanteissa, joissa ei päätäntää voi syystä tai toisesta jättää keinoälyn päätettäväksi.

Tietojärjestelmien tuotannon ajonaikaisten valvonta, ja operointitehtävien määrä tulee kasvamaan pelkästään jo tietojärjestelmien määrän kasvun vuoksi ja samanaikaisesti myös häiriönkohdennukseen ja korjaukseen liittyvän työn automatisoinnin määrä tulee kasvamaan.

Palvelutoimittajilla kontrollihuoneen tarve tulee kasvamaan ja palvelutuottajan kontrollihuone vuonna 2025 on varmastikin fyysisenä tilana samantyyppinen, kuin nykyisinkin, mutta samalla myös virtuaalinen. Työn ollessa kasvavissa määrin 24/7 tyyppistä tuotannon ja myös

prosessien seurantaa, aina kuluttajalta tuotantolaitokselle saakka, tarve tälle funktiolle palvelutoimittajalla sekä myös liiketoiminnan vastuutahoilla on edelleen ilmeinen.

11 Johtopäätökset

Automatiikka – sen sijaan, että monitoroitaisiin missä syntyy virhe – potentiaalinen virhetilanne tulisi korjata jo ennen kuin se pääsee syntymään. Tämä on perustavanlaatuinen tietojärjestelmien suunnitteluun, rakentamiseen ja eritoten kustannuksiin liittyvä piirre. Automatiikkaa voidaan hyödyntää myös tunnistettujen, alempien järjestelmäkerrosten häiriötilanteiden korjaamiseen tälle on edellytyksenä valvonta, ja monitorointityökalujen ja toiminnanohjausjärjestelmän (tikettijärjestelmä) sekä konfiguraationhallinnan integraatio niin, että hälytysten tuottamisesta korjaukseen saakka tarvittava askellus voidaan kuvata, manuaalisesti tehtävä työ dokumentoida ja sitten automatisoida. Lisäksi on tarkkaan syytä pohtia rakennettavan monitoroinnin käyttäjäkuntaa sekä tarkoitusta. APM monitoroinnit ovat hyödyllisiä liiketoiminnan ja sitä tukevien järjestelmien ja prosessien seurannan välineeksi, toisaalta AIOPS tyyppinen monitorointikehikko, jonka tyyppistä kokonaisuutta esittelin kappaleessa 8, saattaa olla viisaampi valinta infrastruktuuri toimittajan työkaluksi, jossa valvontavälineitä on joka tapauksessa kerroksellisuudesta useita ja jotka spesifioituvat nimenomaan ko. teknologian toimivuuteen.

Standardointi – jotta alalle saadaan eri applikaatiotoimittajien välille syntymään toimivia ekosysteemejä monitoroinnin ja valvonnan ja/tai näiden automatisoinnin välille, tulisi jokaisen komponentin, niin fyysisten laitteiden kuin applikaatioidenkin, kyetä yksiselitteisellä tavalla ilmaisemaan rajapinnan kautta oma statuksensa, jotta sen ulkopuolinen valvontaväline voi monitoroida ja tarvittaessa validoida. Tarvitaan siis uusia ratkaisuja sovellusten ajonaikaiseen (Run-Time) valvontaan ja monitorointiin, automaation, operatiiviseen työskentelytapoihin sekä prosessien yhteistoiminnallisuuteen kaikkien tuotannon toimintaan osallistuvien tahojen kesken.

Käyttäjien toiminnan hajaantuessa useisiin eri päätelaitteisiin tulee monitoroitavien kokonaisuuksien määrä kasvamaan niin suureksi, ettei nykyisillä valvonta, ja monitorointituotteilla informaation määrä ole manuaalisesti seurattavissa keskeisten solmupisteiden (Tietoliikennetoimittajat, konesalitoimittajat, sovellustoimittajat, liiketoiminta) toimesta ilman em. automatiikkaa.

Palvelumallien muutoksen myötä (Pilvi-palvelut) valvonnan ja monitoroinnin automatisoitujen valvontamekanismien tarve kasvaa, näiden kyetessä poimimaan häiriötilanteet loppukäyttäjän

tai liiketoimintaprosessin näkökulmasta. Lisäksi koneoppimisen avulla suoritettavasta operatiivisesta hallintatyöstä povataan menestystarinaa. Nämä kolme näkökulmaa painottuvat perinteisten monitorointi, ja valvontamekanismien joukosta.

Valvomosta Ohjaamoksi ja nykyisestä fyysisestä valvomosta virtuaaliseen tilannehuoneeseen. Tulevaisuudessa on selkeänä trendinä nähtävissä etätyöskentelyn lisääntyminen ja tämä koskee myös valvontaa ja monitorointia tietojärjestelmien parissa tapahtuvan työskentelyn kanssa.

Tilannekuvan moniulotteisuus ja toimintavarmuus. Jotta saavutettaisiin riittävän hyvä tilannekuva laajavaikutteisen häiriön sattuessa, tulee valvonta, ja monitorointi infrastruktuurin olla varsinaisista tuotantoympäristöistä riippumaton sekä sen tulee mahdollistaa rooli, ja toimintokohtaisten näkymien luominen kokonaisnäkymän lisäksi. SCADA, eli Supervisory Control And Data Acquisition ohjelmistot ovat tunnettuja valmistavan teollisuuden parissa alkaen jo 70-luvulta, näistä ohjelmistoista tulisi ottaa mallia myös kuluttajapuolen vastaavaan, kasvavaan palvelutarpeeseen.

Tietojärjestelmien ostokäyttäytyminen. Järjestelmätoimituksia ostaessa toimittajilta, tulisi ostajien painottaa myös tietojärjestelmän ajonaikaisen vaiheen kontrollityökalujen kyvykkyyttä, läpinäkyvyyttä ja yhteensopivuutta eri toimittajien kesken. Kuluttaja, käyttäjä, käyttökokeman reaaliaikainen seuranta tulee painottumaan hyvän käyttäjäkokemuksen varmistamiseksi.

Datan kerääminen analysointi ja liiketoiminnallisen edun saavuttamisen ymmärrys. Kone-oppiminen perustuu pitkälti algoritmien tehokkuuteen ja massiiviseen alati karttuvaan sekä muuttuvaan tausta-aineistoon. Tietoa tuottavien ja hallinnoivien organisaatioiden kiinnittää huomiota siihen, että ”Tieto on valtaa” ja että loppukäyttäjää parhaiten palvelevat järjestelmät toistavat automaattisen tietojenkäsittelyn alkuperäistä tavoitetta: suorittaa laskentaa, toimintoja, analysointia ja tehtäviä ihmistä nopeammin ja nykytekniikan valossa myös ihmisen puolesta ja palvelutarpeita ennakoiden. Palveluissa tapahtuvat muutokset on mahdollista ennakoida kerätyn datan analysoinnin avulla.

12 Jatkotutkittavaa

Loppukäyttäjän kokemus palvelusta on ratkaisevan tärkeää. Miten sitten mitata, valvoa ja monitoroida luotettavasti, turvallisesti sekä eettisesti tuhansiin ja jopa miljooniin päätelaitteisiin hajoavaa palvelukokemusta? Loppukäyttäjän kokemus verkkokaupan toiminnasta voi olla hyvää tai huonoa – riippuen käytettävyyssuunnittelusta, jota verkkokauppaa kehittäessä on harjoitettu. Loppukäyttäjä ei aina välttämättä osaa kuitenkaan eritellä palvelun ulkopuolisia, kokemaan vaikuttavaa kerroksellisuutta, taikka kohdentaa häiriöitä tiettyyn palveluker-

rokseen. Kotona tapahtuva internet palveluntarjoajan häiriö tai selaimen tai käyttöjärjestelmän häiriö saattaa johtaa siihen, että verkkokauppa saa syyt niskoilleen oman vaikutusalueensa ulkopuolisesta häiriöstä. Tällä hetkellä kaupat toimivat verkkojen päätelaitteiden, internetselainten sekä mobiiliapplikaatioiden reunaehtojen ja puutteiden puitteissa. Selain ei välttämättä alkujaankaan ole ollut teknisesti optimaalisin työkalu kaupan tai pankkiliikenteen välineeksi ja suurelta osin kuten nykyisinkin, on olemassa mahdollisuus, että tähän käytettyjen investointien lyhytikäisyys uusiutuu aina uusien teknologioiden kanssa.

Lohkoteknologiaa tulisi myös tutkia ja sen mallia sekä toimivuutta valvonnan ja monitoroinnin rinnalla sekä hyödyksi. Esimerkiksi niin että monitoimittajaympäristöissä kriittisten järjestelmien osalta, jossa sanktiokäsittelyt ovat mittavat, jokainen osakomponentti voisi sisältää itsenäisen tilavahti elementin, jota voisi kutsua rajapinnan kautta. Sopimusten sanktiointipykälät sekä vastuurajauskysymykset huomioiden olisi ehkäpä joissain tilanteissa lisäominaisuutena mielekästä kerätä evidenssiä performanssista ketjuittain; luottosuhteiden ja ketjujen säilyessä eheinä. Tehtäväksi jäisi tällöin mallintaa kuluttajien yleisimmät liiketoiminnalliset ja toistuvat palveluketjut ts. relaatiot ja riippuvuudet.

Monitoroinnin ja valvonnan kehitystä tulisi viedä koneoppimisen avulla automaatiosuoritteiseksi sekä ennakoivaksi. Tämä alue jää tässä lopputyössä lähinnä esittelyn alueelle, vaikkakin useat toimittajat tutkivat aktiivisesti juuri tätä aluetta sekä useita näitä tukevia tuotteita on jo esitelty markkinoilla.

Tällä hetkellä monitorointi, ja valvontadata ovat suurelta osin ”kertakäyttö” informaatiota, jota säilytetään lähinnä liiketoiminnallisista syistä sopimuksellisesti sovittu maksimiaika. Tätä dataa ei juurikaan kerätä talteen myöhempää massa-aineistojen analysointia varten ja/tai koneoppimisen tietokannaksi muuten kuin spesifeissä tilanteissa. Kuitenkin juuri Big datan ja koneoppimisen saralla on uskoakseni myös valvonnan ja monitoroinnin osalta saavutettavissa uusia liiketoiminnallisia mahdollisuuksia tulevaisuudessa.

Lähteet

Painetut

Adams, D. (1979). Linnunradan käsikirja liftareille.

Cooper, A. (2003). about face 2.0: The Essentials of Interaction Design. Indianapolis: Wiley publishing, Inc.

Cooper, A. (2004). The Inmates Are Running The Asylum . Sams Publishing.

Hirsjärvi, S., Remes, P. & Sajavaara, P., 2000. Tutki ja Kirjoita. Tampere: Tammer-Paino Oy.

OGC, CSI. (2010). ITIL, Continual Service Improvement, Third Impression. London: TSO (The Stationery Office), Crown.

OGC, SO. (2010). ITIL Service Operation, Third Impression. London: TSO (The Stationary Office), Crown.

Syrjälä, L., Ahonen, S., Syrjäläinen, E. & Saari, S., 1994. Laadullisen tutkimuksen työtapoja. 1-3 toim. Helsinki: Kirjayhtymä.

VanHaren. *Metrics for IT Service Management*. Zaltbommel: VanHaren Publishing, 2006.

Zuboff, S. (1990). Viisaan koneen aikakausi. Otava.Zuboff, S. (1990). Viisaan koneen aikakausi. Otava

Sähköiset

APM Digest. *APM Digest*. 1. Toukokuu 2018. https://www.apmdigest.com/prioritizing-gartners-apm-model (haettu 1. Toukokuu 2018).

Apple. *Apple SIRI*. 20. Joulukuu 2018. https://www.apple.com/siri/ (haettu 20. Joulukuu 2018).

Kaikkialla ATK - ammattina ATK. Ohjannut YLE Elävä Arkisto. Yle, 1973.

BMC. *AIOps Blog*. 19. Toukokuu 2019. https://www.bmc.com/blogs/what-is-aiops/ (haettu 19. Toukokuu 2019).

CIS. *Center for internet security, CIS*. 20. Joulukuu 2018. https://www.cisecurity.org/ (haettu 20. Joulukuu 2018).

Demos Helsinki. *Viisi teesiä tulevaisuuden työstä Työ 2040 -skenaarioraportin perusteella, Koponen, Johannes*. 3. Maaliskuu 2017. https://www.demoshelsinki.fi/2017/03/08/viisi-teesia-tulevaisuuden-tyosta-tyo-2040-skenaarioraportin-perusteella/ (haettu 3. Maaliskuu 2017).

devopstopologies.com. *devopstopologies.com*. 25. Huhtikuu 2019. https://web.devopstopologies.com/ (haettu 25. Huhtikuu 2019).

Dragich, Larry. *The APM Conceptual Framework*. 15. Maaliskuu 2012. http://www.apmdigest.com/prioritizing-gartners-apm-model (haettu 20. Joulukuu 2019).

Gartner, BPM. *IT Glossary, Business Process Management (BPM).* 6. Toukokuu 2019. https://www.gartner.com/it-glossary/business-process-management-bpm/ (haettu 6. Toukokuu 2019).

Gartner, IAAS. *IT Glossary, Infrastructure as a service (IAAS).* 6. Toukokuu 2019. https://www.gartner.com/it-glossary/infrastructure-as-a-service-iaas (haettu 5. Toukokuu 2019).

Gartner, PAAS. *IT Glossary, Platform as a service (PAAS).* 6. Toukokuu 2019. https://www.gartner.com/it-glossary/platform-as-a-service-paas/ (haettu 19. Toukokuu 2019).

Gartner, SAAS. *IT Glossary, SAAS.* 6. Toukokuu 2019. https://www.gartner.com/it-glossary/software-as-a-service-saas/ (haettu 19. Toukokuu 2019).

Gorton, Ian. *Garnegie Mellon University, Sofware Engineering Institure Blog.* 11. Elokuu 2014. https://insights.sei.cmu.edu/sei_blog/2014/08/principles-of-big-data-systems-you-cant-manage-what-you-dont-monitor.html (haettu 01. 05 2019).

—. *Garnegie Mellon University, Sofware Engineering Institure Blog.* 11. Elokuu 2014. https://insights.sei.cmu.edu/sei_blog/2014/08/principles-of-big-data-systems-you-cant-manage-what-you-dont-monitor.html (haettu 01. 05 2019).

Hoyer, Patrik. *Johdatus tekoälyyn.* 25. Huhtikuu 2019. https://www.cs.helsinki.fi/u/ttonteri/ai/ai-fall11-slides9.pdf (haettu 25. Huhtikuu 2019).

ISO. *International Organization for Standardization, ISO/IEC 90003:2014.* 12 2014. https://www.iso.org/standard/66240.html (haettu 30. Toukokuu 2019).

Isokallio, Jari. ”Systeemityö - lehti.” 1. Maaliskuu 2005. http://www.pcuf.fi/sytyke/lehti/kirj/st20053/ST053-22A.pdf (haettu 30. Toukokuu 2019).

ITIL Central. *In A Nutshell: A Short History of ITIL.* 19. Toukokuu 2019. http://itsm.fwtk.org/History.htm (haettu 19. Toukokuu 2019).

itSMF Finland. ”ITIL® Suomenkielinen sanasto, v1.0, 29.” 29. Heinäkuu 2011. https://www.itsmf.fi/site/assets/files/1931/itil_2011_finnish_glossary_v1_01.pdf (haettu 1. Toukokuu 2019).

JUHTA. ”JHS 171, ICT-palvelujen kehittäminen: kehittämiskohteiden tunnistaminen.” Julkisen Hallinnon tietohallinnon neuvottelukunta. 5. Lokakuu 2012. http://docs.jhs-suositukset.fi/jhs-suositukset/JHS171/JHS171.pdf (haettu 1. Toukokuu 2018).

—. *JHS 179, Kokonaisarkkitehtuurin suunnittelu ja kehittäminen.* 7. Helmikuu 2017. http://www.jhs-suositukset.fi/suomi/jhs179 (haettu 30. Toukokuu 2019).

—. *Julkisen hallinnon tietohallinnon neuvottelukunta, JHS 174.* 07. Joulukuu 2009. http://www.jhs-suositukset.fi/suomi/jhs174 (haettu 28. Joulukuu 2018).

Jyväskylän yliopisto. *JYVÄSKYLÄN YLIOPISTO VÄLIRAPORTTI 1(8) Kokonaisaarkkitehtuurihanke.* 22. Joulukuu 2012. https://docplayer.fi/40120301-

Jyvaskylan-yliopisto-valiraportti-1-8-kokonaisarkkitehtuurihanke.html (haettu 27. Joulukuu 2019).

Kleehaus, Martin, Omer Uludag, ja Florian Matthes. ”Martin Kleehaus ym. CEUR Workshop Proceedings, 2nd Workshop on Continuous Software Engineering, 11.” *Towards a Multi-Layer IT Infrastructure Monitoring Approach based on Enterprise Architecture Information.* Hannover: Technische Universtit at Munchen, Software Engineering for Business Information Systems (sebis), 2017. https://wwwmatthes.in.tum.de/file/jdjv6wts2ubp/Sebis-Public-Website/-/Towards-a-Multi-Layer-IT-Infrastructure-Monitoring-Approach-based-on-Enterprise-Architecture-Information/CSE2017_Kleehaus_Uludag.pdf.

Kotimaisten kielten keskus. *Kielitoimiston sanakirja.* 20. Joulukuu 2018. https://www.kielitoimistonsanakirja.fi/ (haettu 20. Joulukuu 2018).

NASA. *APOLLO Mission Control Center.* 14. Helmikuu 2014. https://www.nasa.gov/content/apollo-mission-control-center-0 (haettu 30. Toukokuu 2019).

Niemi, Eetu. ”Enterprise Architecture Stakeholders - holistic view.” *AMCIS 2007Proceedings, 41.* Jyväskylä: AMCIS, 2007. http://aisel.aisnet.org/umcis2007/41.

Oblong. *Oblong.com.* 20. Joulukuu 2018. https://www.oblong.com/company/our-story (haettu 20. Joulukuu 2018).

OPEL. *Opel OnStar.* 20. Joulukuu 2018. http://www.opel.fi/onstar/onstar.html (haettu 20. Joulukuu 2018).

PCI, The Security Standards Council. *The PCI Data Security Standards.* 30. Toukokuu 2019. https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security (haettu 30. Toukokuu 2019).

Puolustusministeriö. ”Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille.” 26. Maaliskuu 2015. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf (haettu 27. Joulukuu 2018).

Smith, David Woodruff. *Phenomenology, The Stanford Encyclopedia of Philosophy.* Versio 2018, Minor. 2018. https://plato.stanford.edu/archives/sum2018/entries/phenomenology/ (haettu 30. Toukokuu 2019).

Stackify. *Real User Monitoring, RUM.* 19. Toukokuu 2019. https://stackify.com/what-is-real-user-monitoring/ (haettu 19. Toukokuu 2019).

Teittinen, Henri, ja Tommi Auvinen. ”Kontrollin käsite muutoksessa: Käskytyksestä kohti asiantuntijaohjausta.” *Kontrollin käsite muutoksessa: Käskytyksestä kohti asiantuntijaohjausta.* Jyväskylä: EJBO, Electronic Journal of Business Ethics and Organization Studies, 2014. 1-2.

Togaf. *The Open Group.* 6. Toukokuu 2019. https://publications.opengroup.org/standards/togaf/specifications/c182 (haettu 6. Toukokuu 2019).

Traficom, Kyberturvallisuuskeskus. *Pilviturvallisuuden arviointikriteeristö, PiTuKri.* Versio 1.0. 4 2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf (haettu 30. 05 2019).

Underkoffler, John. *3 things working on Minority Report's UI taught me about business.* 7. Elokuu 2017. https://thenextweb.com/contributors/2017/08/06/3-lessons-minority-report/ (haettu 7. Elokuu 2017).

Valtionvarainministeriö. *Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto.* 12. 20 2018. https://www.vahtiohje.fi/web/guest (haettu 12. 20 2018).

—. *Vahtiohje, Jatkuvuudenhallinnan toteuttaminen.* 20. Helmikuu 2016. https://www.vahtiohje.fi/web/guest/8-jatkuvuudenhallinnan-toteuttaminen.

VanHaren. *Metrics for IT Service Management.* Zaltbommel: VanHaren Publishing, 2006.

Julkaisemattomat

Kohdeyritys, 2017
Liite 1, Haastattelu 1, Storage alueen asiantuntija, Kohdeyritys, 24.2.2017
Liite 2, Haastattelu 2, Monitorointi, ja valvonta-alueen arkkitehti, Kohdeyritys, 30.3.2017
Liite 3, Haastattelu 3, Tietoturva-alueen asiantuntija, tietoturvapäällikkö, Kohdeyritys, 19.4.2017
Liite 4, Keskeinen käsitteistö

Kuviot

Kuvio 1: Kokonaisarkkitehtuuri esimerkki, Palveluiden kerroksellisuus..... 23

Kuvio 2: Kokonaisarkkitehtuuri esimerkki, palvelun osto, ja ulkoistusmalleista; PRAAS, SIAM, SAAS, IAAS..... 35

Kuvio 3: Tietojärjestelmän monitorointi ja valvonta sekä eri käyttäjäryhmille suunnatut valvontavastuiden mukaiset näkymät kerätystä monitorointidatasta. 38

Kuvio 4: Tietohierarkia ja rakenne esimerkki asiakkaan ja tietojärjestelmän rakenneosien mukaisesti koostettuna tilannekuvaksi (Dashboard) operoivan henkilöstön käyttöön 39

Taulukot

Taulukko 1: Application Performance Management kehikko (Dragich 2012), käännös kirjoittajan..... 16

Taulukko 2: Monitorointi ITIL viitekehyksen mukaisesti 18

Taulukko 3: Esimerkki laitteistotiedosta konesali, ja käyttöpalvelun toimittajan laitteistonhallinnasta 20

Taulukko 4: Palveluarkkitehtuurikerrosten ”personat”, joille on eri monitorointi, ja valvontatyökalut käytössään..... 37

Liitteet

Liite 1: Haastattelu 1, Storage alueen asiantuntija, Kohdeyritys, 24.2.2017 57
Liite 2: Haastattelu 2, Monitorointi, ja valvonta-alueen arkkitehti, Kohdeyritys, 30.3.2017 .. 58
Liite 3: Haastattelu 3, Tietoturva-alueen asiantuntija, tietoturvapäällikkö, Kohdeyritys, 19.4.2017..... 60
Liite 4: Keskeiset käsitteet 62

Liite 1: Haastattelu 1, Storage alueen asiantuntija, Kohdeyritys, 24.2.2017

Storage järjestelmän virheen / häiriönselvitys on haastavaa, sillä ympäristössä joudutaan virhetilanteissa ”kokeilemalla” ajamaan eri komentoja ja vertailemaan näillä saatuja tuloksia. Samalla komennolla saadut tulokset voivat erota toisistaan, ajohetken mukaan, joten ilman saman toimittajan erillistä valvontaa suunnittelemaa lisäohjelmistoa häiriöselvitys on haastavaa. Tuotannossa tapahtuvaa häiriöselvitystä tehdään yleensä suuren paineen alla, häiriön pahimmillaan estäessä monien asiakkaiden tietojärjestelmien toiminnan.

Tilanteessa ei häiriönselvittäjällä yleensä ole nähtävissä kaikkia ympäristössä tehtyjä muutoksia. Asiakkaan tietojärjestelmän häiriötilanteessa toimittaja(t) eivät voi voi sulkea ulos mitään potentiaalista häiriön syytä ja häiriönkohdennus käynnistyykin usein monilla eri tasoilla yhtäaikaisesti niin sovellustoimittajalla, asiakkaan lähiverkon ja työasemapalveluiden kanssa kuin konesali, ja kapasiteettipalveluiden toimittajalla. Häiriönselvitys virhetilanteessa Storage alueella, varsinainen juurisyy saattaa myös johtua sovelluksen tai muiden kerrosten häiriötoiminnasta. Keskustelussa ilmeni toive paremmasta työkalusta valvonnan ja monitoroinnin tarpeisiin niin Storage puolella kuin kokonaisvaltaisestikin.

Haastateltavalla heräsi ajatus keskustelun yhteydessä kerroksellisen kokonaisvalvonnan rakentamisesta tukemaan tietojärjestelmäarkkitehtuuri lähestymistä. Haasteena tarjolla olevissa holistisissa valvontajärjestelmissä on se, että ne eivät tarjoa riittävän yksityiskohtaista tietoa asiantuntijoiden käyttöön ja vastaavasti yksittäisen teknologiatoimittajan työkalujen valvonta ja analysointityö-kalut keskittyvät monitoroimaan, valvomaan ja analysoimaan juuri kyseisen teknologian toimintaa – ei varsinaisesti asiakkaan tai asiakkaiden tietojärjestelmäkokonaisuuden. Sama havainto koskettaa lähes kaikkia tietojärjestelmiä, jotka hyödyntävät useita eri teknologioita.

Tällöin tulisi valvonta rakentaa tukemaan ainakin kahta ulottuvuutta: asiakkaan tietojärjestelmää sekä tämän käyttämän teknologiapaletin kerroksellisesta valvonnasta. Lisäksi kaikkien kerrosten valvonnan tulisi lähettää valvonta, analytiikka ja monitorointitietoja yhtenäiseen tietokantaan, jota analysoitaisiin Big Datan ja/tai keinoälyn keinoin. Yksinkertaisimmillaan valvontahälytysten seuranta ja vertailu kahdella edellä mainitulla muuttujalla; esim. teknologia, ja asiakas/tietojärjestelmä pisteiden yhtäaikainen hälytys auttaisi asiantuntijoita kohdentamaan häiriön nopeammin.

Liite 2: Haastattelu 2, Monitorointi, ja valvonta-alueen arkkitehti, Kohdeyritys, 30.3.2017

Keskustelu monitorointi, ja valvonta-alueen asiantuntijan kanssa 30.3.2017 alueen nykyhaasteista ja tulevaisuuden näkymistä. Nykyisin usealla palvelutoimittajalla nojataan Gartnerin APM, application performance monitoring kehykseen. Mallia on sovitettu ja hyödynnetty pitkään myös Tiedon monitorointi, ja valvontaratkaisuissa.

Liiketoimintajärjestelmä keskeisyys painottuu kasvavissa määrin nykyvalvonnoissa järjestelmän osakomponenttien valvontoja enemmän. Tavoitteena valvonta, ja monitorointiratkaisuissa on kokonaisvaltainen valvonta sisältäen ”koko stackin” seuranta ja näistä eri työrooleja tukevien ”dashboardien” eli valvontanäkymien tuottaminen. Näitä työskentelyrooleja ja funktioita (ITIL) on mm. tekninen tukifunktio, Service desk, Control Desk ja asiakkaat itse.

Tulevaisuudessa BPM – business process management ratkaisut tulevat yhä keskeisempään osaan. Näissä monitorointiratkaisuissa keskitytään järjestelmän sisällä ja/tai järjestelmien välillä tapahtuvan liiketoimintaprosessin tuotoksen (huom. tuotannon, vrt. valmistava teollisuus) seurantaan.

Toinen mielenkiintoinen tulevaisuuden näkymä on mittaussensorien määrän lisääntyminen. Teknologian halpenemisen myötä on mittarien hinta varsin alhainen ja näiden sovelluskohteiden määrä kasvaa mm. terveydenhoidon alueella sekä rakennusten valvonnassa. Mittarien määrän lisääntyessä myös valvottavien kohteiden määrä kasvaa. Monitoroinnin ja valvonnan määrä puolestaan on suorassa suhteessa palvelutarpeiden kasvuun.

Kolmantena näkökulmana valvontaan mainittiin Internet of Things, IOT, trendi. Tässä muutoksessa on kyse traditionaalisten kodinkoneiden ja laitteiden siirtymisestä verkkoon. Muutoksessa on vastaavasti kyse palvelukysynnän ja tarjonnan muutoksesta. Jos ajatellaan vaikkapa nykyistä kaupan alan kuluttajaseurantaa, joka perustuu pitkälti kuittien ja bonusjärjestelmien kautta kerättävään tietoon, jolla ennustetaan eri tuotteiden menekkiä ja näin pystytään paremmin arvioimaan sisäänostoa ja varastointia. Mikäli kodinkoneet, vaikkapa jääkaappi itse ilmoittaa tarpeen, milloin maito alkaa olla lopussa – tulee tämä tieto järjestelmien avulla vaikkapa suoraan meijerille, logistiikalle, kauppiaalle, joka avaa taas aivan erityyppisiä kulutuksen ennustamisia ja tuotannon optimointimahdollisuuksia.

Periaatteessa kaikkea missä on sensori, voidaan mitata ja mitattavien kohteiden määrän kasvaessa lisääntyy tieto, jonka pohjalta voidaan tehdä tarkempaa päätöksentekoa alueella kuin alueella.

Lopuksi palasimme vielä keskustelemaan nykyisistä valvontatyökaluista, jotka aiemmin ovat rajoittuneet yhden teknologian tai toimittajan tuoteperheen seurantaan. Useissa eri työkaluissa on panostettu omaan valvontakyvykkyyden rakentamiseen ja tukemiseen usealle eri

teknologialle. Tämän lisäksi on valvontaohjelmistojen toimittajat rakentaneet tuotteisiinsa rajapintoja, jotka mahdollistavat valvontatiedon kyselyn tai vastaanottamisen yhteen kokonaisvalvontatietokantaan. Tietoa voidaan siis joko hakea valvontapalvelimen suunnasta tapahtuvalla skriptillä haluttuun kohteeseen tai seurattavasta kohteesta voidaan lähettää tieto keskitettyyn valvontapalvelimeen.

Keskustelussa tuotiin esille myös ajatus valvonnasta ja monitoroinnista tietojärjestelmäarkkitehtuurin näkökulmasta ja tätä pidettiin tavoiteltavana ja hyvinkin todennäköisenä ja isolta osin jo toteutuvana kehityskaarena. Käsite ”End-to-End”, lyh.”e2e” on tosin sinänsä haastava, sillä jokainen tietojärjestelmän osakas (Stakeholder) piirtää e2e alku, ja päätepisteen eri näkökulmasta. Esim. käyttöpalvelutoimittajan näkökulma kattaa palvelimien ja reitittimien lisäksi konesalinäkökulman, joka ei applikaatiosuunnittelijalle ole mukana e2e näkökulmassa – jälkimmäisten pitäytyessä n-tier applikaatioarkkitehtuurin loogisessa näkökulmassa. Lisäksi ns. Full stack valvonnan tietoturva-näkökulma tuotiin keskustelussa esille; valvonta, ja monitorointidatan ollessa väärissä käsissä myös ideaali informaatiokanava mahdolliselle hakkerille seurantatyökaluna sekä potentiaalisten haavoittuvuuksien kartoittamiselle tietojärjestelmäarkkitehtuurissa.

Haastattelun jälkeistä yhteistä pohdiskelua ja keskustelua.

Tästä em. syystä totesimme, että mikäli valmistetaan yksittäinen kanta jonkin toimittajan taholle, jonne yksittäisen tietojärjestelmän relaatioiden kautta rakennetaan kaikkia toimittajia palveleva, eri näkökulmia tukeva ja rooli/sidosryhmänäkymiä tuottava valvonta, ja monitorointikanta, on sen rajanveto vaikeaa ja ylläpitotyö haasteellista, varsinkin jos kyselyt on toteutettu erillisillä skripteillä, joita täytyy jatkuvasti muokata mikäli kohde (järjestelmä tai komponentti tai prosessi) päivittyy.

Liite 3: Haastattelu 3, Tietoturva-alueen asiantuntija, tietoturvapäällikkö, Kohdeyritys, 19.4.2017

Haastattelu suoritettiin työpaikalla, työtehtävien yhteydessä erillisenä haastatteluna sekä useina erillisinä jatkokeskusteluina, joista keskeiset havainnot on kirjattu referoituna haastattelun tulokseen.

Keskustelimme tietoturvan monitoroinnista sekä siihen liittyvästä Tiedon palvelusta ”Security Wall”. Kysymyksenä oli haastattelijalla edelleen tietojen tunnistaminen, joita tietoturvan tilannekuvaan tulisi saattaa ja miten sekä missä ko. monitorointia tulisi seurata sekä turvallisuuden tilannekuvan muodostaminen yleisesti nyt ja tulevaisuudessa.

Tietoturvan monitorointia voidaan hyvin suorittaa kontrollihuone tyyppisestä tilasta käsin, mutta on huomioitava, että tietoturvan näkökulmasta osa tunnistetuista seurattavista tietovirroista ja tiedoista voivat olla turvaluokittelun vuoksi sellaisia, joiden käyttöä tai näkymää rajoitetaan palvelutuottajalla vain tunnistetuille, esiehdot täyttäville asiantuntijoille.

Periaatteena tietoturvan huomioimiselle kokonaisvaltaisesti keskiössä on organisaation tietoturvakulttuuri, joka muodostuu useasta eri vaatimuslähteestä kattaen esimerkiksi tilatietoturvan, henkilöturvallisuuteen sekä datan käsittelyyn liittyvistä toimialakohtaisista vaatimuksista.

Esimerkkinä näistä säädöksistä ja toimintaohjeista toimivat tässä yhteydessä Katakri auditointityökalu (Puolustusministeriö 2015) ja Vahti ohjeistukset (Valtionvarainministeriö 2018), jotka ohjeistavat ja määrittelevät esim. julkishallinnon asiakkuuksien, tietojärjestelmien sekä datasisältöjen tietoturvakäytäntöjä sekä sisältävät mm. tietojen luokitteluun liittyvän ohjeistuksen sekä velvoitteen. Toimialakohtaisesti on olemassa myös muita palvelutuottajan toimintaa ohjaavia, vastaavia kehikoita ja standardeja, kuten esim. PCI, Payment Card Industry security standards (PCI, The Security Standards Council 2019) tai ISO standardit. (ISO 2014)

Tietovirtojen ohjaaminen tilannekuvaksi palveluntoimittajan tai asiakkaan seurantaan edellyttää alakohtaisten ja sopimusvaatimusten mukaista tietojenkäsittelyä.

Tyypillisesti seurattavia asioita tietoturvamielessä ovat esim. tietoliikenne, sisään, ja uloskirjautumisten määrä, työasemien / palvelinten määrä sekä jatkuvuuden varmistamiseksi rakennettavat toiminteet, kuten varmistukset, seurantaraportit sekä spesifit jäljitettävyyden valvontakohteet tietojärjestelmissä.

Keskustelimme fyysisen monitorointi ja valvontatilan vs. virtuaalisen monitorointitilan tarpeesta ja todettiin, ettei tietoturva itsessään rajoita valvonta, ja monitorointi tai tilannekuvatyökalujen käyttöä, vaan datan luokittelu, johon yleisesti asetetaan erityyppisiä käsittelyvaateita. Päätelaitekirjo ja etätyöskentely asettavat osaltaan haasteita sekä mahdollistavat

eri tyyppisten virtuaalisten tilannehuoneiden käyttöä. Haasteina voidaan pitää tietoturvan potentiaalisten rikekohtien määrän kasvua, jota tulee hallita riskienhallinnan näkökulmasta kohdekohtaisesti asetelmalla: saavutettava hyöty vastaan toiminnan riskit.

Liite 4: Keskeiset käsitteet

Lyhenne	Englanninkielinen selite	Suomenkielinen selite
	Application component monitoring	Sovelluskomponentin monitorointi
	Real-time Application monitoring, active	Aktiivinen monitorointi, käyttökokemuksen mittaaminen robotteja ja skriptejä, agentteja, käyttäen.
	Real-time Application monitoring, passive	Passiivinen monitorointi on yleensä agentitonta mittausta, joka suoritetaan tietoliikenne portin liikennettä monistamalla ja monistettua dataa analysoiden.
	Reporting & Application data analytics	yleinen mittaristo, joka kerää applikaatioiden suorituskyky dataa ja esittää ne sovitussa formaatissa raportteina tai dashboardista.
ADDM	Application Discovery and Dependency Mapping	Infrastruktuurissa toimivien applikaatioiden ja niiden riippuvuuksien automaattinen keruu ja hallinta
AiOPS	AIOps refers to multi-layered technology platforms that automate and enhance IT operations by 1) using analytics and machine learning to analyze big data collected from various IT operations tools and devices, in order to 2) automatically spot and react to issues in real time. (BMC 2019)	AiOPS viittaa kerroksellisiin teknologia , jotka automatisoivat ja parantavat IT operaatioita 1) käyttämällä analyysiä ja koneoppimista analysoimaan Big data aineistoa jota on kerätty useista IT hallinta työkaluista ja koneista tavoitteenaan 2) automaattisesti havaita ja korjata ongelmatilanteet reaaliaikaisesti
APM	Application Performance Management	Sovelluksen suorituskyvyn hallinta

Baseline		Viitearvo, Lähtötilanne, vertailukohta, johon kerättävää dataa, esim. suorituskykydataa verrataan.
BCM	Business Continuity Management	Liiketoiminnan jatkuvuuden hallinta
BPM	Business Process Monitoring	Liiketoimintaprosessien monitorointi
BTM	Business transaction management	Työkalu transaktioiden seurantaan ja hallintaan sekä applikaatio topologian hallintaan it-infrastruktuurissa.
CI	Configuration Item	Konfiguraation osa, (komponentti, järjestelmä, palvelin, työasema jne.)
CMDB	Configuration Management Database	Konfiguraatiotietokanta
CMS	Configuration Management system	Konfiguraationhallintajärjestelmä
CSI	Continual Service Improvement	Jatkuva palvelun parantaminen
Dashboard	Dashboard	Valvontanäyttö, kojetaulu
DDCM	Deep Dive Component Monitoring	keskittyy yleensä monitorointinäkymän luomiseen välikerroksen ohjelmistojen esim. j2ee ja .net sekä käyttäjän käyttöliittymästä käynnistämiin liiketoiminta transaktioihin edellisiin liittyen.
EUE	End user experience monitoring – (active and passive)	Käyttökokemuksen monitorointi, aktiivinen ja passiivinen
RACI	Responsible, Accountable, Consulted and Informed	Menetelmä, jota käytetään helpottamaan vastuiden ja roolien määrittelyä.

		(Englanninkieliset) kirjaimet tulevat sanoista vastuullinen, tulosvastuullinen, konsultoitava ja tiedotettava.
RUM	Real User Monitoring	TCP/IP ylitse lähetettyjen pyyntöjen kuuntelu ja analysointi
Run time	Run time	Ajon-aikainen
SLA	Service Level Agreement	Palvelutasosopimus
UEM, UX	User Experience Management	Käyttökokemuksen hallinta
	Control panel	Valvontanäyttö, kojetaulu. Graafinen esitys IT-palvelun yleisestä suorituskyvystä ja saatavuudesta. Valvontanäytön näkymät voidaan päivittää reaaliajassa, ja ne voidaan myös sisällyttää johdon raportteihin ja websivuille. Valvontanäyttöjä voidaan käyttää palvelutasonhallinnan, herätteidenhallinnan ja häiriödiagnosoinnin apuna.

(ITIL CSI 2010), (itSMF Finland 2011)