Haaga-Helia
ammattikorkeakoulu Oy

Tietoturvapolitiikkapoikkeamien käsittelyprosessi ja menetelmät

Fingrid Oyj

Matti Tuovinen

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2018

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Matti Tuovinen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Raportin/Opinnäytetyön nimi
Tietoturvapolitiikkapoikkeamien käsittelyprosessi ja menetelmät

Sivu- ja liitesivumäärä
44 + 4

Opinnäytetyön toimeksiantajana toimii Suomen kantaverkkoyhtiö Fingrid Oyj. Yritys vastaa Suomen maanlaajuisen sähkön kantaverkon ylläpitämisestä sekä kehittämisestä.

Tässä opinnäytetyössä tutkitaan Fingrid Oyj:n tietoturvapoikkeamanhallinnan ja siihen liittyvien prosessien nykytilaa. Lisäksi pohditaan, kuinka prosesseja voitaisiin kehittää nykyistä tehokkaammiksi ja siten vastaamaan ennalta asetettuja tavoitetasoja. Lopuksi tutkimus esittää poikkeamanhallinnan nykytilan tason kriittisen arvioinnin tukemiseksi vertailun kahteen kotimaiseen huoltovarmuuskriittiseen energia-alan yritykseen. Tästä syntyvä kehityssuunnitelma ei ota kantaa muutosten toteuttamiseen käytännön tasolla.

Tutkimus toteutettiin empiirisenä ja laadullisena tapaustutkimuksena, jossa materiaalia hankittiin teemahaastatteluiden, kirjallisuuskatsauksen sekä dokumenttien avulla. Tätä tutkimusta varten haastateltiin Fingrid Oyj:stä tietoturvayksikkö kokonaisuudessaan ja ulkoisista vertailuyrityksistä tietoturvapäälliköt. Haastattelut nauhoitettiin ja litteroitiin perusmuotoisina ennen niiden laajaa analysointia aineistolähtöisenä sisällönanalyysina.

Nykytilan kartoituksessa paljastui useita kehityskohteita aina keskeisistä politiikoista ja dokumenteista henkilöstön kouluttamiseen sekä poikkeamanhallinnan tehostamiseen. Vertailu vahvisti Fingrid Oyj:n havaittuja puutteita, mutta toisaalta sen vahvuuksia ovat johtoryhmän jatkuva sitoutuminen poikkeamanhallintaan, henkilöstön ammattitaito ja koulutustaso sekä viestintään ja säännölliseen perehdyttämiseen panostaminen. Saadut tulokset kertovat Fingrid Oyj:n nykytilan olevan vertailukelpoinen astetta suurempiin yrityksiin, kunhan nykytilan kartoituksessa esitetyn kehittämissuunnitelman mukaiset muutokset saadaan huomioitua poikkeamanhallinnan toiminnan jatkokehittämisessä.

Asiasanat
Poikkeamanhallinta, tietoturva, tietoturvapolitiikka, tietoturvastandardi

Alkusanat

Tämä opinnäytetyö toteutettiin Fingrid Oyj:n tietoturvayksikön toimeksiantona. Haluan osoittaa erityiskiitokset työni ohjaajalle, tietoturvapäällikkö Jyrki Pennaselle rakentavasta palautteesta, joustavuudesta sekä haastavasta tutkimusaiheesta. Haluan kiittää myös työni valvojaa Tero Tuoriniemeä tuesta ja kannustuksesta sekä toisena tarkastajana toiminutta Teemu Ruohosta Haaga-Helia ammattikorkeakoulusta. Suuri kiitos Marko Haikaraiselle saamastani mahdollisuudesta suorittaa opintoihini liittynyt työharjoittelu Fingrid Oyj:lle – ilman sitä toimeksianto ei olisi toteutunut. Lopuksi kiitos haastatteluihin osallistuneille.

Helsingissä 15.3.2018

Matti Tuovinen

Sisällys

Kuviot

Lyhenteet

ENISA	Euroopan unionin verkko- ja tietoturvavirasto (European Union Agency for Network and Information Security)
HAVARO	Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä
IEC	Kansainvälinen sähköalan standardointiorganisaatio (International Electrotechnical Commission)
ISACA	Tietojärjestelmien tarkastus ja valvonta (Information Systems Audit and Control Association)
ISF	Information Security Forum
ISO	Kansainvälinen standardisoimisjärjestö (International Organization for Standardization)
ITIL	Kokoelma käytäntöjä it-palveluiden hallintaan ja johtamiseen (Information Technology Infrastructure Library)
NIST	Yhdysvaltalainen standardielin (National Institute of Standards and Technology)
SIEM	Tietoturvatiedon ja -tapahtumien hallinta (Security Information and Event Management)
SOC	Tietoturvan hallintakeskus (Security Operations Center)

1 Johdanto

Globalisoituvasta liiketoiminnasta periytyvä paine hallita lisääntyviä menoja ja kohdentaa resursseja aktiivisemmin johtavat yritysmaailman tietoteknisten ratkaisujen jokapäiväisen käytön laajentumiseen. Yritykseen kohdistuva rikollinen kiinnostus kohoaa painopisteen siirtyessä salassa pidettävän tiedon rooliin, lisäten siten kohdennetun hyökkäyksen riskiä. Henkilöstö voi muodostaa potentiaalisen tietoturvariskin, jossa tietovarastojen eheyttä ja luotettavuutta ei kyetä enää varmistamaan. Harmittomilla tietoturvapoikkeamilla voidaan aiheuttaa yrityksen toiminnalle ja imagolle korvaamatonta vahinkoa. Tietoturvallisuuden hallitsemiseksi yrityksiltä edellytetään tänä päivänä yhä järjestelmällisempiä toimenpiteitä, pakottaen yritykset siten pohtimaan kattavina pidettyjen käsittelyprosessiensa riittävyyttä ja lisäämään resursseja varhaiseen havainnointiin, torjumiseen sekä niistä palautumiseen.

Tässä tutkimuksessa kartoitetaan Fingrid Oyj:n tietoturvapoikkeamanhallinnan nykytilaa ja pohditaan, kuinka siihen liittyviä käsittelyprosesseja voidaan kehittää tehokkaammiksi. Kotimainen, yritysmaailmaa hyödyttävä tutkimustieto poikkeamien käsittelyprosesseista on olematonta, ja käytännönläheisten johtopäätösten vetäminen tuloksista siksi hankalaa. Tutkimustarve yhdistettynä toimeksiantajan havaitsemiin puutteisiin prosessitasolla, sekä haluni selvittää kuinka toimintamalleja noudatetaan, luovat pohjan tälle opinnäytetyölle.

1.1 Tutkimuksen tavoitteet ja rajaukset

Tämän opinnäytetyön toimeksiantaja, vuonna 1996 perustettu kantaverkkoyhtiö Fingrid Oyj (jäljempänä Fingrid), vastaa maanlaajuisesta sähköverkosta, jonka ylläpitäminen sekä kehittäminen – ja siten myös sähkömarkkinoiden toimivuuden edistäminen – lukeutuvat sen ydintehtäviin. Fingridin toimintaa ohjaa sähkömarkkinalaki, joka asettaa päivittäiselle toiminnalle tiukat vaatimukset. Suomen valtion enemmistöomisteisena yhtiönä Fingridin asiakaskunta muodostuu pääasiassa sähköntuottajista, sähkömarkkinatoimijoista, alue- ja jakeluverkonhaltijoista sekä suurteollisuusyrityksistä. Kuluneiden vuosien aikana Fingrid on investoinut ja parantanut liiketoimintaansa selkeästi, konsernin liikevaihdon kasvaessa vuoden 2015 tammi-joulukuussa 600 miljoonaan euroon sekä liikevoiton 100 miljoonaan euroon. Fingrid omistaa noin 110 sähköasemaa ja työllistää noin 315 henkilöä, jakautuen Helsingin pääkonttorin lisäksi viidelle eri toimipaikalle. (Fingrid 2015a; Fingrid 2015b.)

Kantaverkon toiminnan tulee olla turvattu vaikeimmissakin poikkeustilanteissa, johtaen merkittäviin tietoturvavaatimuksiin. Fingrid on hiljattain saanut päätökseen johtotasolla hyväksytyn, strategisia linjauksia ja ICT-strategiaa noudattavan tietoturvapolitiikan, jossa määritellään erikseen tietoturvalle asetetut päämäärät, tavoitteet ja vastuut, sekä erityisesti niiden toteuttamiseen liittyvät vaihtoehdot. Säännöllisesti päivitetyn tietoturvapolitiikan sisältö on julkista tietoa, ja vapaasti yrityksen henkilöstön saatavilla sisäisessä intranetissä.

Fingrid toivoo parantavansa tietoturvapoikkeamanhallintansa nykytilaa luotettavampaan ja selkeämpään suuntaan, sekä saavansa tutkimuksen päätteeksi kehittämissuunnitelman, joka voitaisiin käyttöönottaa vähäisin muutoksin. Suurimpia ongelmia ovat poikkeamien puutteelliset ja epäformaalit toimenpiteet niiden määrittelyyn, luokitteluun ja vakavuuden arviointiin, todistusaineiston keräämiseen ja raportointiin liittyen; kuin myös epätarkoiksi todetut kirjaamismenetelmät, jotka päätyessään eri sähköposteihin mahdollistavat turhan pohjan tietoturvariskien syntymiselle ja liiketoiminnan vaarantumiselle (EY 2014, 22, 45).

Tämän tutkimuksen ensisijaisena tutkimustavoitteena on pohtia Fingridin tämänhetkisiin tietoturvapoikkeamanhallinnan käsittelyprosesseihin liittyviä toimintatapoja, sekä kuinka nykytilanteesta on mahdollista muodostaa yhtenäinen kokonaisuus ennalta määritettyjen tavoitetasojen saavuttamiseksi. Tutkimus selvittää edelleen, kuinka poikkeamanhallinnan nykytilanne kestää vertailussa kahteen kotimaiseen huoltovarmuuskriittiseen energia-alan organisaatioon. Tutkimus toteutetaan sisäisen ja ulkoisen dokumentaation, kirjallisuuden sekä asiantuntija- ja päällikkötason haastatteluiden pohjalta, tuottaen myös suunnitelman prosessien kehittämiseksi – se ei ota kantaa muutosten toteuttamiseen käytännön tasolla.

Tutkimuksessa vastataan seuraaviin kysymyksiin:

Pääkysymys: Mikä on tietoturvapoikkeamanhallinnan prosessien nykytila?

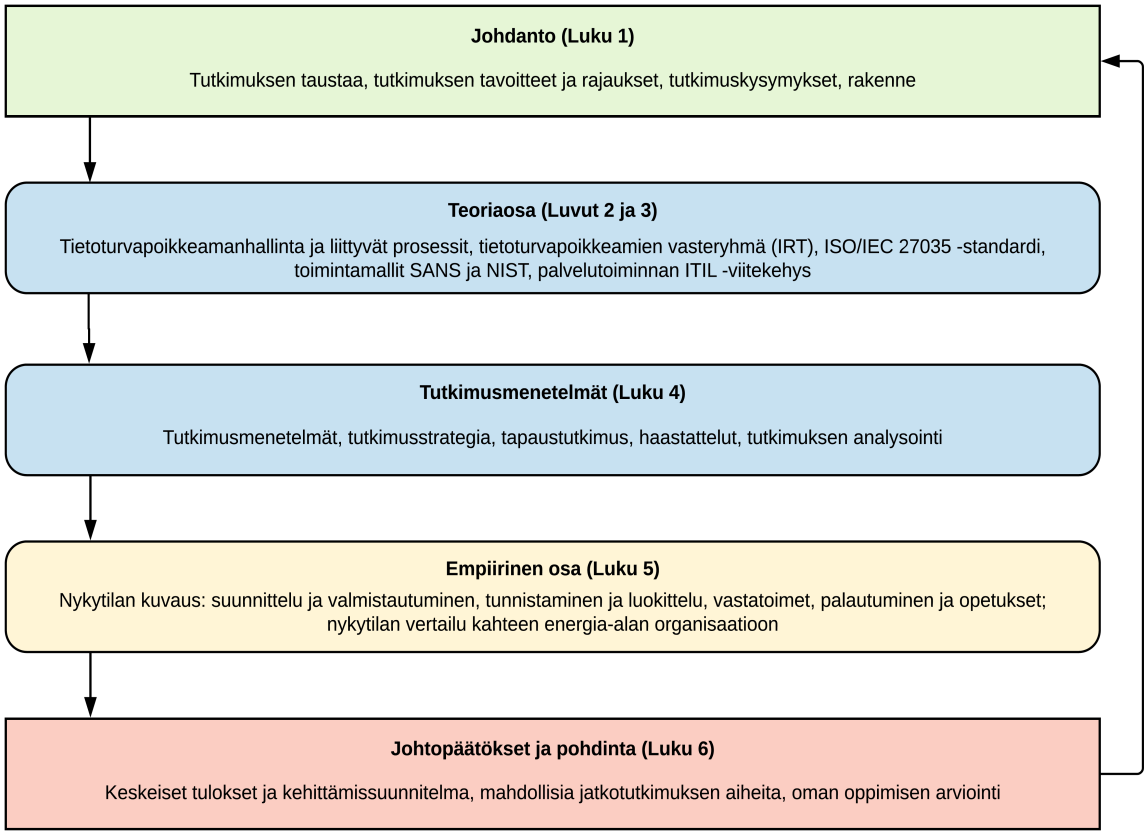
1. alakysymys: Kuinka käsittelyprosesseja voidaan tehostaa, jotta saavutetaan läpinäkyvän toiminnan kannalta mahdollisimman luotettava ja turvallinen, laaja-alainen tietoturvapoikkeamanhallinnan taso?

2. alakysymys: Kuinka käsittelyprosessien nykytila kestää vertailussa kahteen toiseen huoltovarmuuskriittiseen energia-alan organisaatioon?

1.2 Tutkimuksen rakenne ja eteneminen

Tutkimuksen teoreettinen osio esitetään kirjallisuuskatsauksena toisessa ja kolmannessa luvussa – siinä tutustutaan tietoturvastandardien ja toimintamallien yhteisiin suosituksiin tietoturvapoikkeamanhallinnan teoriaa ja määritelmiä käsiteltäessä. Tutkimusmenetelmät kuvataan neljännessä luvussa. Viides luku esittelee empiirisen osion eli tutkimustulokset, joka kartoittaa kokonaiskuvan Fingridin poikkeamanhallinnan nykytilasta peilaamalla eri lähteistä kerättyä materiaalia asetettuihin tutkimuskysymyksiin ja kirjallisuuskatsaukseen, sekä lopuksi esittää tulokset vertailusta kahteen kotimaiseen energia-alan organisaatioon.

Johtopäätöksissä pohditaan käsiteltyjä tutkimustuloksia ja esitetään kehittämisehdotuksia poikkeamanhallinnan prosessien tehostamiseen. Lisäksi luvussa pohditaan potentiaalisia jatkotutkimuksen aihealueita, joita voitaisiin toteuttaa parempien resurssien ja aikataulun puitteissa. Tutkimus päättyy lopuksi oman oppimisen arviointiin – kuinka tutkimuksessa onnistuttiin kokonaisuutena, olisiko joitain kohtia voitu käsitellä paremmin, sekä kuinka ammatillinen osaaminen kehittyi. Kuvio 1 esittelee tutkimuksen rakenteen ja etenemisen.



Kuvio 1. Opinnäytetyön rakenne ja tutkimusprosessin vaiheittainen eteneminen

2 Tietoturvapoikkeamanhallinnan perusteet

Tämän teorialuvun tarkoituksena on pureutua lyhyesti poikkeamanhallinnan perusteisiin sekä niihin olennaisesti liittyviin käsitteisiin alla mainittujen suositusten mukaisesti, ennen varsinaista siirtymistä standardien ja toimintamallien syvällisempään esittelyyn luvussa 3.

2.1 Johdanto standardeihin ja toimintamalleihin

Tietoturvapoikkeamanhallinnan suunnittelun ja käytännön tueksi on tarjolla varsin laajat kokoelmat kansainvälisesti tunnettuja standardeja ja toimintamalleja, joiden ensisijaisena päämääränä on yrityksen liiketoiminnan huojentaminen yhteisten toimintamallien avulla, sekä siten tuotteiden ja palveluiden turvallisuuden ja yhteensopivuuden kasvattaminen – näin toimimalla pyritään varmistamaan niin kotimaisen kuin kansainvälisen kaupanteon sujuvuus. (Laaksonen, Nevasalo & Tomula 2006, 83-86, 88.) Mikäli yrityksessä harkitaan toimintamallien ja standardien käyttöönottamista, on hyvä huomioida niiden olevan vain yleisellä tasolla määriteltyjä ja suuntaa antavia suosituksia, eivätkä ne siten itsessään tarjoa takeita riittävästä tietoturvallisuuden tasosta. Siksi niitä sovelletaan yrityksen kulloisenkin tilanteen ja asetettujen tavoitetasojen mukaisesti. (Hakala, Vainio & Vuorinen 2006, 46.)

Näistä poikkeamanhallintaa käsittelevistä standardeista keskeisimpiin tekijöihin kuuluvat International Organization for Standardization (ISO) ja International Electrotechnical Commissionin (IEC) tuottama ISO/IEC 27000 -standardi, joka käsittelee yleisellä tasolla ISO/IEC 27000 -standardiperhettä ja siihen läheisesti liittyvää sanastoa, asettaen samalla edellytykset hallintajärjestelmän luonnille (SFS 2014, v); sekä ISO/IEC 27035 -standardi, jossa poikkeamanhallinnan tarkastelun näkökulma keskittyy enimmäkseen suuryrityksiin ja keskisuuriin yrityksiin, soveltuen muokattuna pienemmillekin yrityksille (SFS 2011, 1).

Poikkeamanhallinnan eri prosesseja ja tietoturvallisuutta käsitteleviä toimintamalleja ovat erityisesti National Institute of Standards and Technologyn (NIST) Computer Security Incident Handling Guide, SANS Instituten Incident Handler's Handbook, Information Systems Audit and Control Associationin (ISACA) Incident Management and Response, European Network and Information Security Agencyn (ENISA) Good Practice Guide for Incident Management, sekä Information Technology Infrastructure Library (ITIL).

2.2 Tietoturvatapahtuma ja tietoturvapoikkeama

Ennen tietoturvapoikkeamanhallinnan määrittelyä käsitteenä, on tietoturvapoikkeaman ja tietoturvatapahtuman välinen eroavaisuus ymmärrettävä tarkasti – niiden kun monesti luullaan virheellisesti tarkoittavan samaa asiaa. Tämä muodostuu erityisen tärkeäksi, kun esimerkiksi lokitietojen pohjalta on pohdittava käynnissä olevan tilanteen vaikutusasteen laajuutta – voidaanko tilanne ratkaista lähituessa, vai edellyttääkö se eskalointia ylemmäs.

Tietoturvatapahtuman voidaan ISO/IEC 27000 -standardin mukaan katsoa tarkoittavan yrityksen järjestelmän, palvelun tai verkon tunnistettua tietoturvallisuuden, -politiikan tai -hallintamenetelmien epäiltävää murtumista, tai entuudestaan tuntematonta tilannetta, jonka katsotaan vaarantavan yrityksen tietoturvan (SFS 2014, 5). NIST toimintamallina havainnollistaa sen merkitsevän rekisteröitävissä olevaa esiintymää tietojärjestelmässä tai verkossa – tällainen voi ilmetä esimerkiksi palomuurin pysäyttämänä käyttäjän yrityksenä päästä käyttösäännöissä kielletylle verkkosivustolle – sekä eriyttää tapahtumasta edelleen kielteiseen lopputulokseen johtavan tapahtuman (adverse event), tarkoittaen esimerkiksi pääkäyttäjätunnusten luvatonta käyttöä (Cichonski, Grance, Millar & Scarfone 2012, 6). Toisaalta, ISO/IEC 27035 -standardi painottaa, ettei tapahtumaa tule aina nähdä takeena onnistuneesta yrityksestä, eikä se vaikuta toimintojen luotettavuuteen, saatavuuteen tai eheyteen – toisin sanoen, jokaista tapahtumaa ei voida pitää poikkeamana. (SFS 2011, 2).

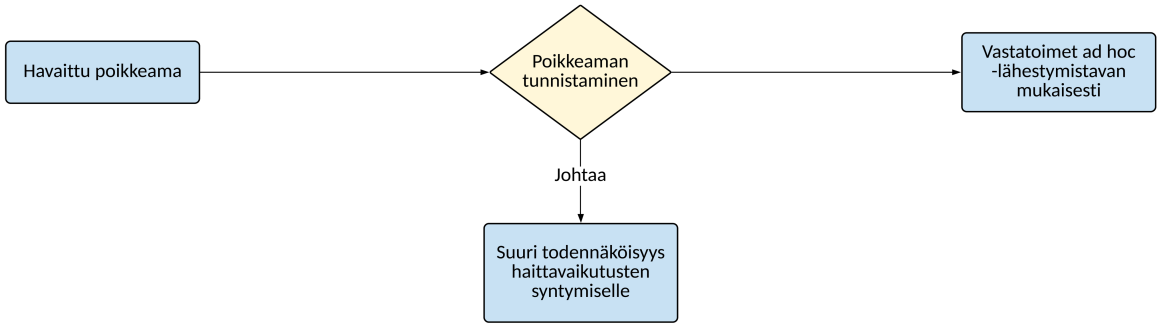
Mitä sitten tarkoitetaan poikkeamalla? ISO/IEC 27000 -standardi näkee sen tarkoittavan yhtä tai useampaa etukäteen odottamatonta tapahtumaa, jotka voivat yhdessä muodostaa mittavan todennäköisyyden sekä liiketoiminnan vaarantumiselle, että tietoturvallisuuden eheydelle (SFS 2014, 5). NIST ryhmittelee poikkeaman yrityksen tietoturvapolitiikkaa ja suoraan turvallisuuteen vaikuttavia periaatteita loukkaavaksi tapahtumaksi, tai vähintään välittömäksi rikkomisen vaaraksi (Cichonski ym. 2012, 6). Samoilla linjoilla oleva SANS luokittelee poikkeaman koskemaan yrityksen it-resursseja käsitteleviä politiikkoja, lakeja tai ohjeita rikkovaksi toiminnaksi (Kral 2011, 1). Edellä mainituista poiketen, ITIL lähtee palvelutuotannon viitekehyksessään tarkastelemaan poikkeamaa suunnittelemattomana tietotekniikkapalveluiden keskeytymisenä, sen laadun heikentymisenä, tai konfiguraation rakenneosan pettämisenä, joka ei kuitenkaan ole vielä ehtinyt vaikuttamaan ratkaisevassa määrin käytännön palvelutoimintaan (Brewster, Griffiths, Lawes & Sansburg 2012, 166).

2.3 Tietoturvapoikkeamanhallinta käsitteenä

Poikkeamanhallintaa voidaan lähestyä hyvinkin monesta suunnasta. ITIL tarkastelee sitä kaikkia poikkeamia käsittelevänä prosessina – nämä voivat olla poikkeamia, jotka ehtivät vaikuttaa palveluiden laatuun, tai vastaavasti poikkeamia, joille tällaista vaikutusta ei vielä ole kehittynyt. Hallinnalle varatut voimavarat kohdistetaan tässä prosessissa poikkeamien vaikutusten tehokkaaseen hallitsemiseen linjassa liiketoiminnan strategisten prioriteettien kanssa. (Brewster ym. 2012, 166.) ISO/IEC 27035 -standardi painottaa keskeisenä osana hallintaa jäsenneltyä ja hyvin suunniteltua lähestymistapaa, jossa etenemällä hierarkkisesti poikkeaman elinkaaren ajan suunnittelusta ja tunnistamisesta torjuntaan sekä käsittelystä oppimiseen, parannetaan hallinnan laatua niin tietoturvan, poikkeamien priorisoinnin ja varhaisen estämisen osalta, kuin myös hellitetään hallinnollisia rutiineja (SFS 2011, 3-5). Voidaan siis avoimesti todeta, että poikkeamanhallinnan kokonaisuudessa poikkeamien tehokas estäminen, hallinta ja ratkaiseminen ovat avainroolissa, kun tavoitteena on nopea palvelutoiminnan palautuminen ja haitallisten vaikutusten minimointi (ENISA 2010, 9).

2.4 Tietoturvapoikkeamien vasteryhmä

Huolimatta kasvaneista tietoturvauhkista, monella yrityksellä on yhä taipumusta vähätellä poikkeamanhallinnan roolia liiketoiminnan kriittisenä tukipilarina. Taustaprosessit ovat usein epäformaaleja ja poikkeamiin reagoidaan hitaasti ad hoc -tyylisellä lähestymistavalla (kuvio 2), jossa kukin organisaatioyksikkö aloittaa itsenäisesti poikkeaman käsittelyn aina poikkeaman ilmaantuessa. Formaalien toimintatapojen puute mahdollistaa liiketoimintaa haittaavien poikkeamien synnyn, ja siten lisää riskiä turhille oikeudellisille toimenpiteille tietoturvaloukkausten seurauksena. (Killcrece, Kossakowski, Ruefle & Zajicek 2003, vii.)



Kuvio 2. Tietoturvapoikkeamien hallinta ad hoc -lähestymistapaan pohjautuen

On varsin yleistä, että reagointi poikkeamiin on hidastunut puutteellisen dokumentaation takia, johtaen vastuunpakoiluun, viivästyksiin, sekä siten mittavampiin haittavaikutuksiin. Yhtenä mahdollisena ratkaisuna tilanteeseen voidaan harkita yrityksen eri asiantuntijoista koostuvan tietoturvapoikkeamien vasteryhmän (Incident Response Team) sulauttamista osaksi sen nykyistä poikkeamanhallintaa, jonka tehtävänä on varmistaa dokumentoitujen toimintatapojen oikeaoppisella käsittelyllä vaihtuvan tilanteen nopea hallinta, analysointi ja palautuminen koko elinkaaren ajan. (Borodkin 2001, 2.) Nopeus on siis valttia tässäkin asiassa – mitä nopeammin yrityksen onnistuu ottaa käyttöönsä kyseinen vasteryhmä, sitä tehokkaammin pystytään lyhentämään poikkeamien elinaikaa, heikentämään vaikutuksia päivittäiselle liiketoiminnalle, vähentämään palautumisesta aiheutuvia kustannuksia, sekä mahdollistamaan todisteiden kerääminen ja virheistä oppiminen (Wheatman 2010, 1-4).

Vasteryhmän rakenne, roolit ja tehtävät vaihtelevat yrityksen koosta ja tarpeista riippuen. NIST ehdottaa ratkaisuna kolmea eri rakenne- ja henkilöstömallia. Näistä ensimmäisessä, keskitetyssä rakennemallissa tietoturvaloukkauksia käsittelevä ryhmä on yksin vastuussa poikkeamanhallinnasta, soveltuen siten pienille tai suuremmillekin yrityksille, edellyttäen kuitenkin tietoteknisiltä laitteilta vähäistä maantieteellistä etäisyyttä. Hajautetussa mallissa ryhmiä on useita, jokaisen vastatessa eri yksiköstä tai toimipaikasta, muodostaen yhdessä koordinoidun kokonaisuuden, joka soveltuu erityisesti suurille tai lukuisilla toimipaikoilla toimiville yrityksille. Koordinoivassa mallissa ryhmä tarjoaa opastusta muillekin ryhmille, muttei omaa niiden suhteen erityistä päätäntävaltaa. Asiantuntijat valitaan joko sisäisestä, osittain ulkoistetusta tai täysin ulkoistetusta henkilöstöstä. (Cichonski ym. 2012, 13-14.)

Vasteryhmän henkilöstön tulee olla teknisesti koulutettua ja osaavaa. Ryhmässä tuleekin siis olla erityistä asiantuntemusta vähintään tärkeimmiltä osa-alueilta, kuten tietoverkoista ja -turvallisuudesta, järjestelmistä, ohjelmoinnista sekä teknisestä tuesta. On ensiarvoisen tärkeää kasvattaa ja ylläpitää asiantuntijoiden erikoisosaamista, sillä tällä tavoin pystytään paljastamaan ilmeisiä ongelmakohtia poikkeamanhallinnan prosesseissa ja koulutuksessa. (Cichonski ym. 2012, 15.) Päällikkötason henkilöä suositellaan ryhmän vetäjäksi, toimien samalla yhdyshenkilönä yrityksen ylimpään johtoon – näin varmistetaan ryhmän riittävän toiminnan edellyttämät resurssit (Borodkin 2001, 5; ENISA 2010, 22). Koska tehtäviin kuuluvat asiantuntijoilta saatujen tietojen pohjalta tehtävät päätökset, päälliköllä tulee olla teknistä osaamista. Siksi valinta osuu usein yrityksen tietoturvapäällikköön (SFS 2011, 9).

NIST suosittelee vasteryhmälle sen teknisestä suorituskyvystä vastaavaa vastuuhenkilöä, sekä lisäksi suuremmissa yrityksissä toisen vastuuhenkilön nimittämistä yhteyshenkilöksi poikkeamanhallintaa tukemaan. Ryhmän päällikölle ja vastuuhenkilöille on myös tarpeen asettaa varahenkilöt. (Cichonski ym. 2012, 14-16.) Koska resurssit ovat monesti rajalliset, tulee yrityksen analysoida nykyisiä tehtäviä ja havaittujen poikkeamien määriä, sekä lisäksi selvittää, nähdäänkö täysipäiväiselle, vuorokauden ympäri päivystävälle ryhmälle tarvetta, vai sopisiko virtuaalinen malli näiden kustannustehokkaampana välimuotona paremmin yrityksen tarpeisiin. Tällä tavoin asiantuntijajäseniä voidaan kutsua ryhmän avuksi, mikäli tilanteen vakavuus edellyttää juuri kyseisen osa-alueen asiantuntijan osaamista. Ketterällä ja joustavalla ratkaisulla voidaan supistaa merkittävästi henkilöstökustannuksia, johtaen kustannustehokkaaseen ja mukautumiskykyiseen ryhmään. (McMillan & Walls 2012, 3.)

Poikkeamanhallinnassa ei kuitenkaan ole kyseessä pelkästään tekninen prosessi, vaan sen vaikutukset ulottuvat yrityksen jokapäiväiseen liiketoimintaan. Ketterä hallinta edellyttää organisatoristen ryhmien yhteistyötä, ja siksipä yrityksessä onkin pohdittava, millä tavoin muiden ryhmien osaamista voidaan hyödyntää. (Cichonski ym. 2012, 16-17.) Esimerkiksi laki- ja henkilöstöyksiköistä saatava asiantuntemus voi osoittautua erityisen tarpeelliseksi yrityksen kartoittaessa yksittäisen työntekijän aiheuttaman poikkeaman liiketoiminnallisia seurauksia, kun taas viestintäyksikkö ottaa vastuun kaikesta kommunikoinnista ulospäin. Turvallisuusyksikköä voidaan puolestaan hyödyntää eskaloituneen tilanteen rauhalliseen purkamiseen, tai esimerkiksi rikostutkinnan kannalta oleellisen fyysisen todistusaineiston turvalliseen säilyttämiseen tulevaa oikeudenkäyntiä varten. (Vangelos 2004, 2979-2980.)

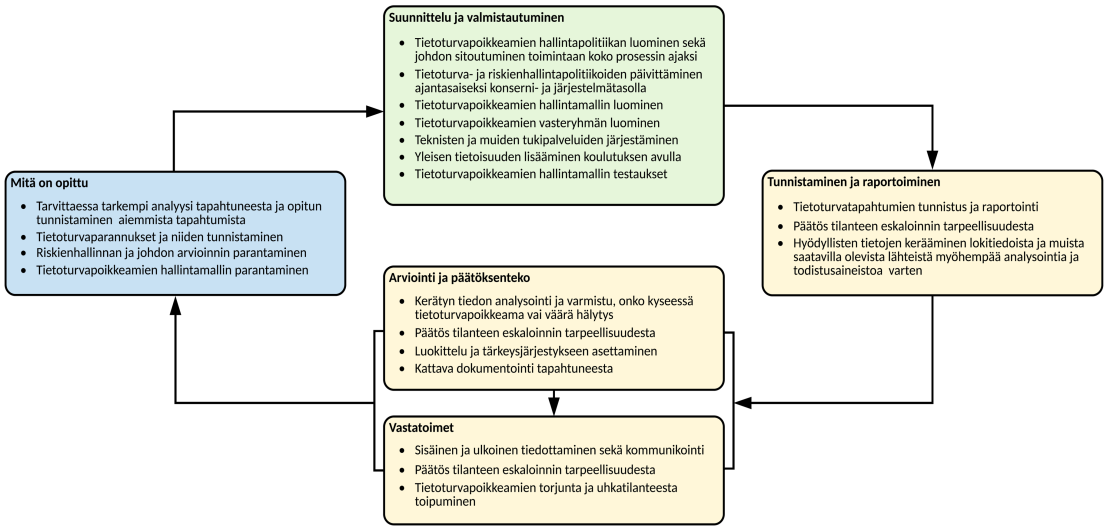
Tietoturvapoikkeamien hallintapolitiikassa ja -mallissa on olennaista määritellä etukäteen tarkat pelisäännöt yhteistoiminnan osalta. Tällä tavoin varmistetaan lisävoiman saaminen ryhmän avuksi mahdollisimman pikaisella aikataululla poikkeamatilanteen niin vaatiessa. (Proffitt 2007, 25; SFS 2011, 18-19.) Poikkeamanhallinnan toteuttaminen lasketaan usein vasteryhmän päätehtäväksi, mutta tämä muodostaa vain osan sen tuottamista palveluista – riippuen yrityksen rakenteesta ja tarpeista, ryhmä voi tarjota itsenäisesti tai yhteistyössä muiden yksiköiden kanssa osaamistaan tunkeutumisen havaitsemiseen liittyvissä tiloissa, tiedottaa ajankohtaisista uhkista, tai esimerkiksi järjestää poikkeamanhallinnan perusteita käsittelevää koulutusta yrityksen koko henkilöstölle, keventäen näin ryhmän työtehtävien runsautta pitkällä aikavälillä (Cichonski ym. 2012, 18-19; West-Brown ym. 2003, 23-24).

3 Standardit ja toimintamallit

Tässä teorialuvussa tarkastellaan tarkemmin ISO/IEC 27035 -standardin perusteita sekä siinä esitettyjä suosituksia tietoturvapoikkeamanhallinnan osalta. Lisäksi käydään lyhyesti läpi kahden tunnetun toimintamallin ja ITIL-palvelutuotannon viitekehyksen suosituksia poikkeamanhallintaan. Tutkimus perustuu keskisuuren toimijan prosessien tarkasteluun, joten ISO/IEC 27035 -standardi soveltuu ominaisuuksiltaan tämän teorialuvun pohjaksi.

3.1 Standardit: ISO/IEC 27035

Edellisen luvun johdannon yhteydessä todettiin ISO/IEC 27035 -standardin perustuvan tietoturvapoikkeamanhallinnan käsittelyyn, sen ensisijaisen tavoitteen ollessa päivittäisen yritystoiminnan ja tietoturvallisuuden turvaamisessa. Standardin toissijaisena tavoitteena on toimia tukipilarina tietoturvapoikkeamien hallintajärjestelmälle vaatimukset asettaville ISO/IEC 27001- ja ISO/IEC 27002 -standardeille, kasvattaen yritysten mahdollisuuksia vaatimustasojen läpäisemiseksi. (SFS 2011, 1-4.) Tämän toteuttamiseksi standardi esittää viisiosaista hallintamallia (kuvio 3), jossa ensimmäisellä vaiheella on jatkuva rooli, muiden vaiheiden keskittyessä pelkästään operatiiviseen toimintaan. Hallintamalli alkaa jatkuvasti päivittyvästä suunnittelusta ja valmistautumisesta, edeten operatiivisiin tunnistamiseen ja raportointiin, arviointiin ja päätöksentekoon, vastatoimiin, sekä lopuksi prosessin aikana havaituista ja kattavasti dokumentoiduista häiriötilanteista oppimiseen. (SFS 2011, 6-7.)



Kuvio 3. Tietoturvapoikkeamien hallintamalli (lähde mukaillen SFS 2011, 7)

3.1.1 Suunnittelu ja valmistautuminen

Suunnittelun ja valmistautumisen vaihe muodostaa hallintamallissa jatkuvasti päivittyvän roolin, jossa painotetaan kriittisten haavoittuvuuksien selvittämistä tietoturva-auditointia hyödyntäen, tietoturvapoikkeamien hallintamallin tarpeellisuuden selvittämistä, sekä siitä niin yritykselle kuin myös sen yksiköille aiheutuvien hyötyjen tunnistamista. Kartoituksen pohjalta malli esittää poikkeamien, tapahtumien sekä haavoittuvuuksien hallintapolitiikan luomista, joka voidaan eriyttää itsenäiseksi kokonaisuudeksi, tai sulauttaa osaksi yrityksen tietoturvallisuuden hallintajärjestelmä- ja tietoturvapolitiikoita. Hallintapolitiikka erittelee selkeästi tapahtumien tunnistamiseen, raportointiin ja tiedonkeruuseen liittyvät prosessit, millä perusteilla tietoja käytetään poikkeamien määrittelyssä, kriittisimpien tapahtumien tunnusmerkistöt ja raportoimisen, sekä uusissa olosuhteissa toimimisen. (SFS 2011, 8-9.)

Hyödyllisinä aiheina voidaan nähdä myös tapahtumasta poikkeamaksi etenemisen sisältö, sen jälkeisten vaiheiden ja opitun tiedon hyväksikäytön määrittely, teknisten ja juridisten tukitoimien yleiskuvaus, sekä yrityksen henkilöstön poikkeamanhallinnan ymmärtämistä lisäävän koulutuksen ja harjoittelun selkeä esilletuominen. Poikkeamien vasteryhmä ottaa vetovastuun operatiivista toiminnoista – siksi sen organisatorisen rakenteen kuvaaminen ja päivittäisestä toiminnasta vastaavien johto- ja avainhenkilöiden yhteystietojen tulee olla yrityksen koko henkilöstön vapaasti saatavilla helpottamaan ja nopeuttamaan esimerkiksi ennalta odottamattomien poikkeamatilanteiden tiedottamista. Mallissa painotetaan myös ryhmän mission eli toiminta-ajatuksen, ydintehtävien ja niiden laajuuden, sekä yrityksessä asetettujen tavoitteiden määrittelemistä itsenäisenä dokumentaationa. (SFS 2011, 10-12.)

Tietoturvapoikkeamien hallintamalli käsittää siis viisi vaihetta, joista jokaisella on roolinsa yrityksen tietoturvan tehokkaassa turvaamisessa. Sen tavoitteena on kuvata poikkeamien, tapahtumien ja haavoittuvuuksien sekä niihin oleellisesti liittyvän tiedonvälityksen parissa tapahtuvia toimenpiteitä yksityiskohtaisena dokumentaationa, tullen voimaan havaittujen poikkeamien tai tapahtumien ilmaantuessa. Hallintamalli voidaankin nähdä hierarkkisena oppaana poikkeamatilanteessa, sekä olennaisena taustavaikuttajana poikkeamanhallinnan suunnittelun ja valmistautumisen prosesseissa. Siksi onkin tärkeää osoittaa hallintamallin dokumentaatio niin henkilöstölle, palvelutoimittajille kuin kolmansille osapuolille, jakaen näin yhdessä vastuun poikkeamien tunnistamisesta ja raportoinnista. (SFS 2011, 13-14.)

Tämän samaisen dokumentaation on annettava yksityiskohtainen kuvaus siihen läheisesti sidoksissa olevasta hallintapolitiikasta, eriteltävä hallintamallin toimintavaiheiden sisällöt, sekä sisällettävä tarvittavat tukityökalut korkealuokkaisen hallinnan mahdollistamiseksi. Näitä ovat esimerkiksi poikkeamien luokittelemisessa ja kategorioinnissa hyödynnettävät asteikot (classification/categorization scale), uhkatilanteen eskaloitumista ja raportointia yritystasolla helpottavat järjestelmälliset toimintatavat, poikkeamista ja muista haitallisista tapahtumista ilmoittamista ja niiden käsittelemistä nopeuttavat sähköiset lomakkeet sekä mahdollista oikeuden istuntoa varten suoritettavaa laajaa rikostutkintaa yhdenmukaistava tekninen lokiseuranta ja tunkeilijoiden havaitsemisjärjestelmä. Tarkasti dokumentoitujen toimintaprosessien ja henkilövastuiden luomista osana varsinaista tietoturvapoikkeamien vasteryhmän perustamista pidetään merkkinä tehokkaasta hallinnasta. (SFS 2011, 13-16.)

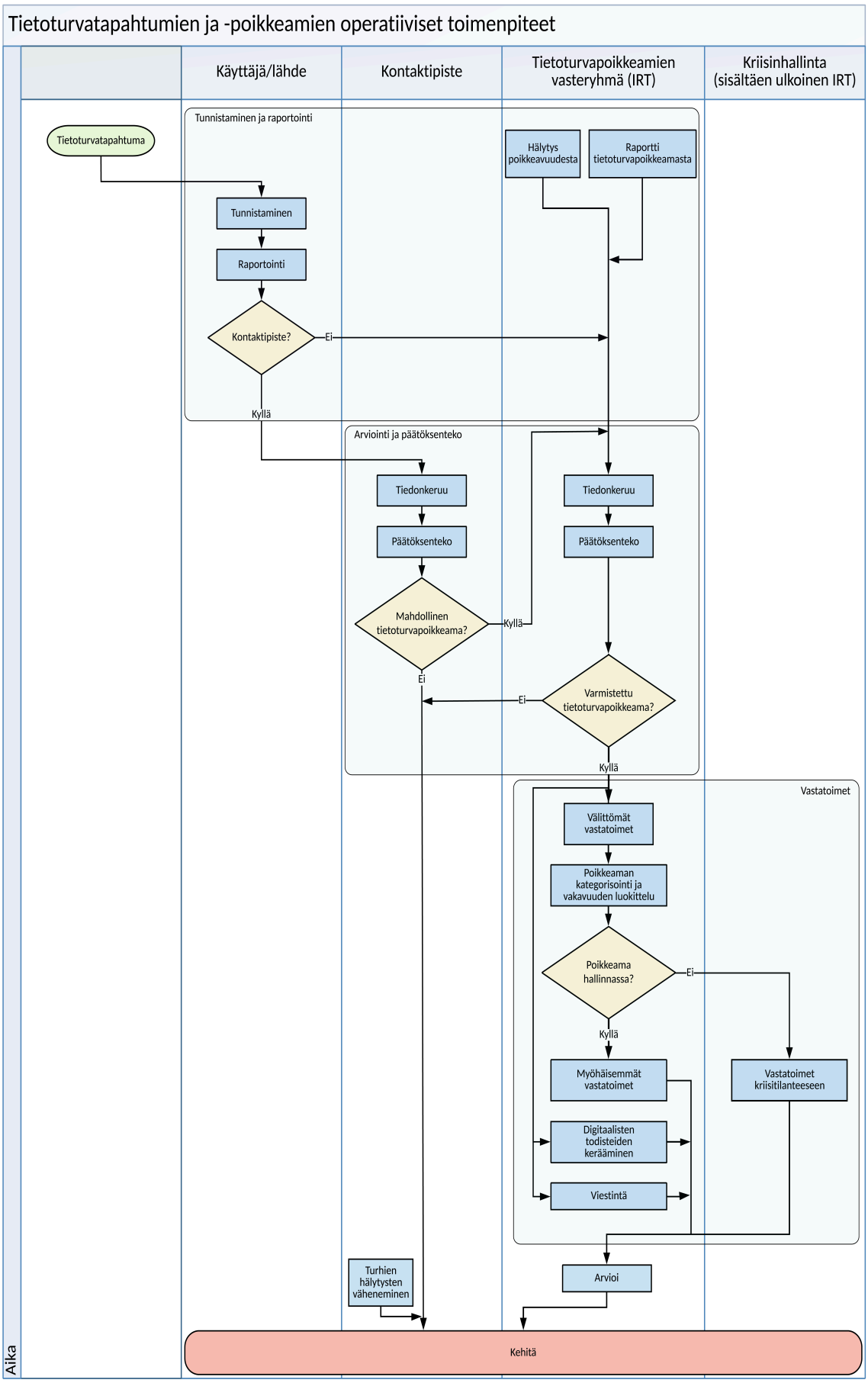
Tietoturvapoikkeamien vasteryhmällä on merkittävä rooli yrityksen tietoturvallisuudessa, turvautuen suurelta osin henkilöstön yhteistyökykyyn poikkeamien tunnistamisen, niiden määrittämisen sekä ratkaisemisen suhteen, painottaen näin ryhmän ja henkilöstön välisen luottamuksen merkityksellisyyttä. Hallintamallin tulisikin huomioida yksityisyydensuojan takaamiseen tarvittavat toimenpiteet sekä huolehtia ryhmän toiminnan läpinäkyvyydestä. Jälkimmäinen onnistuu esimerkiksi toistuvalla henkilöstön kouluttamisella ja päivittäisen toiminnan esittelemisellä, eli osoittamalla miten käyttäjiltä kerättyjä tietoja hyödynnetään sekä miten niiden anonyymiyttä suojellaan – näin pystytään maksimoimaan poikkeamien raportoinnista lyhyellä ja pitkällä aikavälillä saavutettavat hyödyt. (SFS 2011, 17.) Ryhmän rakennetta, rooleja ja suhteita yrityksen eri yksiköihin tarkasteltiin laajemmin luvussa 2.4.

Standardi näkee eritoten tärkeänä toimintatapojen dokumentointia ja niiden saatavuuden takaamista ennen hallintamallin käyttöönottoa, sekä dokumentoidun hallintapolitiikan ja muiden hallintamallin eri dokumentaatioiden välistä täsmäävyyttä. Kannattaa huomioida, että operatiivisista toimintatavoista on ilmettävä selvästi kenen vastuulle mikäkin tehtävä kuuluu, ja että tunnettujen ja tuntemattomien poikkeamien käsittelyyn tarvitaan itsenäiset toimintaprosessit. Monet yritykset ovat kuitenkin ottaneet jo aiemmin käyttöön useitakin politiikkoja – näiden yhteensopivuus hallintapolitiikan kanssa varmistetaan sulauttamalla hallinta osaksi päivittyviä tietoturva- ja riskienhallintapolitiikoita, sekä peilaamalla sisältöä politiikoissa viitatun hallintamallin keräämään materiaaliin. Näin taataan niiden saumaton yhteistoiminta ja poikkeamanhallinnan merkityksen osoitus johdolle. (SFS 2011, 16-18.)

Kuten edellä todettiin, henkilöstöllä on siis merkittävä rooli poikkeamien tunnistamisessa ja raportoinnissa, sekä siten vasteryhmän menestyneessä toiminnassa. Tätä ei kuitenkaan voida pitää itsestäänselvyytenä, mikäli henkilöstö ei tiedosta oman panoksensa vaikutusta paitsi yrityksen poikkeamanhallintaan, myös omiin yksiköihinsä, ja siten lopulta itseensä. Yritysjohdolta edellytetäänkin poikkeamanhallinnan roolin tärkeyden tietoisuutta lisääviä toimenpiteitä, kuten esimerkiksi koulutuksen järjestämistä. Siihen liittyvän materiaalin on oltava vapaasti koko henkilöstön, mutta myös kolmansien osapuolien, ja soveltuvilta osin urakoitsijoiden saatavilla. Koulutusmateriaalin on hyvä huomioida poikkeamanhallinnan ja henkilöstön saamat hyödyt järjestelmällisestä lähestymistavasta, laaditun hallintamallin toimintaperiaatteet ja operatiivisten vaiheiden eteneminen sekä edellytykset tapahtumien, poikkeamien ja muiden haavoittuvuuksien raportoinnin toteutukseen. (SFS 2011, 20-21.)

Poikkeamanhallinnassa toimii eri alojen asiantuntijoita, kuten esimerkiksi vasteryhmän ja tietoturvayksikön jäsenet sekä poikkeamanhallinnan erillinen yhteyshenkilö, asettaen siis koulutuksen sisältöä suunniteltaessa yksilön erikoistarpeille omat vaatimuksensa. Jatkuva henkilöstön vaihtuminen on syytä huomioida jaksottaisella ja säännöllisesti päivitettävällä koulutusohjelmalla, sekä esimerkiksi lisäämällä poikkeamanhallinta osaksi työntekijöiden perehdytystä. Yksi tärkeimmistä hallintamallin käyttöönoton vaiheista on kuitenkin siinä esiteltyjen toimintatapojen ja prosessien toimivuuden varmistaminen säännöllisten, uusia vakavia ja monimutkaisia reaalimaailman poikkeamia simuloivien harjoitusskenaarioiden avulla. Näiden ensisijainen tarkoitus on oletettavien ongelmakohtien esiintuominen, sekä poikkeamanhallinnan ja vasteryhmän tarkkaileminen paineen alaisena. (SFS 2011, 21-22.)

Kyseisistä harjoituksista kerättyjen havaintojen pohjalta hallintamalliin voidaan toteuttaa tarvittaessa muutoksia, joiden toiminta tulee testata huolellisesti ennen uudistetun mallin operatiivista käyttöönottoa. Näin saavutetaan mallin käynnistysvaiheen menestyksellinen toteutus, henkilöstön selkeä ymmärrys ja motivaatio poikkeamien tunnistamiseen, niihin liittyviin toimenpiteisiin ja niistä raportointiin, ylimmän yritysjohdon säännönmukainen ja dokumentoitu sitoutuminen hallintamalliin ja -politiikkaan sekä niiden parantamiseen. Nämä edellä mainitut muodostavat yhdessä luonnollisen siirtymän poikkeamanhallinnan operatiivisiin vaiheisiin (kuvio 4), ja mahdollistavat samalla perusedellytysten syntymisen hierarkkisen etenemisen kokonaisuudelle, johtaen lopulta laadukkaammin suunniteltuun, johdonmukaiseen sekä turvalliseen poikkeamanhallinnan toteuttamiseen. (SFS 2011, 22.)



Kuvio 4. Operatiivisten toimenpiteiden rakenne (lähde mukaillen SFS 2011, 23)

3.1.2 Tunnistaminen ja raportointi

Kun tietoturvapoikkeamien hallintamalli ja siihen läheisesti sidoksissa olevat politiikat on saatu dokumentoitua – ja siten ensimmäinen eli jatkuva suunnittelun ja valmistautumisen vaihe käyttöönotettua menestyksellisesti – aloitetaan poikkeamanhallinnan nelivaiheinen operatiivinen prosessi, jossa tunnistamisen ja raportoinnin tärkeässä roolissa keskitytään nimensä mukaisesti tapahtumien, poikkeamien ja haavoittuvuuksien tunnistamiseen sekä saatavilla olevan tiedon keräämiseen ja niistä edelleen raportoimiseen. Usein ensihavainto tuleekin yrityksen omalta henkilöstöltä, asiakkailta, tai automatisoituna tietojärjestelmien sekä ohjelmistojen välityksellä. Tunkeilijoiden havaitsemis- ja lokienseurantajärjestelmät, virustentorjuntaohjelmistot, palomuurit, verkon suodattaminen, hyökkääjiä harhauttavat järjestelmät, kuten hunajapurkki (honeypot), sekä lokitietojen analysointi ovat yleisimpiä esimerkkejä jälkimmäisestä. Ulkoiset toimijat, kuten tietoliikenneoperaattorit, kansalliset viranomaiset ja kilpailevat vasteryhmät voivat myös varoittaa uhkista. (SFS 2011, 24-25.)

Riippumatta yrityksen toiminnalle potentiaalisesti haitallisten tapahtumien tunnistamisen lähteestä, ilmoituksen tekijä tai automatisoidusta tietojärjestelmästä tiedon vastaanottava henkilö vastaa tunnistamisen ja raportoinnin toimintojen aloittamisesta sekä tapahtuman saattamisesta yritysjohdon ja edeltäpäin nimettyjen yhteyshenkilöiden (Point of Contact) tietoisuuteen toimintatapojen mukaisesti hallintamallissa kuvaillun raportointilomakkeen avulla. Yhteyshenkilön vastuulla on kirjata käsittelyn vaiheet, varmistaa todistusaineiston kerääminen ja turvallinen, monitoroitu säilytys. Tapahtumista ja poikkeamista on tärkeää hankkia mahdollisimman kattavasti tietoa ennen tallentamista vasteryhmän ylläpitämään tietokantaan sekä poikkeamien seurantajärjestelmään; automatisointi nähdään käytännön prosessien ja tarkistuslistojen noudattamista tukevana parannuksena. (SFS 2011, 25-26.)

Vasteryhmän tulee eriyttää yksi jäsenistään vastaamaan saapuvien raporttien selvittelystä, vuorojen vaihdellessa esimerkiksi viikoittain. Sähköisten raportointikeinojen käyttämistä ei suositella vakavan uhkan ilmaantuessa, mikäli järjestelmien eheydestä ei ole varmuutta. Potentiaalisena vaarana olisi ulkopuolisten pääsy raportointilomakkeiden arkaluonteisiin tietoihin. Tästä johtuen on tärkeää huomioida henkilöstön olevan perehtynyt huolellisesti poikkeamanhallinnan ohjeisiin ja yhteyshenkilöihin, sekä missä lomakkeita varastoidaan, helpottaen operatiivisen prosessin arvioinnin ja päätöksenteon toimintaa. (SFS 2011, 26.)

3.1.3 Arviointi ja päätöksenteko

Hallintamallin toinen operatiivinen vaihe käynnistyy tietoturvatapahtuman onnistuneesti suoritetun tunnistamisen jälkeen. Tehtävänä on tapahtumaan liittyvien tietojen läpikäynti ja arviointi sekä pohtiminen, kuinka arvioinnin pohjalta olisi hyvä edetä. Tapahtumaketju saa alkunsa poikkeamanhallinnan yhteyshenkilön vastaanottaessa ilmoituksen havaitusta tapahtumasta ja kirjatessa nämä tiedot vasteryhmän ylläpitämään tietokantaan, arvioiden samalla yrityksessä yhteisesti hyväksytyn luokitteluasteikon avulla täyttäisikö tapahtuman esitiedot sittenkin poikkeaman tunnusmerkistön. Luokittelussa painottuu uhkan alaisena olevan kohteen tai palvelun vaikutukset yrityksen ydintoiminnoille luottamuksellisuuden, eheyden ja saatavuuden osalta. Arviointivaiheen aikana on oleellista ennakoida sähköisen todistusaineiston keräys myöhäisempää käyttöä varten, jotta lokitiedot ovat käytettävissä heti tilanteen alusta, edellyttäen asiankuuluvan koulutuksen järjestämistä. (SFS 2011, 27.)

Tapahtuman osoittautuessa vääräksi hälytykseksi, suljetaan tapaus ja varmistetaan sujuva tiedonkulku sekä tapahtumasta ilmoittaneelle henkilölle että vasteryhmälle, unohtamatta kuitenkaan käsittelyvaiheiden kirjaamista ryhmän tietokantaan. Mikäli tapahtuma lopulta todetaan merkittävällä todennäköisyydellä haitalliseksi poikkeamaksi, voidaan käsittelijän asiantuntemuksesta riippuen pyrkiä löytämään tilanteeseen ainakin osittainen ratkaisu jo tässä vaiheessa, sekä tarvittaessa eskaloida tilanne johdon tietoon. Lisäksi yhteyshenkilön tehtävänä on varmistaa tapauksen olevan työstettävissä ilmoituksessa annettujen tietojen perusteella, informoida tietoturvapäällikköä tapahtuneesta sekä tarvittaessa ohjata tilanne vasteryhmälle sen perinpohjaisempaa analysointia ja käsittelyä varten. (SFS 2011, 27-28.)

Vasteryhmän tehtävänä puolestaan on varmistaa yhteyshenkilön suorittaman arvioinnin paikkansapitävyys sekä tarvittaessa edellä mainitun luokitteluasteikon avulla saada riittävä selvyys, onko kyseessä aito vai väärä hälytys. Tässä vaiheessa on tärkeää verrata kerättyjä tietoja aiempiin tapauksiin yhtenevien tapausten poissulkemiseksi. Varsinaisessa uhkassa tilanne tulee arvioida uudelleen – millainen uhka on kyseessä, mistä se aiheutui ja millaiset sen vaikutukset yrityksen liiketoiminnalle ovat – sekä siten kartoittaa uhkan vakavuusaste ja aloittaa tarvittavat jatkotoimenpiteet. Erityisesti päällekkäisissä tilanteissa vasteaikojen on oltava nopeita, ja siksi yrityksen liiketoimintaan pohjautuvalla priorisoinnilla saatetaan ohjata resursseja tehokkaasti kunkin tilanteen vaatimusten mukaisesti. (SFS 2011, 30-31.)

3.1.4 Vastatoimet

Hallintamallin kolmas operatiivinen vaihe käsittelee poikkeamatilanteen vastatoimia sekä niihin liittyviä ohjeistuksia. Kyseiset vastatoimet pohjautuvat mallin edellisessä vaiheessa tehtyihin päätöksiin. Tämä vaihe sisältää vastatoimet sisäisesti tai ulkoisesti raportoituihin uhkatilanteisiin. Huolimatta tehdyistä päätöksistä, vasteryhmä vastaa poikkeamatilanteen hallinnan varmistamisesta, sekä käynnistää ennalta sovitut toimenpiteet, kuten tilanteesta palautumisen, kattavan dokumentoinnin ja yhteydenpidon tarvittavien osapuolten välillä. Muutoin tilanteen eskalointi kriisinhallintaa varten voi olla välttämätöntä. (SFS 2011, 31.)

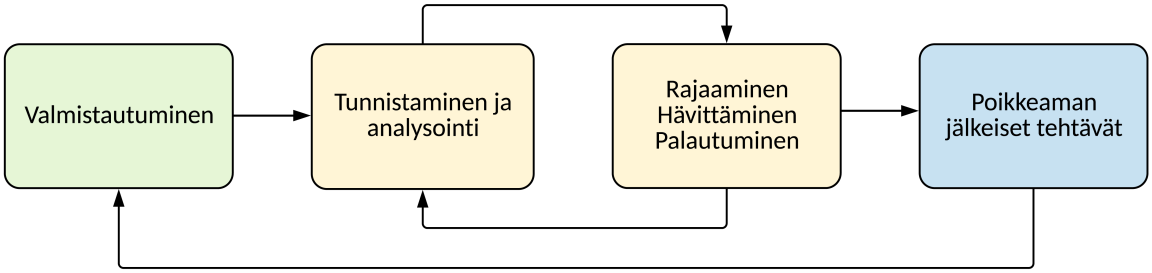
On erityisen tärkeää pitää huoli, että kaikki vasteryhmän tekemät toimenpiteet ja ratkaisut kirjataan sen ylläpitämään tietokantaan ja formaaleja ohjeistuksia noudatetaan yhtenäisen dokumentoinnin varmistamiseksi. Lokimerkinnät vauhdittavat myöhemmässä vaiheessa yrityksen kartoitusta, jossa tilanteen ratkaisemisen tehokkuutta ja suorituskykyä pystytään arvioimaan tarkasti, sekä mahdollistavat todistusaineistojen hyväksikäytön mahdollisissa rikostilanteissa. Onkin vasteryhmän vastuulla, että eheydeltään vaarantuneet järjestelmät saadaan pikaisesti jälleen toimintakykyisiksi, ja ettei samaisella uhkalla voida enää jatkossa häiritä kyseisiä järjestelmiä. Tilanteen lopuksi ryhmä sulkee tapauksen. (SFS 2011, 32-33.)

3.1.5 Mitä on opittu

Hallintamallin viimeinen operatiivinen vaihe on samalla myös yksi sen merkittävimmistä, käynnistyen edellisen vaiheen vastatoimenpiteiden tehottua ja uhkatilanteen tullessa siten ratkaistuksi. Oppimisen vaihe keskittyy nimensä mukaisesti pohtimaan, kuinka yrityksen poikkeamanhallinnan prosessit ovat edistyneet kokonaisuudessaan, toimiko hallintamalli suunnitellusti sekä mitä voitaisiin tehdä jatkossa paremmin. Lisäksi vaiheessa keskitytään politiikoissa, toimintatavoissa, raportointilomakkeissa ja riskiarvioinneissa rekisteröityjen puutteiden korjaamiseen joko välittömästi tai päivitysten yhteydessä. Onkin huomioitava tarvittavien muutosten koskevan aina koko järjestelmää, ei siis vain vaarantunutta osiota. Oppimisen vaiheessa näkyvät monet toistuvat toiminnot, kuten esimerkiksi poikkeamien jatkuvaluonteinen dokumentointi ja trendianalyysit. Näistä saatuja tuloksia tulee käsitellä luotettavien yhteistyökumppanien kesken. Tämän kaiken tarkoituksena on johtaa lopulta tietoturvapolitiikoiden sekä toimintatapojen jatkuvaan parantamiseen, muodostaen siten yhden kenties tärkeimmistä vasteryhmän pitkän aikavälin tavoitteista. (SFS 2011, 41-43.)

3.2 Toimintamallit: NIST ja SANS

ISO/IEC 27035 -standardin tärkeimmät perusominaisuudet poikkeamanhallinnan osalta kuvattiin edellä. Suurin osa luvussa 2.1 mainituista toimintamalleista ovat lähtökohdiltaan yhteneväisiä standardin kanssa. Niissä prosessiketju käynnistyy tunnistamisesta ja päättyy lopuksi virheistä oppimiseen – vain näiden välimaastossa esiintyy pieniä poikkeavuuksia. NIST ja SANS Instituten toimintamallit valittiin osaksi tutkimuksen kirjallisuuskatsausta niiden osoittauduttua tutkimuksen rakennetta ja tavoitteita parhaiten tukevaksi. Malleista esitetään seuraavaksi tiivistetysti niiden suositukset poikkeamanhallinnan toteuttamiseen.



Kuvio 5. Poikkeamanhallinnan elinkaari (lähde mukaillen Cichonski ym. 2012, 21)

3.2.1 Valmistautuminen

Poikkeamanhallinnan elinkaari (kuvio 5) on jatkuva tapahtumaketju, jossa tavoitteena on huolellisen valmistautumisen ja toistuvan oppimisen prosessin kautta estää poikkeamien sekä niistä aiheutuvien vahinkojen syntyminen (Kral 2012, 2). Valmistautuminen voidaan siten nähdä poikkeamanhallinnan tärkeimpänä osana, jossa määritetään kuinka tehokasta yrityksen poikkeamiin varautuminen ja vastaaminen todellisuudessa on. Yrityksessä tulisi ottaa käyttöön tietoturvapolitiikka sekä liiketoimintaan läheisesti kytkeytyvä poikkeamien priorisoinnin sisältävä toimintasuunnitelma – se helpottaa tarvittavien resurssien keräystä ja sitouttaa ylimmän johdon sen noudattamiseen. Oleellista on huomioida viestintä osana valmistautumista häiriötilanteiden aikaisilta viivästyksiltä säästymiseksi. (Kral 2012, 2-4.) Säännöllinen dokumentointi edesauttaa virheistä oppimista sekä toimii todistusaineiston roolissa rikostutkinnassa. Tietoturvapoikkeamien vasteryhmä on tärkeä pala myöhempää poikkeamanhallinnan elinkaarta, mutta se voi auttaa riskienhallinnassa ja kouluttamisessa – siksi resurssien ja koulutuksen järjestäminen on keskeistä. (Cichonski ym. 2012, 23-24.)

Menestyneen vasteryhmän toiminnalle on kuvaavaa yrityksen sisäisten yksiköiden välisen yhteistoiminnan merkitys poikkeamanhallinnalle sekä siten kokonaisvaltainen ymmärrys sen vaikutuksista pidemmällä aikavälillä tarkasteltuna – esimerkiksi hyväksymällä ryhmän toimintaan henkilöstö-, laki- ja viestintäyksiköiden asiantuntijoita kriisitilanteiden aikana, saavutetaan monipuolinen ja ketterä varautuminen kehittyviin tilanteisiin. (Kral 2012, 4).

3.2.2 Tunnistaminen ja analysointi

Poikkeama voi esiintyä monella eri tavalla, eikä tunnistamiseen ole vain yhtä menetelmää. Siksi yrityksessä tulisi valmistautua kaikenlaisiin tilanteisiin, mutta keskittyä poikkeamiin, jotka noudattelevat yleisiä hyökkäysvektoreita – esimerkiksi siirrettäviä tallennusmedioita tai sähköpostin liitetiedostoja. Haasteena on varsinaisen poikkeaman tunnistaminen sekä sen vaikutukset yrityksen liiketoiminnalle. Havaintoja voidaan saada monista eri lähteistä, päivittäisten määrien pyöriessä jopa tuhansissa, edellyttäen siten laajaa teknistä osaamista. Tunnistamista helpottavat tunnusmerkit voidaan jakaa kahteen ryhmään: prekursoreihin eli mahdollisesti myöhemmin tapahtuviin sekä indikaattoreihin eli mahdollisesti paraikaa käynnissä oleviin tai jo sattuneisiin poikkeamiin. Niiden yleisiä lähteitä ovat tunkeilijoiden havaitsemisjärjestelmät, SIEM-järjestelmät ja lokiseurannat. (Cichonski ym. 2012, 25-27.) Mikäli tapahtuma osoittautuu lopulta poikkeamaksi, tulee se raportoida mahdollisimman nopeasti ja saattaa vasteryhmän sekä johdon tiedoksi. Käsittelyä varten tulisi nimetä kaksi ryhmän jäsentä – yksi pääasialliseksi käsittelijäksi ja toinen keräämään lisätodisteita. Tässä vaiheessa on tärkeää dokumentoida kaikki tehdyt toimenpiteet ja varmistaa vain rajatuilla henkilöillä olevan pääsy saatuun aineistoon. (Kral 2012, 5-6.) Poikkeaman priorisoinnissa painottuvat toiminnalliset vaikutukset sekä niistä palautuminen (Cichonski ym. 2012, 32).

3.2.3 Rajaaminen, hävittäminen ja palautuminen

Poikkeaman rajaaminen on olennaista pyrittäessä estämään lisävahinkojen syntyminen ja kun halutaan saada lisäaikaa vastasuunnitelman toteuttamiseen. Rajaamisessa painottuvat päätöksenteko sekä etukäteen määritetyt strategiat ja toimintatavat eroavien poikkeamien rajaamista varten. (Cichonski ym. 2012, 35.) Rajaamiseen kuuluu kolme vaihetta: sattunut vahinko rajataan nopeasti eli lyhytaikaisesti esimerkiksi eristämällä osan työasemasta pois verkosta, varmuuskopioidaan saastunut järjestelmä esimerkiksi rikostutkintaa varten sekä pitkäaikainen rajaaminen, jossa järjestelmät korjataan vain väliaikaisesti. (Kral 2012, 6-7.)

Toisinaan pelkkä poikkeaman rajaaminen ei ole riittävä toimenpide, vaan vaaditaan selviä toimenpiteitä poikkeaman haittavaikutusten poistamiseksi. Säännöllinen dokumentointi on tärkeässä roolissa – vain sillä voidaan saada varmuus edellisen vaiheen toimenpiteiden virheettömyydestä. Dokumentoinnilla voidaan myös selvittää poikkeaman toiminnallisia vaikutuksia yritykselle sekä siten parantaa järjestelmien turvallisuutta vastaavilta tilanteilta suojautumiseksi. (Kral 2012, 7-8.) Saastuneiden järjestelmien ollessa todistetusti puhtaita, voidaan palautumisen vaiheessa keskittyä toimintojen uudelleenkäynnistämiseen, samalla varmistaen tarkkailun avulla järjestelmien normaalin toiminnan (Cichonski ym. 2012, 37).

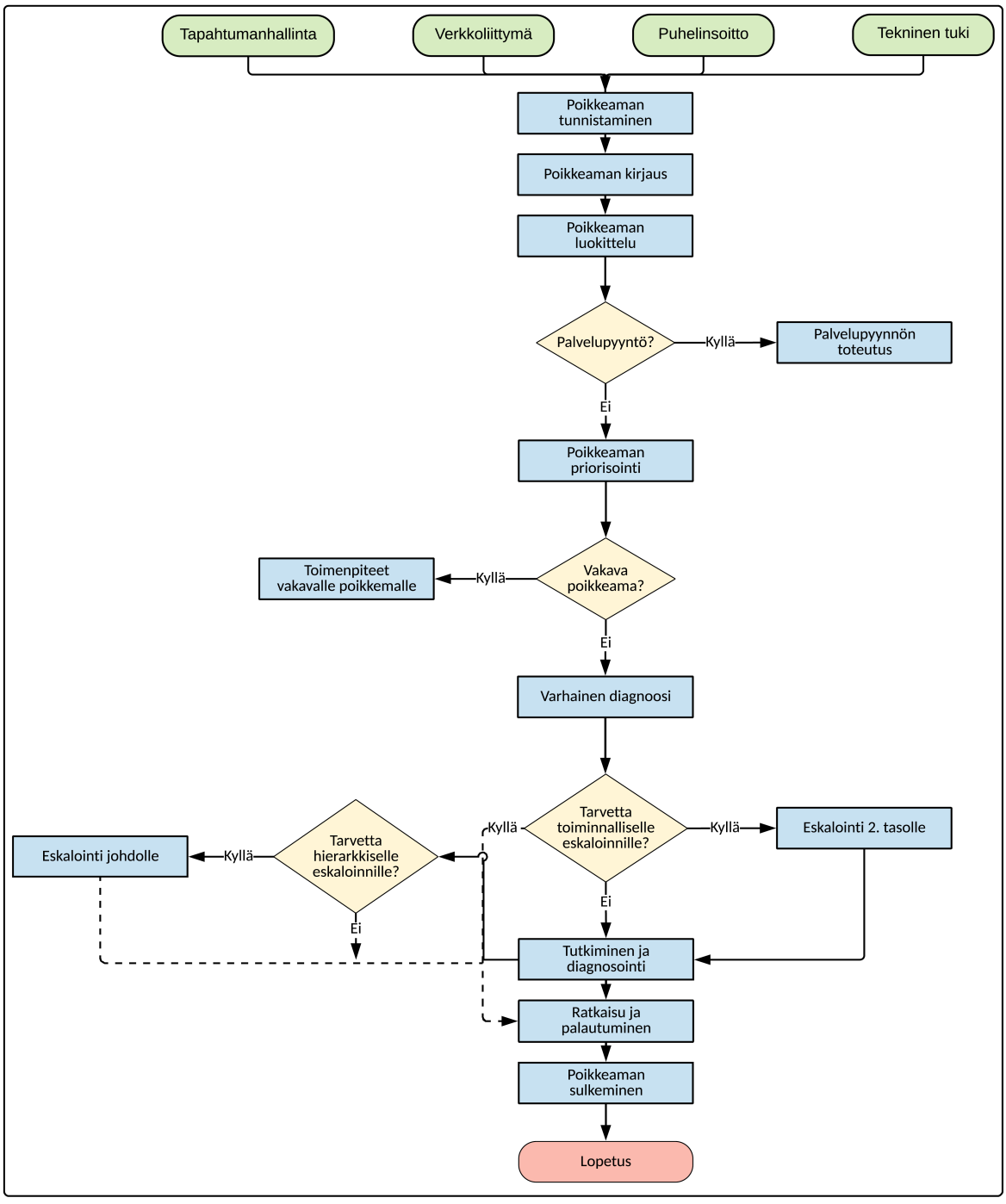
3.2.4 Poikkeaman jälkeiset tehtävät

Virheistä oppiminen ja kehittyminen ovat poikkeamanhallinnan tärkeimpiä mutta useasti laiminlyötyjä vaiheita. On tärkeää saattaa loppuun keskeneräinen dokumentointi ja lisäksi järjestää yhteinen oppimista kasvattava tapaaminen jokaisen merkittävän poikkeamatilan käsittelyn jälkeen. Tapaamisten tulisi keskittyä pohtimaan parannuskohteita, mitkä aiheet epäonnistuivat ja toisaalta mitkä onnistuivat – näin saatavaa aineistoa voidaan hyödyntää kouluttamisessa tai lähdemateriaalina vastaavissa poikkeamatilanteissa. Usein politiikkoja ja toimintatapoja myös päivitetään huomioiden perusteella. (Cichonski ym. 2012, 38-39.) Kaiken tavoitteena on siis vasteryhmän ja yrityksen valmiustason vahvistaminen virheistä oppimalla sekä siten jatkossa vastaavien tilanteiden uusimisen estäminen. (Kral 2012, 9).

3.3 Toimintamallit: ITIL (poikkeamanhallinta)

Poikkeamanhallintaa voidaan lähestyä hyvinkin monesta suunnasta. ITIL tarkastelee sitä kaikkia poikkeamia käsittelevänä prosessina – nämä voivat olla poikkeamia, jotka ehtivät vaikuttaa palveluiden laatuun, tai vastaavasti poikkeamia, joille tällaista vaikutusta ei vielä ole kehittynyt. Hallinnalle varatut voimavarat kohdistetaan tässä prosessissa poikkeamien vaikutusten tehokkaaseen hallitsemiseen linjassa liiketoiminnan strategisten prioriteettien kanssa. Poikkeamanhallinnan prosessien tehtävänä on toimintojen nopea palauttaminen ja liiketoiminnalle aiheutuvien haittavaikutusten lievittäminen. (Brewster ym. 2012, 166.) Tämän prosessin vaiheita on esitetty tarkemmin kuviossa 6. Siinä ilmoitus poikkeamasta vastaanotetaan monesti suoraan käyttäjiltä, tekniseltä henkilöstöltä tai tietojärjestelmistä. Poikkeamat täytyy kuitenkin pystyä tunnistamaan, kirjaamaan sekä luokittelemaan ennen tärkeysjärjestyksiin asettamista. Tärkeysjärjestyksiä on kolme: matala, keskitaso ja korkea.

Tärkeysjärjestys määrittyy poikkeaman vaikutuksen tason ja kriittisyyden mukaan. Mikäli poikkeama osoittautuu vakavaksi, käynnistetään erilliset toimenpiteet vakaville tilanteille. Tarvittaessa poikkeaman käsittely ohjataan eteenpäin eli eskaloidaan joko toiminnallisesti tai hierarkkisesti – ensimmäisellä tarkoitetaan tilannetta, jossa lähituki ei esimerkiksi pysty ratkaisemaan poikkeamatilannetta yksin, kun taas jälkimmäisen tapauksessa poikkeaman vakavuus edellyttää korkeamman tason auktoriteettia. Lähituen tulisi olla vetovastuussa tutkimisesta ja tunnistamisesta ennen tilanteen sulkemista. (Brewster ym. 2012, 167-170.)



Kuvio 6. Poikkeamanhallinnan rakenne (lähde mukaillen Brewster ym. 2012, 168)

4 Tutkimusmenetelmät

Tässä tutkimuksessa päädyttiin valitsemaan metodiseksi lähtökohdaksi kvalitatiivinen eli laadullinen tutkimusstrategia. Fingridin poikkeamanhallinnan nykytilan kartoittamisen ja kahteen suureen huoltovarmuuskriittiseen energia-alan yritykseen kohdistuvan vertailun mahdollistava empiirinen luku toteutettiin haastattelemalla ja perehtymällä aihealueeseen liittyvään kirjallisuuteen sekä Fingridin toimittamiin sisäisiin materiaaleihin. Tässä luvussa läpikäydään valitun tutkimusmetodin teoriapohjaa, kuvataan haastatteluiden suunnittelua ja toteutusta käytännössä, sekä millä perusteilla tuloksia analysoitiin kehitysideoita varten.

4.1 Tutkimusstrategia

Jokaisella tutkimuksella on jokin tavoite. Päästäkseen tähän tavoitteeseen, tutkimuksessa sen toteutusta ohjaa periaate – mitkä ovat ne keinot joilla tavoite on mahdollista toteuttaa järkevästi. Tätä tutkimuksen menetelmällisten ratkaisujen kokonaisuutta kutsutaan myös tutkimusstrategiaksi. (Hirsjärvi, Remes & Sajavaara 2009, 132.) Strategia voidaan eriyttää ensisijaisesti teoreettiseen tutkimukseen, jossa kohteen hahmottaminen perustuu pääosin aiempaan tutkimuskirjallisuuteen sekä empiiriseen tutkimukseen, jossa tutkimustulokset saadaan kohteesta tehtyjen konkreettisten havaintojen avustuksella. Perinteisesti strategia voidaan vielä jakaa kokeelliseen eli eksperimentaaliseen, tilastolliseen eli kvantitatiiviseen sekä laadulliseen eli kvalitatiiviseen tutkimuksen toteutukseen. (Hirsjärvi ym. 2009, 135.)

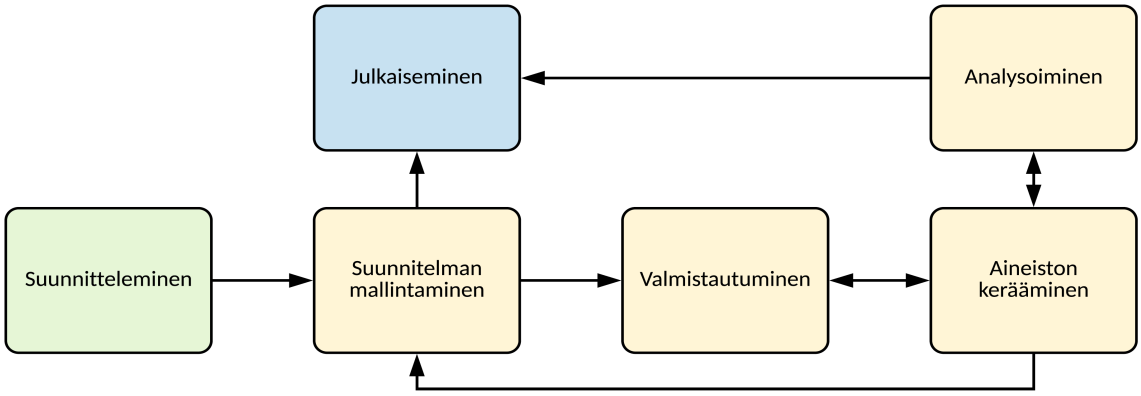
Kokeellisen tutkimuksen tarkoituksena on saavuttaa hypoteeseja kokeilemalla luotettavia tuloksia. Tilastollisen tutkimuksen materiaali kerätään kyselyiden ja haastatteluiden avulla satunnaisotannalla seulotusta ihmisjoukosta. Laadullisessa tutkimuksessa pääpaino pysyy todellisen elämän kuvaamisessa sekä siten kohteen kokonaisvaltaisessa ymmärtämisessä, tutkimusaineiston pysytellessä verrattain vähäisenä. (Hirsjärvi ym. 2009, 136.) Koottaessa materiaalia laadullista tutkimusta varten, on huomionarvoista ymmärtää ihmisen rooli ja tutkittavien näkökantojen esiintulon mahdollistavat menetelmät – näitä ovat esimerkiksi ryhmä- ja teemahaastattelut, havainnointi, dokumenteista johdetut analyysit sekä kyselyt. Tilastollisesta tutkimuksesta poiketen, laadullisessa tutkimuksessa jokainen tapaus näkyy ainutlaatuisena, kohteiden valikoituessa asianmukaisesti. Tutkimus elää jatkuvasti, jolloin myös sitä ohjaavien kysymysten muodot saattavat vaihtua. (Hirsjärvi ym. 2009, 132-133.)

Laadullisessa tutkimuksessa tutkimusaineistoa analysoidaan tyypillisesti induktiivisesti eli aineistolähtöisesti, tällä tavoin voidaan esiintuoda pelkän teorian testaamisen sijaan myös tuoreita näkökulmia aineiston yksityiskohtaisessa tarkastelussa (Hirsjärvi ym. 2009, 134). Tämä tutkimus on toteutettu empiirisenä ja laadullisena tapaustutkimuksena, jossa kaikki aineisto on koottu teemahaastatteluiden, kirjallisuuskatsauksen ja sisäisten dokumenttien pohjalta. Lopuksi materiaalia on analysoitu induktiivisena sisällönanalyysina. Seuraavissa alaluvuissa tarkennetaan näiden määritelmien taustoja sekä selvitetään tutkimusprosessia.

4.2 Tapaustutkimus

Tapaustutkimus on empiirinen syvätutkimus, jossa tutkitaan sosiaalisia yksikköjä, antaen niistä hyvin organisoidun kuvan (Yin 2009, 14). Se ei kuitenkaan ole tutkimusmenetelmä, vaan voidaan nähdä monipuolisena ja taipuvana lähestymistapana, tutkimusotteena, jossa empiria ja teoria ovat jatkuvassa vuorovaikutuksessa keskenään. Siinä painottuu rajatussa toimintaympäristössä keskittyminen yksittäisen tapauksen tai pienen, toisiinsa sidoksissa olevan ryhmän tarkasteluun, jossa prosessit ovat usein syvällisen kiinnostuksen kohteena. Tutkimusprosessin tulee olla läpinäkyvää ja kattavasti perusteltua, jotta sen luotettavuutta pystytään arvioimaan kriittisesti ja rakentavasti. (Eskola & Saarela-Kinnunen 2015, 181.) Tapaustutkimuksessa on ominaista tutkimusaineiston kerääminen luonnollisen tilanteen yhteydessä niin kyselyiden, haastatteluiden, havainnoinnin kuin dokumenttien tutkimisen avulla, mahdollistaen näin sekä laadullisen että tilastollisen tiedonkeruun. Merkittävää on tapauksen kokonaisvaltainen esitys omassa ympäristössä. (Järvinen & Järvinen 2011, 74.)

Hartley (2004, 332) luonnehtii tapaustutkimusta vaativaksi prosessiksi, jossa tutkimuksen tekijän täytyy kyetä muodostamaan ymmärrettävä yhteys sekä teorian ja aineiston keruun että analysoinnin ja teorian ympärille. Tapaustutkimus soveltuukin tutkimusotteeksi, kun tarkoituksena on hahmottaa tutkijan kontrolloimattomissa olevia nykypäivän tapahtumia vastaamalla tutkimuskysymysten ”mitä” tai ”kuinka paljon” sijasta kysymyksiin ”kuinka” tai ”miksi” (Yin 2009, 2). Tämän johdosta Yin (2009, 3) tähdentää tutkimuskysymyksiin sekä teoriaan panostamisen merkitystä tapaustutkimuksen mallissaan (kuvio 7) ennen itse tutkimusprosessin aloittamista. Mallissa tutkimus etenee lineaarisesti mutta iteratiivisesti, jatkaen tutkimussuunnitelman ja siinä selvitetyn tutkimuksen tarpeellisuuden sekä valitun analysointitavan esittelyn jälkeen kohti tutkimukseen valmistautumista (Yin 2009, 24-25).



Kuvio 7. Tapaustutkimuksen etenemisprosessi (lähde mukaillen Yin 2009, 1)

Valmistautumisen vaiheessa Yin (2009, 66-67) korostaa onnistuneen tapaustutkimuksen läpivientiin tarvittavien taitojen kehittämistä sekä käsiteltävän aihealueen kokonaiskuvan ymmärtämistä, johtaen huolelliseen valmistautumiseen ennen tutkimusaineiston keruuta. Aineiston keräämisessä ja sen analysoinnissa tulee ottaa huomioon monet eri tietolähteet sekä pohtia niiden käyttämistä rinnakkain – tällä poikkeavien aineistojen käytöllä samassa tutkimuksessa, eli triangulaatiolla voidaan kasvattaa tutkijan tietämystä, ja siten saavuttaa luotettavampi lopputulos tutkimukselle (Eriksson & Koistinen 2005, 30; Yin 2009, 127). Yinin (2009, 166) mukaan julkaisu on kenties koko prosessin vaativin vaihe – siinä ei riitä tulosten esittäminen, vaan tutkijan tulee julkaisutapaa valitessaan huomioida myös lukija.

Tässä tutkimuksessa kartoitetaan poikkeamanhallinnan prosessien nykytilaa ja pohditaan siihen käytännönläheisiä parannusehdotuksia kirjallisuuskatsaukseen, dokumentteihin ja teemahaastatteluihin pohjautuen, tutkimuksen painopisteen pysyessä nykyisessä hetkessä ja siten todellisessa elämässä. Haastatteluiden ja sisäisten dokumenttien pohjalta kerättyjä empiirisiä tutkimustuloksia päätettiin analysoida vertaamalla niitä kirjallisuuskatsauksessa esiteltyyn tietoon sekä toisaalta ennalta asetettuihin tutkimuskysymyksiin ja -tavoitteisiin. Näillä perusteilla laadullinen tapaustutkimus osoittautui luonnolliseksi tutkimusotteeksi.

4.3 Haastatteluiden toteutus

Laadullisessa tutkimuksessa haastattelulla on päärooli tutkimusmateriaalin keräämisessä, sen ensisijaisen tavoitteen ollessa asettaa haastattelija eli tutkimuksen tekijä haastateltavan asemaan – siis elävöittämään tutkimuksen aihealuetta vastapuolen näkökulmasta käsin ja saavuttamaan ymmärrys, kuinka tähän näkökulmaan lopulta päädyttiin (King 2004, 11).

Haastattelu voidaankin tyypillisesti nähdä tiedonhankintamenetelmänä, kun tutkimuksen kohteesta ei ole tarvittavissa määrin ennakkotietoa, tai etsittäessä perusteellisempaa tietoa ja mahdollisia perusteluja haastateltavilta. Toisaalta on hyvä tiedostaa haastattelun olevan aina aikaa vievä prosessi, joka voi tuottaa tutkimuksen kannalta usein myös turhaa tietoa. (Hirsjärvi & Hurme 2005, 35.) Haastattelut voidaan jakaa karkeasti kolmeen eri luokkaan: strukturoituun, strukturoimattomaan ja puolistrukturoituun. Strukturoidun haastattelun kysymykset ovat ennalta rajattuja, haastattelutilanteiden noudattaessa johdonmukaista ja selkeää kyselytapaa haastateltavasta kohteesta riippumatta. Sen toimintatapaa voidaan siis verrata lomakekyselyyn, jossa kysymysten vastausvaihtoehdot ovat tarkoin määritettyjä. Strukturoimattomassa haastattelussa syvennytään avoimeen keskusteluun, jossa tilanteen ja kysymysten annetaan kehittyä haastateltavan johdolla. (Wildemuth & Zhang 2009, 1.)

Puolistrukturoitu haastattelu – yleisemmin teemahaastattelu – sijoittuu edellä mainittujen muotojen välimaastoon, mutta muistuttaa rakenteeltaan enemmän strukturoimatonta eli avointa haastattelua. Teemahaastattelu on selvästi strukturoitua vapaamuotoisempi, eikä siinä määritellä haastattelukysymysten muotoa tai järjestystä yhtä kurinalaisesti. Aihepiirit eli teemat ovat kuitenkin kaikille samat ja toistuvat siten haastattelusta toiseen. Ominaista teemahaastattelulle on haastattelijan pyrkimys omaksua itsenäisesti tutkittava aihealue, ja tämän pohjalta luoda osaamiseensa perustuen teemapohjaisesti jaetun haastattelurungon. Haastateltavia yhdistävät yhteinen kokemustausta ja haastattelussa tutkimuksen kohteina oleville asioille annettujen merkitysten syntyminen yhdessä. Teemahaastattelussa voidaan siis sanoa korostuvan pohjimmiltaan yksilön kokemus. (Hirsjärvi & Hurme 2015, 47-48.)

Tässä tutkimuksessa empiirisen tutkimusosan kirjallisuuskatsaukseen, dokumentteihin ja haastatteluihin pohjautuva tietoperusta on tutkimuksen aihealue huomioiden varsin laaja, ja ennalta asetetut tutkimuskysymykset selkeitä, eikä avoin haastattelutapa siten soveltuisi tutkimuksen pääasialliseksi tiedonkeruumenetelmäksi. Wildemuth ja Zhangin (2009, 29) mukaan strukturoitu haastattelutapa asettaisi haastattelulle kohtuuttoman jyrkät raamit ja näin rajoittaisi saatuja tutkimustuloksia. Edellä mainitut haasteet tiedostaen, tutkimuksen haastattelut päädyttiin lopulta järjestämään laadullisina teemahaastatteluina. Laaja-alaisen kokonaiskuvan saamiseksi haastattelut hajautettiin sekä päällikkö- että asiantuntijatasolle; näin pyrittiin välttymään tunnelinomaiselta ajattelutavalta, jossa suorittavan henkilöstön kuulemisen sijaan johdon näkemyksiä arvostettaisiin liikaa (Myers & Newman 2007, 17).

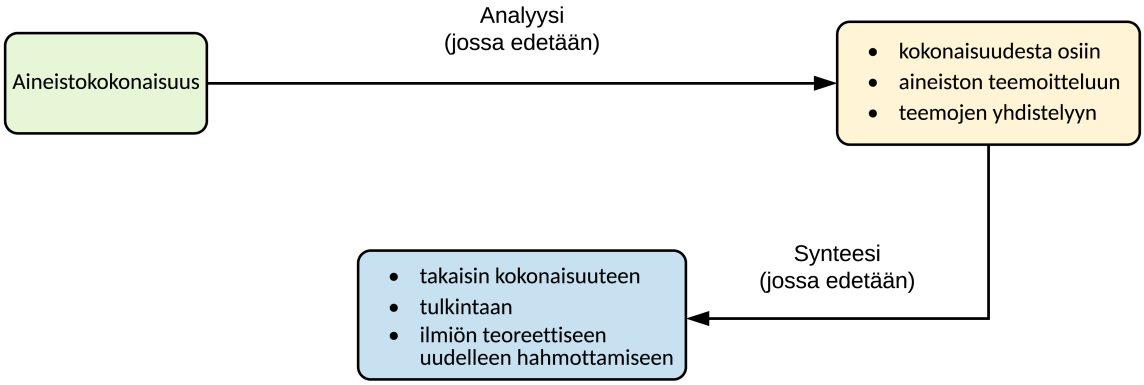
Tutkimuksessa haastateltaviksi valikoituivat sisäisellä tasolla Fingridin tietoturvapäällikkö ja kaksi tietoturvayksikön asiantuntijaa sekä vertailuaineiston muodostamiseksi ulkoisella tasolla kahden huoltovarmuuskriittisen energia-alan yrityksen tietoturvapäälliköt – kaikki siis päivittäisessä kosketuksessa yritystensä tietoturvallisuuteen ja poikkeamanhallintaan. Teemahaastatteluja varten luotiin yhteinen haastattelurunko (liite 1), jonka teema-alueiksi asetettiin johdanto; suunnittelu ja varautuminen; tunnistaminen ja raportointi; torjunta ja palautuminen sekä virheistä oppiminen. Teemojen suunnittelussa hyödynnettiin eritoten ISO/IEC 27035 -standardin sekä NIST ja SANS Instituten toimintamallien suosituksia. Suunnittelussa on huomioitava, että asetettuihin tutkimuskysymyksiin saadaan johdettua riittävät vastaukset, ja ettei haastattelurunko ole johdonmukainen kysymyslista, vaan siinä jätetään tilaa improvisaatiolle vapaamuotoisessa dialogissa (Hirsjärvi & Hurme 2005, 66).

Kaikki haastattelut toteutettiin kasvotusten haastateltavien toimipaikoilla ja siten omassa ympäristössään. Kukin haastattelu järjestettiin yhden työpäivän aikana, mutta sisäisten ja ulkoisten haastatteluiden välillä pidettiin noin kuukauden tauko – näin siis ensimmäisestä haastattelusta kirjattuja ongelmakohtia pystyttiin vielä parantamaan. Vertailuun valittujen ulkopuolisten yritysten kanssa päädyttiin allekirjoittamaan salassapitosopimukset (liite 2), haastateltavien ollessa toisilleen entuudestaan tuntemattomia. Tällä tahdottiin poissulkea tilanne, joka voisi pahimmassa tapauksessa johtaa luottamuksellisen ja salassa pidettävän, tutkimuksen lopputuloksen kannalta kriittisen vertailumateriaalin saannin kariutumiseen luottamuspulan takia (Myers & Newman 2007, 4). Haastattelut nauhoitettiin analysointia varten ja osapuolille toimitettiin haastatteluiden yhteenvedot mahdollisia lisäyksiä varten.

4.4 Tulosten analysointi

Sisällönanalyysi on laadullisen tutkimuksen perusmenetelmä, jonka tehtävänä on tiivistää tutkimusaineisto järkevään, johdonmukaiseen muotoon, ja siten sen informaalisen arvon kasvattaminen mahdollisimman luotettavien johtopäätösten tekemistä varten, oleellisten tietojen pysyessä ennallaan (Sarajärvi & Tuomi 2009, 103-105). Tämä edellyttää kuitenkin ensin aineiston saattamista luettavaan muotoon – haastatteluin kerätty aineisto pystytään purkamaan tekstimuotoon litteroimalla eli puhtaaksikirjoittamalla, tai suoraan aineistosta päätelmiä tekemällä, esimerkiksi jakamalla aineiston teema-alueisiin. Litterointi soveltuu parhaiten käytettäväksi, kun haastateltavia on muutamia. (Hirsjärvi & Hurme 2015, 138.)

Laadullisessa tutkimuksessa aineistoa voidaan analysoida selittämiseen ja ymmärtämiseen tähtäävillä lähestymistavoilla – näistä ensimmäisessä johtopäätökset saadaan tilastollisten analyysien pohjalta, kun taas jälkimmäisessä päätelmät perustuvat laadulliseen analyysiin. Laadullisia analyysimenetelmiä on useita, joista kenties yleisin on teemoittelu. Se voidaan nähdä parhaimmillaan vuoropuheluna kirjallisuuden ja tutkimusaineiston välillä; aineisto ryhmitetään teemoittain verraten sitä aiemmin esiteltyyn teoriaan, tarkoituksena loogisen kokonaiskuvan muodostaminen sekä oleellisen aineiston esiintuominen. Teemoittelussa on siis selvät etunsa pyrittäessä ratkaisemaan käytännön ongelmia. (Hiltunen 2009, 3-4.)



Kuvio 8. Aineistolähtöinen analyysi (lähde mukaillen Hirsjärvi & Hurme 2015, 144)

Laadullisessa sisällönanalyysissä voidaan noudattaa niin induktiivista eli aineistolähtöistä, deduktiivista eli teorialähtöistä kuin abduktiivista eli teoriaohjaavaa päättelytapaa. Näistä aineistolähtöinen sisällönanalyysi (kuvio 8) on kolmivaiheinen prosessi – siinä aineistosta redusoidaan eli tiivistetään osia, jonka jälkeen aineisto klusteroidaan eli sisällöstä haetaan samankaltaisuuksia tai eroavaisuuksia ennen niiden ryhmittämistä teemoittain. Analyysin päätteeksi aineisto vielä abstrahoidaan eli siitä erotetaan lopputuloksen kannalta oleelliset tiedot, muodostaen siten tutkimuksen teoreettisen käsitteistön. Synteesi sen sijaan tähtää kokonaiskuvan luomiseen sekä uusien näkökulmien esittelemiseen. (Hiltunen 2009, 6-7.)

Tämän tutkimuksen haastattelut litteroitiin haastatteluja seuraavina päivinä, varmistaen kerätyn aineiston johdonmukaisen tulkinnan. Litteroinnit toteutettiin perusmuodossaan, jotta sisältöä pystyttäisiin mahdollisesti hyödyntämään myöhemmin. Tutkimusongelmiin pureuduttiin ymmärtävän lähestymistavan mukaisesti. Koostettu aineisto teemoiteltiin ja analysoitiin aineistolähtöisenä sisällönanalyysina ongelmien käytännönläheisyyden takia.

5 Tutkimustulokset

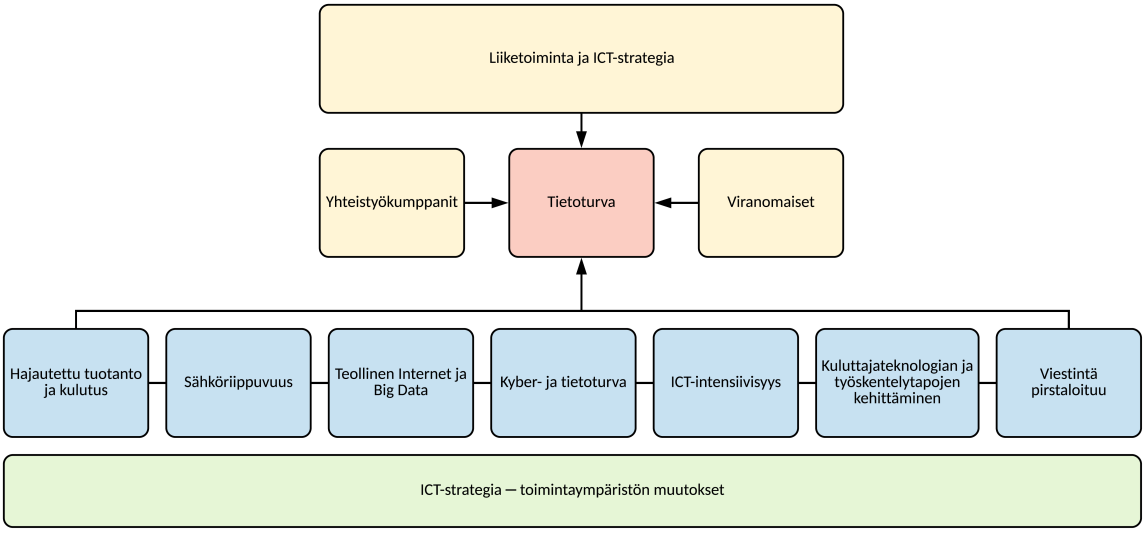
Tässä luvussa kuvataan Fingridin poikkeamanhallinnan nykytila, peilaten saatuja tuloksia kirjallisuuskatsauksessa esitettyihin suosituksiin. Luvussa kuvataan lisäksi vertailutulokset kahden kotimaisen huoltovarmuuskriittisen energia-alan yrityksen poikkeamanhallinnan tasojen suhteen. Fingridin nykytilan kuvaaminen pohjautuu tietoturvapäällikön ja kahden tietoturvayksikön asiantuntijan haastatteluihin sekä sisäisesti jaettuihin dokumentteihin. Vertailuyritysten poikkeamanhallinnan selvittämisessä haastateltiin tietoturvapäälliköitä.

5.1 Nykytila ja tavoite

5.1.1 Suunnittelu ja valmistautuminen

Fingridillä on merkittävä yhteiskunnallinen rooli, jossa tietoturvan ydintehtävänä on taata Suomen kantaverkon käyttövarmuus tilanteesta riippumatta. Fingrid on ottanut käyttöön sekä yhteisen ICT-strategian että tietoturvapolitiikan, jotka molemmat nauttivat ylimmän johdon luottamusta, ja joiden jatkuvaan kehittämiseen johto on sitoutunut. ICT-strategia ja tietoturvapolitiikka noudattavat Fingridin strategisia linjauksia, jotka painottavat oman henkilöstön riittävää ammattitaitoa tehokkaan ja ketterän toiminnan mahdollistamiseksi. Lähtökohtana käyttövarmuuden varmistamiselle on kriittisten palveluiden toteuttaminen yrityksen sisäisesti. ICT-strategiassa tiedostetaan tietoturvauhkien kasvu tulevaisuudessa sekä ennakoivan lähestymistavan painoarvo toiminnan jatkumisen ja toiminnan kannalta kriittisten järjestelmien turvaamiseksi kohdennetuilta hyökkäyksiltä. (Fingrid 2015c, 4-6.)

Fingridin itsenäinen tietoturvapolitiikka määrittää tietoturvalle päämäärät eli tavoitteet ja vastuualueet, korostaen sen tietojärjestelmien ja -verkkojen toiminnan sujuvuutta, tiedon luotettavuuden ja eheyden säilyttämistä, poikkeustilanteiden hallintaa sekä jo syntyneiden vahinkojen minimoimista. Politiikka näkee merkittävänä henkilöstön roolin tietoturvasta huolehtimisessa, unohtamatta kuitenkaan ulkoisia yhteistyökumppaneita ja viranomaisia, joiden kanssa toimiessa noudatetaan aina Fingridin sisäisiä arvoja. Kaikki toiminta tähtää siis liiketoiminnan turvaamiseen. Tietoturvapolitiikka on koko henkilöstön esteettömästi saatavilla – vuosittaisen sisällön ajankohtaisuuden tarkistamisen ja siten tarvittaessa myös päivittämisen kuuluessa ICT-johtajan vastuulle. (Fingrid 2015d, 2-6.) Tietoturvan suhteet Fingridin toimintaympäristön sidosryhmien välillä on kuvattu syvällisemmin kuviossa 9.



Kuvio 9. Fingridin tietoturvan toimintamalli (lähde mukaillen Fingrid 2015d, 4)

Tutkimuksen kirjallisuuskatsauksessa todettiin ISO/IEC 27035 -standardin sekä ITIL ja SANS Instituten toimintamallien painottavan tietoturvapolitiikan välttämätöntä tehtävää poikkeamanhallinnan ohjenuorana sekä henkilöstön rajoittamatonta pääsyä tutustumaan sen sisältöön ajankohdasta riippumatta. Politiikan tulee nauttia yritysjohdon luottamusta, edellyttäen siten sisällön ajankohtaisuuden tarkistamista ja tarvittaessa myös päivittämistä vähintään vuosittaisella tasolla tarkasteltuna. Fingridin tietoturvapolitiikka on sisällöltään näiden suositusten mukainen, sijaiten intranetistä erotetussa Wikissä, jonne kaikki sisäiset politiikat ja ohjeistukset on keskitetty. Politiikan sijainti on hieman syrjäinen, vaikeuttaen siten päivitetyn version näkyvyyttä henkilöstölle, mutta toisaalta säännöllinen tietoturvan verkkokoulutus lievittää sen vaikutusta organisatorisella tasolla. (Haastattelu 21.12.2015.)

ISO/IEC 27035 -standardi ja SANS Institute näkevät tietoturvapolitiikan lisäksi tärkeänä yritysjohdon tunnustaman, formaalin ja selkeästi dokumentoidun tietoturvatapahtumien, -poikkeamien ja -haavoittuvuuksien hallintapolitiikan luontia osana tietoturvapolitiikkaa. Puutteellisilla tai epäselvillä politiikoilla voidaan mahdollistaa oikeudellisten velvoitteiden syntyminen – siksipä poikkeamanhallintaan suositellaan järjestelmällistä lähestymistapaa, esimerkiksi hallintamallin välityksellä. Fingrid ei käytä hallintapolitiikkaa tai -mallia, mutta yrityksessä on kyllä ajateltu poikkeamiin keskittyvän politiikan luontia. Fingrid ei noudata toiminnassaan standardeja, toimintamalleja tai sertifiointeja, vaan katsoo hyödyntävänsä niiden parhaita puolia, joihin ei voida heikon hyöty-panos-suhteen tai resurssipulan takia sitoutua, painottaen käytännöllistä ja joustavaa lähestymistapaa. (Haastattelu 21.12.2015.)

Wikissä on kaksi eri ohjetta oletettavia häiriötilanteita varten: ohje korjaustoimenpiteiden käynnistämiseksi, jossa kuvataan tarvittavien toimenpiteiden eteneminen ja oleellisimmat yhteystiedot, sekä lisäksi ohje vakaviin ICT-häiriöihin varautumista varten, joka määrittää tarvittavat vastuut ja tehtävät – tämä ohje käsittelee vakavissa häiriötilanteissa vaadittavia toimenpiteitä, keskittyen liiketoiminnan kannalta kriittisiin tietojärjestelmiin, laitetiloihin, tietoliikenteeseen sekä tietoturvaloukkauksiin ja -uhkiin. Poikkeamien käsittelyä varten ei ole luotu erillistä ohjetta, eikä vakaviin ICT-häiriöihin varautumisen ohjetta päivitetä tällä hetkellä kovinkaan aktiivisesti, vihjaten siten osaltaan sen näkemistä tärkeysjärjestyksessä vähäisenä. (Fingrid 2015, 3-6.) Tietoturvapäällikkö tiedostaakin ohjeen sisällön nykytilan olevan riittämätön yhdessä asetettuihin tavoitetasoihin nähden (Haastattelu 21.12.2015).

ISO/IEC 27035 -standardi ja useat toimintamallit näkevät erillisen poikkeamanhallinnan vasteryhmän muodostamisen oleellisena osana hallinnan yhdensuuntaistamista sekä siten tehostavan sen poikkeamien luotettavaa ja kustannustehokasta käsittelyä. SANS Institute muistuttaa yrityksen sisäisten yksiköiden välisen yhteistoiminnan tärkeydestä, ehdottaen esimerkiksi henkilöstö-, laki- ja viestintäyksiköiden asiantuntijoiden mukanaoloa ryhmän toiminnassa tilanteen vaatiessa – tällä tavoin saavutetaan mahdollisimman monipuolinen ja ketterä varautuminen jatkuvasti kehittyviin poikkeamatilanteisiin. Fingridillä on sovittu aiemmin mainitun vakaviin ICT-häiriöihin varautumisen ohjeen kattavan sekä tilanteiden johtamiseen että tiedottamiseen liittyvät asiat, eikä käytössä ole erillistä vasteryhmää – on tietoturvayksikön vastuulla arvioida tilanteita tapauskohtaisesti (Haastattelu 21.12.2015).

Tietoturvayksikkö ei kuitenkaan kykene toteuttamaan onnistunutta poikkeamanhallintaa ilman asiantuntevaa ja motivoitunutta henkilöstöä. ISO/IEC 27035 -standardi ja SANS Institute pitävät ensisijaisena säännöllistä, tunnistamisen ja raportoinnin roolin tärkeyden tietoisuutta kasvattavaa koulutusta, alleviivaten samalla erillisen koulutuksen järjestämistä poikkeamien käsittelijöille. Fingridissä on käytössä säännöllinen verkkokoulutusohjelma, jossa tietoturvallisuus on huomioitu irrallisena osa-alueena. Koulutuksessa ei kuitenkaan huomioida henkilöstön roolia poikkeamanhallinnassa, eikä tietojärjestelmävarallaolijoita ole perehdytetty poikkeamien analysointiin. Koulutuksen sisältö päivitetään vuositasolla, edellyttäen siten koko henkilöstöltä koulutuksen ja ymmärtämistä testaavan loppukokeen läpäisemistä. Verkkokoulutus on ollut menestyksekäs – tästä on osoituksena henkilöstön oma aktiivisuus poikkeamien tunnistamisessa ja raportoinnissa. (Haastattelu 21.12.2015.)

5.1.2 Tunnistaminen ja luokittelu

Fingridissä henkilöstö koetaan poikkeamien tunnistamisessa ja raportoinnissa keskeisenä tiedonlähteenä, ITIL:n viitekehystä toiminnassaan pitkälti noudattavan lähituen saadessa useasti tiedon häiriötilasta. Selkeä enemmistö poikkeamista havaitaan tietoturvapäällikön mukaan kuitenkin tietojärjestelmien ja laitteistojen automaattisten hälytysten kautta, joita pyritään kehittämään niin, että ne lähettäisivät hälytysilmoituksen aina ennalta määritetyn uhan vakavuuden mukaisesti. Näin entuudestaan tunnettujen uhkatilanteiden varhaiseen havainnointiin voidaan vaikuttaa. Hälytysilmoitus vastaanotetaan Fingridissä esimerkiksi käyttöönotetuista tunkeilijoiden havaitsemisjärjestelmästä, SIEM-järjestelmästä (Security Information and Event Management), virustentorjunnasta ja palomuureista, mutta myös tietoliikennelaitteista – kuten kytkimistä ja reitittimistä – joiden ohjelmoimisella pystytään tarvittaessa säännöstelemään tai jopa estämään tietoliikennettä. (Haastattelu 21.12.2015.)

Yhdeksi keskeiseksi tiedonlähteeksi voidaan luokitella myös Fingridin läheinen yhteistyö Viestintäviraston alaisen Kyberturvallisuuskeskuksen kanssa, jonka HAVARO-palvelun huoltovarmuuskriittisten yritysten jäsenverkostoon Fingrid lukeutuu. Palvelulla viitataan tietoturvaloukkausten havainnointi- ja varoitusjärjestelmään, jossa pyritään havaitsemaan yrityksen toimintaa uhkaavat poikkeustilanteet ennen niiden kehittymistä vakavammiksi. Palvelulla pyritään siten suojelemaan yrityksen jatkuvuuden hallintaa ja helpottamaan sen riskien kartoittamista. Tietoturvapäällikkö näkeekin palvelun tarjoavan uusia näkökulmia ja mukana tulevan tapahtumien analysoinnin täydentävän tämänhetkisiä tietojärjestelmiä, vastaten siten ISO/IEC 27035 -standardin yhteisiä suosituksia. (Haastattelu 21.12.2015.)

Luokittelu- ja kategorisointiasteikoilla on keskeinen tehtävä määriteltäessä häiriötilanteen vakavuutta. Esimerkiksi ITIL suosittelee ratkaisuksi asteikkoa, jossa poikkeama voitaisiin luokitella sen liiketoiminnalle aiheuttaman välittömän uhkan perusteella kolmelle tasolle: vähäisen, keskitason tai korkeimman tason uhkaksi, määrittäen samalla tilanteen vaatimat resurssit ja reagoimisen nopeuden. Fingridillä ei ole käytössä varsinaisia asteikkoja, mutta tärkeimmistä tietojärjestelmistä on olemassa oma dokumenttinsa, jota voisi jatkokehittää. Vakavuuden arviointi toteutuu pitkälti tietoturvayksikön kokemukseen pohjautuen – sen koulutetut asiantuntijat ymmärtävät liiketoiminnan vaatimukset, minkä johdosta arviointi sekä luokittelu pystytään järjestämään edellytetyllä tarkkuudella. (Haastattelu 21.12.2015.)

5.1.3 Vastatoimet, palautuminen ja opetukset

Poikkeamien nitistämiseen suuntaavissa vastatoimenpiteissä tähdätään ainoastaan yhteen tavoitteeseen – palauttamaan Fingridin liiketoimintaan sidoksissa olevat kriittiset palvelut ja prosessit niiden alkuperäiselle tasolle sekä siten estämään tilanteen uusiminen ottamalla havaituista virheistä opiksi (Fingrid 2015e, 3). Sekä ISO/IEC 27035 -standardi että NIST ja SANS Instituten toimintamallit alleviivaavat lisäksi poikkeamanhallinnan vasteryhmän varhaisen tilanteeseen väliintulon vaikutusta – esimerkiksi vaarantuneen tietojärjestelmän eristämisellä estetään lisävahinkojen muodostuminen sekä saadaan lisäaikaa tehokkaan ja korkealaatuisen jatkosuunnitelman työstämiseen. Lokitietojen säännöllisellä keräämisellä tai työvaiheiden dokumentoimisella pystytään paitsi nopeuttamaan poikkeamatilanteiden turvallista ja johdonmukaista ratkaisemista myös arvioimaan ratkaisemisen suorituskykyä sekä siten mahdollistamaan todistusaineistojen hyväksikäytön oletetuissa rikostilanteissa.

Fingridillä ei ole käytössään erillistä poikkeamanhallinnan vasteryhmää – siten epäiltäessä tietoturvaloukkausta, ilmoituksen häiriötilasta vastaanottaa tietoturvayksikkö ensisijaisen kontaktipisteen roolissaan, arvioiden samalla mahdollisen poikkeaman vakavuuden tasoa yrityksen liiketoiminnan kannalta. Tietoturvayksikkö informoi tietoturvapäällikköä, joka organisoi häiriötilan edellyttämät it-asiantuntijat koolle sekä välittää vetovastuun ottavalle ICT-johtajalle tiedon tapahtuneesta. ICT-johtaja ja tietoturvapäällikkö päättävät yhdessä jatkotoimenpiteistä – uhkaako tilanne kantaverkkokeskuksen toimintaa ja nähdäänkö sen tietojärjestelmien eristäminen tarpeelliseksi sekä tiedotetaanko yritysturvallisuusyksikköä tai viranomaisia, kuten esimerkiksi Kyberturvallisuuskeskusta. (Haastattelu 21.12.2015.)

Tietojärjestelmävarallaolija toimii ensisijaisena kontaktipisteenä sekä työajan ulkopuolella että viikonloppuisin, varmistaen häiriön vakavuuden yhteistyössä kantaverkkokeskuksen päivystäjän kanssa. Varallaolija on tarvittaessa suoraan yhteydessä tietoturvapäällikköön, joka käynnistää ennalta määritetyt prosessien mukaiset toimenpiteet – nämä toimenpiteet pystytään tutkimaan lokitiedoista ja kaikki vakavat tapaukset dokumentoidaan – eheyden ylläpitämistä painotetaankin Fingridissä koko poikkeaman elinkaaren aikana. ICT-johtaja vastaa resurssien koordinoinnista ja valmiustilan nostamisesta it-yksiköiden päälliköiden toimiessa varahenkilöinä. Tarvittaessa lisävoimaa saadaan yhteistyökumppaneilta ripeällä aikataululla, noudattaen siten kirjallisuuskatsauksen suosituksia. (Haastattelu 21.12.2015.)

Häiriötilanteen lähteen onnistuneen eristämisen ja ratkaisemisen jälkeen, NIST ja SANS Instituten toimintamallit muistuttavat korruptoituneen tietojärjestelmän kehittämiseen ja testaamiseen panostamisen tärkeyttä ennen sen uudelleen käyttöönottoa. Tapahtuneesta on hyvä luoda kirjallinen yhteenveto käytäväksi ryhmässä läpi tilanteeseen osallistuneiden kanssa. Fingrid noudattaa näitä suosituksia – käytössä on Sandbox-turvatekniikkaa, jonka avulla pystytään selvittämään, kuinka tilanne olisi kehittynyt ilman varhaista puuttumista. Vakavista poikkeamatilanteista tehdään lyhyt yhteenveto, joka pyritään käymään yhdessä läpi sekä hyödyntämään vastaavien tilanteiden selvitystyössä ja koulutuksessa. Fingridissä ulospäin liikkuva tieto kulkeutuu viestintäyksikön kautta viestintä- ja kriisiviestintäohjeen mukaisesti – yhteiskuntakriittisen aseman johdosta avoimella ja ennakoivalla viestinnällä on keskeinen rooli. (Haastattelu 21.12.2015.) Fingridin poikkeamanhallinnan nykytilaa ja sen operatiivisten toimenpiteiden rakennetta on selostettu perusteellisemmin liitteessä 3.

5.2 Vertailun tulokset

Fingridin poikkeamanhallinnan nykytilan kriittisen arvioinnin ja vertailuaineiston saannin varmistamiseksi tutkimuksessa haastateltiin kahden kotimaisen huoltovarmuuskriittisen energia-alan yrityksen (jäljempänä yritykset A ja B) tietoturvapäälliköitä. Kumpikin yritys kantaa yhteiskunnallisesti merkittävän roolin energiahuoltovarmuuden varmistamisessa. Molemmat vertailuyritykset ovat ottaneet käyttöön sisäisen, tietoturvapäällikön vetämän tietoturvayksikön, jossa työskentelee kahdesta kolmeen täysipäiväistä asiantuntijaa, ollen suoraan vertailukelpoisia Fingridin tietoturvayksikön kanssa. Yrityksessä A on hiljakkoin otettu käyttöön koko henkilöstön vapaasti saatavilla oleva ja ylimmän johdon hyväksymä tietoturvapolitiikka, joka koetaankin selkeänä parannuksena lähtötilanteeseen verrattuna. Ajantasainen tietoturvapolitiikka ja kyberstrategia muodostavat tärkeän osan yrityksen B johtamisjärjestelmästä, sitouttaen siten yrityksen ylimmän johdon ja yksiköiden esimiehet niiden kuvaamien periaatteiden taakse. (Haastattelu 20.1.2016a; Haastattelu 20.1.2016b.)

Kaikkien yritysten tietoturvapäälliköt korostavat standardien ja toimintamallien tärkeyttä, pyrkien näin hyödyntämään niiden parhaimmat puolet, näkemättä kuitenkaan varsinaista tarvetta sertifioinneille niiden aikaa vievän byrokratian ja kustannusten takia. Yritys A on päätynyt ISO/IEC 27001 -standardiin tietoturvapolitiikan sekä siihen sidoksissa olevien ohjeiden eräänlaisena pohjarunkona. Tietoturvapäällikkö kokee sen soveltuvan parhaiten

liiketoimintamaailmaan Information Systems Audit and Control Associationin (ISACA) toimintamallin suosituksiin yhdistettynä. Yrityksessä B puolestaan pidetään Information Security Forumin (ISF) Standard of Good Practice -standardia sen tietoturvan globaalina lähteenä, ISO/IEC 27001-, 27005- ja 27035 -standardien vaikuttaessa taustalla. Yritysten tietoturvapäälliköt ovat yksimielisiä kuvaillessaan tietoturvaa liiketoimintaa hyödyttäväksi rooliksi, jonka asianmukainen taso kartoitetaan riskienhallinnalla. Poikkeamien luokittelu ja niiden elinkaaren säännöllinen dokumentointi muodostavat ensisijaisen osan oppivana yrityksenä toimimisesta – esimerkiksi poikkeaman elinkaaren aikana tehdyt toimenpiteet rekisteröidään yrityksessä A lähituen ylläpitämään tiketöintijärjestelmään ja vakavimmista poikkeamista tiedotetaan johtoryhmää. (Haastattelu 20.1.2016a; Haastattelu 20.1.2016b.)

Yritys A on pohtinut erillisen poikkeamanhallinnan vasteryhmän perustamista, vaikkakin poikkeamatilanteessa kokoontuvia asiantuntijoita ei ole vielä ennalta määritetty. Nykyisin tietoturvayksikön henkilöstö toimii ensisijaisena kontaktipisteenä, todellisen selvitystyön voidessa päätyä tietohallinnolle häiriötilasta riippuen. Tietoturvapäällikön mukaan suurin osa havaituista poikkeamista tulevat eri järjestelmien kautta, joiden puutteellinen toiminta aiheuttaa nykymuodossaan turhia viivästyksiä häiriötiloihin reagoinnissa, hyödyllistenkin lokitietojen ollessa usein sisällöltään epäsäännöllisiä. Yrityksessä on parhaillaan käynnissä SIEM-järjestelmän ja SOC-palvelun (Security Operations Center) hankinta tehostamaan paitsi normaalia lokienhallintaa, myös poikkeamien käsittelyä sekä esimerkiksi kriittisessä poikkeamatilanteessa perusforensiikkaan liittyviä toimenpiteitä. (Haastattelu 20.1.2016a.)

Yritys B rekisteröi yritystasolla havaitsemansa poikkeamat prosessinhallinnan sisältävään NCR-järjestelmään (Non-Conformance Reporting), joka toimii lisäapuna sen tietoturvaa koskevissa selvityksissä. Poikkeamat luokitellaan ennen rekisteröintiä, siten taloudellisesti ja toiminnollisesti ensisijaisten kehitystarpeiden kulkeutuessa johtoryhmän tietoisuuteen. It-toiminnoilla on käytössä pilvipalveluna toteutettu toiminnanohjausjärjestelmä – kaikki toimintapoikkeamat rekisteröidään noudattaen ITIL:n palvelutuotannon elinkaarimallin tasojen luokittelua. Lähituki toimii loppukäyttäjien ensisijaisena kontaktipisteenä. Lisäksi yrityksellä on käytössä kriittisen poikkeamatilanteen varalle häiriötilanteiden vasteryhmä, joka ottaa tilanteessa vastuulleen viestinnän, koordinoinnin sekä tehtävänjaon, keskittäen päätöksenteon ja seuraukset samaan pisteeseen. Vasteryhmän ensisijainen ja ainut tavoite on liiketoimintakyvyn palauttaminen alkuperäiselle tasolle mahdollisimman kivuttomasti.

Yritys tallentaa toistuvasti infrastruktuurin lokitietoja SIEM-järjestelmään, keskittyen yhä useammin myös sovellusmaailmaan, varmistaen tällä tavoin laajojen tai yksityiskohtaisten tapahtumaketjujen selvittämisen. Voimavarat eivät kuitenkaan aina osoittaudu riittäviksi, jolloin yhteistyösopimusten pohjalta turvaudutaan kolmansien osapuolten toimittamaan lisäapuun esimerkiksi korkeimman tason forensiikassa tai auditoinneissa – näin osapuolet kantavat omalta osaltaan huomattavan vastuun raportoinnista. (Haastattelu 20.1.2016b.)

Molemmat tietoturvapäälliköt painottavat henkilöstön säännöllisen kouluttamisen roolia menestyksekkäässä poikkeamanhallinnassa. Yritys A on aiemmin testannut säännöllisesti järjestettyä ja päivitettyä tietoturvallisuuden koulutusohjelmaa, mutta tulokset eivät olleet vakuuttavia. Osa it-asiantuntijoista on harjoitellut mahdollisia hyökkäystiloja yhteistyössä Tampereen teknillisen yliopiston kanssa. Vaikka tietoturvallisuus on edelleen läsnä uuden työntekijän perehdytyksessä, tietoturvapäällikkö toteaa koulutuksen olevan nykytasollaan riittämätöntä ja parannustarve siten merkittävä. Yritys B on ottanut toimintaansa sisäisen HSEQ-organisaation (Health, Security, Environment and Quality), vastaten henkilöstön säännöllisestä koulutuksesta yritystasolla. Poikkeamatilanteiden hallinnan ja vasteryhmän työkalujen käytön säännölliseen harjoitteluun osallistuvat viestintäyksikön lisäksi ulkoiset palvelutoimittajat. Tietoturvapäällikkö näkee toimintatasoa mittaavilla harjoituksilla siten vain positiivisia vaikutuksia; mikäli kokonaisuutta ei hallita, häiriötilasta kehittyy nopeasti yritysbrändiä vahingoittava poikkeama. (Haastattelu 20.1.2016a; Haastattelu 20.1.2016b.)

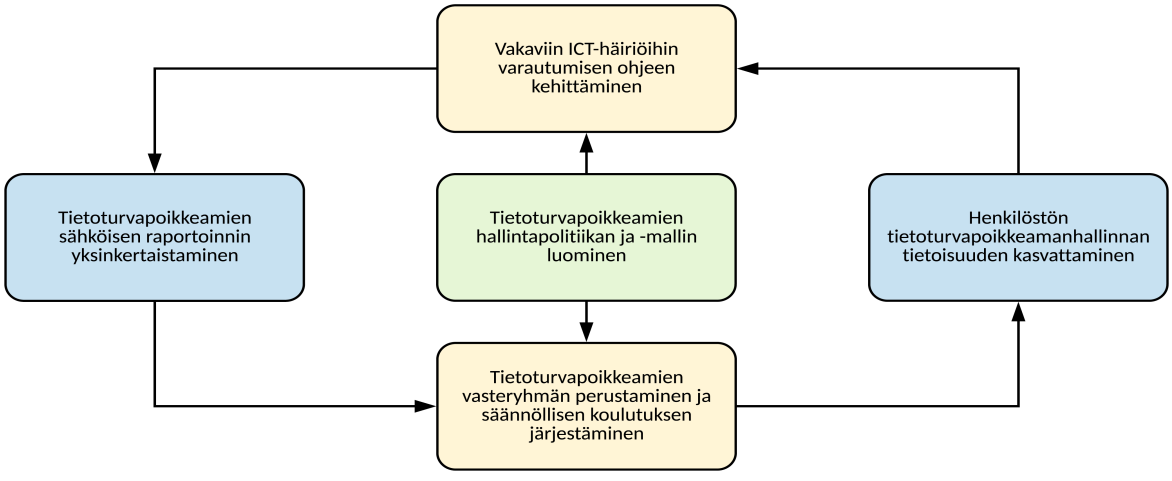
Tietoturvapäälliköt olivat yksimielisiä kysyttäessä heitä pahiten uhkaavasta häiriötilasta – prosessiautomaatioon kohdistuva häiriö tuottaisi mittavat fyysiset ja taloudelliset tappiot. Yritykset ovat velvoitettuja jakamaan tietoa tietoturvaloukkauksista HAVARO-palvelun sääntöjen mukaisesti jäsenverkostoon kuuluville yrityksille, tarjoten näin etulyöntiaseman vastaaviin uhkiin varautumiselle sekä mahdollisuuden kehittää järjestelmien turvallisuutta luottamuksellisen yhteistyön puitteissa. (Haastattelu 20.1.2016a; Haastattelu 20.1.2016b.) Tehokkaassa poikkeamanhallinnassa kulminoituvat järjestelmällinen lähestymistapa sekä muodolliset, yhdenmukaiset politiikat ja dokumentit, joissa Fingrid jää yrityksen A tavoin yrityksen B taakse. Fingridin vahvuuksiksi voidaan katsoa johtoryhmän keskeytymätöntä sitoutumista poikkeamanhallinnan harjoittamiseen, henkilöstön ammattitaitoa ja korkeaa koulutustasoa sekä viestintään ja säännölliseen perehdyttämiseen panostamista. Fingridin nykytaso kestää siten vertailua, erityisesti henkilöstömäärien ja resurssien erot tiedostaen.

6 Johtopäätökset ja pohdinta

Tässä luvussa esitetään yhteenveto keskeisistä tutkimustuloksista ja kehittämisehdotuksia poikkeamanhallinnan prosessien tehostamiseksi. Luvussa pohditaan lisäksi potentiaalisia jatkotutkimuksen aihealueita, joita voitaisiin toteuttaa parempien resurssien tai aikataulun puitteissa. Luku päättyy oman oppimisen arviointiin – kuinka tutkimuksessa onnistuttiin kokonaisuutena, jäikö jotain käsittelemättä sekä kuinka ammatillinen osaaminen kehittyi.

6.1 Keskeiset tulokset ja kehittämissuunnitelma

Fingrid on Suomen valtion enemmistöomisteinen kantaverkkoyhtiö, joka kantaa vastuun sähkön kantaverkon käyttövarmuuden takaamisesta, asettaen siten sen tietoturvalle laajat toimintaedellytykset. Yrityksessä on hiljattain rekisteröity ongelmia poikkeamanhallinnan päivittäisissä toimenpiteissä, luoden turhan pohjan tietoturvariskien syntymiselle. Fingrid toivookin parantavansa poikkeamanhallintansa tasoa aiempaa yhtenäisempään suuntaan. Tämän tutkimuksen ensisijaisena tavoitteena oli selvittää Fingridin poikkeamanhallinnan käsittelyprosessien nykytila sekä toissijaisena tavoitteena, kuinka näitä prosesseja voidaan tehostaa ja saada muodostettua yhtenäinen kokonaisuus. Tutkimuksessa selvitettiin myös kahden kotimaisen huoltovarmuuskriittisen energia-alan yrityksen poikkeamanhallinnan tasojen eroavaisuuksia Fingridin vastaavaan verrattuna. Nykytilan kartoituksessa paljastui selkeitä kehityskohteita aina kriittisistä politiikoista ja dokumenteista kouluttamiseen sekä poikkeamanhallinnan tehostamiseen. Tämän tutkimuksen aikana havaitut kehityskohteet on kuvattu kuviossa 10, jonka jälkeen valikoituja kehityskohteita perustellaan laajemmin.



Kuvio 10. Fingridin poikkeamanhallinnan havaitut kehityskohteet

Fingrid on ottanut käyttöönsä ylimmän johdon hyväksymän tietoturvapolitiikan, tarjoten tietoturvalle yleiset pelisäännöt, mutta siinä ei sinänsä oteta kantaa tietoturvapoikkeamien tunnistamiseen, raportointiin tai tiedonkeruuseen liittyviin toimenpiteisiin, eikä politiikka sisällä poikkeamanhallinnan avainhenkilöiden tai palvelutoimittajien yhteystietoja tulevia poikkeustilanteita varten. Hallintapolitiikka ja siihen sidoksissa oleva hallintamalli tukevat yritystä kohti järjestelmällisempää poikkeamanhallintaa – hallintamallia pidetäänkin usein eräänlaisena hierarkkisena oppaana menestykselliselle poikkeamatilanteen selvittämiselle.

ISO/IEC 27035 -standardin ehdottama hallintamalli tarjoaa erinomaisen perustan, jonka pohjalta voidaan suunnitella Fingridin liiketoiminnan tarpeisiin parhaiten soveltuva malli. Siihen on suotavaa yhdistellä muiden toimintamallien suosituksia, joista SANS Instituten toimintamalli suosittelee dokumentoinnin sekä sähköisten ja fyysisten todistusaineistojen kokoamisen aloittamista poikkeaman tunnistamisvaiheen yhteydessä, samalla varmistaen todistusaineistojen eheyden ja luottamuksellisuuden koko poikkeamatilanteen elinkaaren ajan – näin mahdollisesti muuttunut todistusaineisto ei pääse häiritsemään rikostutkintaa ja tehdyistä toimenpiteistä talletettujen lokitietojen avulla tilannetta pystytään tarvittaessa arvioimaan ryhmänä sekä siten oppimaan huomatuista virheistä. Fingridin kohdalla tämä olisi järkevintä toteuttaa liittämällä hallintapolitiikka jo entuudestaan henkilöstölle tutuksi tulleen tietoturvapolitiikan yhteyteen, jolloin politiikoiden säännöllisellä päivittämisellä ei kuormiteta turhaan resursseja, luoden siten helposti ymmärrettävän asiakokonaisuuden.

Fingridillä ei ole käytössä itsenäistä poikkeamanhallinnan vasteryhmää, tietoturvayksikön vastatessa kaikista poikkeamanhallinnan prosesseista. Tarve yhdenmukaiselle toiminnalle on kuitenkin selkeää ja vasteryhmän perustaminen siten aiheellista. NIST ehdottaakin eri henkilöstö- ja rakennemalleja perustamisprosessin tukemiseksi. Fingridissä ei ole tarvetta ympärivuorokautiselle vasteryhmälle tietojärjestelmävarallaolijan toimiessa jo parhaillaan ensisijaisena kontaktipisteenä työaikojen ulkopuolella. Tietoturvayksikön asiantuntijat on koulutettu poikkeamatilanteiden varalle, minkä johdosta niiden tulee toimia vasteryhmän pysyvänä perustuksena, muutoin noudatettaessa virtuaalista mallia, jossa it-asiantuntijoita kutsutaan paikalle vain tarvittaessa. Henkilöstö-, laki-, turvallisuus- ja viestintäyksiköiden asiantuntemusta tulisi hyödyntää osana vasteryhmän toimintoja – esimerkiksi epäiltäessä poikkeaman lähteen olevan sisäinen tai kun todistusaineistoa halutaan säilyttää valvotusti rikostutkintaan. Tuoreita näkökulmia voidaan hakea yksiköiden osaamista kierrättämällä.

Tietoturvapäällikön tulee ottaa vastuu vasteryhmän päivittäisestä toiminnasta sekä toimia suorana linkkinä Fingridin ylimpään johtoon ryhmän tarvitsemien työkalujen ja toistuvan kouluttamisen mahdollistavien resurssien takaamiseksi. Tietoturvayksikössä työskentelee kaksi täysipäiväistä asiantuntijaa – toisen tulisi toimia teknisen vastuuhenkilön roolissa ja toisen paneutua saapuneiden häiriöilmoitusten läpikäymiseen, roolien vaihtuessa tasaisin väliajoin. Tietojärjestelmävarallaolijat toimivat ensisijaisina kontaktipisteinä vasteryhmän työajan ulkopuolella, joten heidän kouluttaminen muun ryhmän rinnalla tulee huomioida erityisesti poikkeamien luokitteluun sekä kategorisointiin liittyvien toimenpiteiden osalta.

Poikkeaman vakavuuden tehokkaan luokittelun mahdollistamiseksi tunnistamisvaiheessa on keskeistä tiedostaa liiketoiminnan kannalta tärkeimmät tietojärjestelmät. Fingrid ei ole ottanut käyttöönsä poikkeamien kategorisointi- tai luokitteluasteikkoja tietoturvayksikön asiantuntijoiden arvioidessa tilanteet aina tapauskohtaisesti. Käytäntö on sinänsä toimiva, mutta formaali ja yhdenmukainen dokumentaatio keventäisi etenkin työajan ulkopuolella päivystävien tietojärjestelmävarallaolijoiden työtaakkaa – heillä ei ole vasteryhmän tapaan merkityksellistä tietotaitoa, eivätkä siten kykene arvioimaan jokaisen tilanteen vaikutuksia liiketoiminnan näkökulmasta. Fingrid on dokumentoinut kriittisimpiä tietojärjestelmiään vakaviin ICT-häiriöihin varautumisen ohjeessa, joka soveltuu hyväksi perustaksi asteikon luomiselle. ITIL:n kolmitasoinen luokitteluasteikko ja sen kiireellisyyttä kuvaava asteikko sopivat Fingridin käyttöön, sillä viitekehys ohjaa nykyisellään pitkälti lähituen toimintoja.

Aiemmin todettiin henkilöstöllä olevan suuri rooli poikkeamanhallinnassa. Fingridillä on säännöllisesti päivitettävä verkkokoulutusohjelma, jonka sisältöön myös tietoturvallisuus kuuluu erillisenä osa-alueena, ja jonka läpäisemistä edellytetään koko henkilöstöltä. Siinä ei ole kuitenkaan nykyisessä muodossa käsitelty poikkeamanhallintaa – kuinka henkilöstö on velvollinen raportoimaan havaituista poikkeamista ja kuinka se tapahtuu käytännössä. Kun koulutuspakettia päivitetään seuraavan kerran, siihen tulisi sisällyttää kattava katsaus päivittäisten poikkeamanhallinnan prosessien toimintaan erityisesti uusien työntekijöiden näkökulmasta tarkasteltuna. Nykyinen henkilöstö ymmärtää tietoturvan ja raportoimisen merkityksen liiketoiminnalle – tietomäärät ovat kuitenkin epäformaaleja, aiheuttaen siten turhaan lisätietojen pyytämistä. Toiminnanohjausjärjestelmään sulautettavien sähköisten raportointilomakkeiden avulla turhat viestit vähenevät ja häiriötilasta saadaan kattavampi käsitys, samalla parantaen anonymiteettiä ja luottamusta vasteryhmän toimintaa kohden.

Fingridin poikkeamanhallinnan nykytilan kriittisen arvioinnin ja vertailuaineiston saannin varmistamiseksi tutkimuksessa haastateltiin kahden kotimaisen huoltovarmuuskriittisen energia-alan yrityksen tietoturvapäälliköitä. Vertailussa paljastui kummastakin yrityksestä löytyvän kahdesta tai kolmesta kokopäiväisestä työntekijästä koostuva tietoturvayksikkö, jonka toiminnasta tietoturvapäällikkö on vastuussa ylimmälle johdolle. Kumpikaan yritys ei näe tarvetta sertifioinneille, vaan pyrkivät hyödyntämään toiminnassaan niiden parhaat näkökulmat. Molemmat yritykset kuuluvat HAVARO-palveluun, ollen näin velvoitettuja ilmoittamaan huomatuista tietoturvaloukkauksista jäsenverkostoon kuuluville yrityksille. Tietoturvapäälliköt ovat yksimielisiä henkilöstön säännöllisen kouluttamisen tärkeydestä osana menestyksekästä poikkeamanhallintaa sekä näkevät yhteistyökumppaneilta ripeästi saatavan lisäavun turvallisena. Näiltä osin yritykset ovat verrannollisia Fingridin nykytilan kanssa. Selkeimpiä eroja havaittiin Fingridin ja yrityksen B välillä vasteryhmän luomiseen, henkilöstön kouluttamiseen sekä politiikoihin ja dokumentteihin liittyvissä kysymyksissä.

Vertailun perusteella voidaan todeta Fingridin poikkeamanhallinnan olevan suurelta osin yrityksen A edellä, mutta parhaimmillaankin korkeintaan tasoissa yritykseen B verrattuna. Toisaalta vertailun tulosta osattiin odottaa henkilöstömäärien ja resurssien eroavaisuudet tiedostaen. Saatu tulos kertoo kuitenkin Fingridin poikkeamanhallinnan nykytilan olevan vertailukelpoinen astetta suurempiin yrityksiin, kunhan nykytilan kartoituksessa esitettyjä kehityskohteita toteutetaan käytännössä. Kehittämissuunnitelman mukaiset operatiiviset parannusehdotukset ovat nähtävissä tarkemmin liitteessä 4 kuvatussa prosessikaaviossa.

6.2 Mahdollisia jatkotutkimuksen aiheita

Tietoturvapoikkeamanhallinta ja siihen liittyvät käsittelyprosessit ovat sangen rajoitetusti tutkittuja aiheita – kotimainen, yritysmaailmaa aidosti palveleva tutkimustieto on vähäistä ja käytännönläheisten johtopäätösten vetäminen tuloksista siten hankalaa, luoden omalta osaltaan perusteet tutkimuksen toteuttamiselle. Jatkotutkimusmahdollisuudet keskittyvät pitkälti aiheen laajempaan tutkimiseen – aihe tarjoaisi maisterintyön laajuisena paremmat mahdollisuudet poikkeamanhallinnan nykytilan kartoittamiseen esimerkiksi suorittamalla laajoja käyttäjäkokemusta mittaavia henkilöstökyselyitä ja vertaamalla nykytilaa Fingridin pohjoismaisiin yhteistyökumppaneihin. Paremmat resurssit ja aikataulu mahdollistaisivat myös tarkastelun ulkopuolelle jätettyjen kehitysideoiden toteuttamisen käytännön tasolla.

6.3 Oman oppimisen arviointi

Tutkimusprosessi käynnistyi loppuvuodesta 2015 Fingridin tietoturvayksikön tarjoaman toimeksiannon pohjalta. Fingridissä tahdottiin kartoittaa tietoturvapoikkeamanhallinnan prosessien nykytilaa ja pohtia, kuinka prosesseja voitaisiin kehittää vastaamaan paremmin ennalta asetettuja tavoitetasoja. Tutkittavaa aihealuetta rajattaessa kävi kuitenkin nopeasti selväksi, että poikkeamanhallinta on käsitteenä valtaisan laaja. Siksipä tutkimus päädyttiin rajaamaan kehittämissuunnitelman osalta teoreettiseksi – tutkimuksessa ei otettu kantaa muutosten toteuttamiseen käytännön tasolla. Itselläni ei ollut tutkimusprosessin alkaessa lainkaan käytännön työkokemusta tietoturvan tai poikkeamanhallinnan tehtävistä, mistä johtuen matka aihealueen kokonaiskuvan täydelliseen hahmottamiseen oli erittäin raskas.

Tutkimuksen kirjallisuuskatsauksella oli ymmärrettävästi ensisijainen rooli lopputuloksen onnistumisen kannalta – lähdemateriaalin täytyi siis olla luotettavaa. Materiaalin seulonta aloitettiin heti aihealueen rajauksen jälkeen. Lähdekriittisen pohdinnan jälkeen valinnassa tutkimuksen kannalta parhaiksi lähteiksi osoittautuivat ISO/IEC 27035 -standardi, NIST ja SANS Instituten toimintamallit, ITIL palvelutoiminnan viitekehyksensä osalta, sisäiset dokumentit sekä kotimainen ja ulkomainen poikkeamanhallintaan pureutuva kirjallisuus. Kirjallisuuskatsauksen kirjoittaminen oli tutkimuksen haastavin osa-alue – perimmäisenä syynä tähän ei ollut niinkään suurelta osin englanninkielisen, kieliasultaan vaikeaselkoisen materiaalin sujuva kääntäminen ja siten kokonaisvaltainen ymmärtäminen, vaan mittavan ja usein toinen toistaan toistavan aineistomäärän järjellisen kokonaisuuden hallitseminen.

Fingrid halusi toimeksiantajana laajentaa tutkimuksen tavoitteita kesken jo käynnistyneen tutkimusprosessin. Toiveena oli selvittää, kuinka poikkeamanhallintaa suoritetaan muissa huoltovarmuuskriittisissä energia-alan yrityksissä sekä toisaalta, kuinka Fingridin nykytila kestäisi vertailussa. Tästä johtuen tutkimus päätettiin toteuttaa empiirisenä ja laadullisena tapaustutkimuksena, jossa haastattelut toteutettiin vapaamuotoisina teemahaastatteluina. Suositukseni mukaisesti Fingridin tietoturvayksiköstä haastateltiin tietoturvapäällikköä ja kahta asiantuntijaa. Alkuperäinen tarkoitus oli noudattaa samaa kaavaa vertailun yritysten kohdalla, mutta päällekkäisten aikataulujen johdosta vain tietoturvapäälliköt haastateltiin. Koska haastatteluista ei ollut aiempaa kokemusta, tilanteeseen valmistautuminen edellytti taustojen laajaa ymmärrystä, jotta kaikista aiheista pystyttiin keskustelemaan rakentavasti.

Kun itselläni oli kirjallisuuteen tutustumisen kautta hankittu kokonaisvaltainen ymmärrys tutkimusaiheesta, saatoin keskittyä kokemuksen tutkimiseen muutenkin kuin sanallisesti. Haastatteluihin valmistautuminen ja niiden toteuttaminen oli yllättävän paljon aikaa vievä prosessi, joka pidensi tutkimuksen suunnitellun valmistumisen ajankohtaa merkittävästi. Haastatteluita varten luotiin teemoihin perustuva yleinen haastattelurunko, jota käytettiin ohjaamaan vapaamuotoista keskustelua – se ei toiminut järjestelmällisenä kysymyslistana. Näitä teemoja käytettiin haastatteluiden litteroinnissa sekä myöhemmin saatujen tulosten analysoinnissa. Vaikka haastattelut olivat kestoiltaan vain noin tunnin luokkaa, litterointia hidasti tutkimuskysymyksiin soveltuvien vastausten löytämistä palveleva teemoittelu sekä erityisesti Fingridin tietoturvayksikön kohdalla usean haastateltavan samanaikainen puhe.

Pohdittaessa tutkimuksen luotettavuutta, on hyvä tiedostaa kaksi käsitettä – reliabiliteetti eli tulosten tarkkuus ja validiteetti eli tulosten pätevyys. Tutkimuksen reliabiliteettia tukee tutkimuksen kulun sekä saatujen tulosten kuvaaminen tarkasti ja kriittisesti. Tutkimuksen voidaan katsoa olevan validi eli pätevä, kun asetettuihin tutkimuskysymyksiin on pystytty vastaamaan. (Hirsjärvi ym. 2009, 231-232.) Kirjallisuuskatsaukseen valittiin ajankohtaisia ja tunnettuja lähteitä, jotka käsittelevät tutkimusaihetta eri näkökulmista. Haastatteluihin valmistauduttiin huolellisesti ja ne nauhoitettiin litterointia varten. Itselle tuntemattomien vertailuyritysten kanssa allekirjoitettiin salassapitosopimukset, poissulkien arkaluonteisen aineiston saamisen kariutumisen luottamuspulan takia. Toisaalta luotettavuutta heikentää oma kokemattomuuteni ja asiantuntijoiden poisjääminen vertailuyritysten haastatteluista.

Rajoituksista huolimatta tutkimus onnistui vastaamaan tutkimuskysymyksiin ja laatimaan toivotun kehittämissuunnitelman poikkeamanhallinnan prosessien parantamiseksi. Työn saaminen valmiiksi oli pitkä ja opettavainen prosessi, jossa kartutin osaamistani yrityksen poikkeamanhallinnan ja siihen sidoksissa olevan liiketoiminnan ydinprosesseihin liittyen. Haasteellista opinnäytetyössä oli ajanhallinta täysipäiväisen työn ja opiskelun ohella, mikä osaltaan johti lopullisen palautuksen myöhästymiseen. Varsinainen toimeksiannon osuus palautettiin kuitenkin sovitussa aikataulussa ja tutkimuksen lopputulokseen oltiin erittäin tyytyväisiä. Tuloksia onkin jo hyödynnetty Fingridin poikkeamanhallinnan kehitystyössä ja esitysmateriaaleissa. Tutkimustuloksiin tullaan palaamaan mahdollisen jatkokehityksen tarpeiden yhteydessä. Kaiken kaikkiaan olen tyytyväinen lopulliseen tuotokseen ja toivon tutkimuksesta olevan hyötyä toimeksiantajalle myös pidemmällä aikavälillä tarkasteltuna.

Lähteet

Borodkin, M. 2001. Computer Incident Response Team. GIAC Certification Version 1.2F. SANS Institute Information Security Reading Room. Luettavissa: http://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641. Luettu: 25.2.2016.

Brewster, E., Griffiths, R., Lawes, A. & Sansburg, J. 2012. IT Service Management. A Guide for ITIL Foundation Exam Candidates. British Informatics Society Limited.

Cichonski, P., Grance, T., Millar, T. & Scarfone, K. 2012. NIST Special Publication 800-61. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. Luettavissa: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf. Luettu: 13.1.2016.

ENISA 2010. Good Practice Guide for Incident Management. Luettavissa: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management. Luettu: 5.2.2016.

Eriksson, P. & Koistinen, K. 2005. Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus. Helsinki. Luettavissa: https://helda.helsinki.fi/bitstream/handle/10138/152279/Monenlainen_tapaustutkimus.pdf. Luettu: 14.1.2016.

EY 2014. Fingrid Oyj – Tietoturvallisuuden hallinnan arviointi ja johdon kehityssuunnitelma. Luottamuksellinen, vain Fingridin sisäiseen käyttöön.

Fingrid Oyj 2015a. Arvot. Luettavissa: http://www.intra.fingrid.fi. Luettu: 28.1.2016.

Fingrid Oyj 2015b. Fingrid Oyj:n tilinpäätöstiedote tammi-joulukuu 2015. Vahva talous -investoinnit jatkuivat suunnitellusti Pörssitiedotteet. Luettavissa: https://www.fingrid.fi/sivut/ajankohtaista/tiedotteet/2016/fingrid-oyjn-tilinpaatostiedote-tammi-joulukuu-2015/. Luettu: 20.2.2016.

Fingrid Oyj 2015c. Strategiset suuntaviivat 2015–2024. ICT. Yhtiö. Organisaatio. ICT. Strategia ja hankekehitys. Strategia. Luettavissa: http://intra.fingrid.fi. Luettu: 8.3.2016.

Fingrid Oyj 2015d. Fingridin tietoturvapolitiikka. Periaatteet ja politiikat. Politiikat. Tietoturvapolitiikka. Luettavissa: http://wiki.fingrid.fi. Luettu: 4.3.2016.

Fingrid Oyj 2015e. Varautuminen vakaviin ICT-häiriöihin - KI40014. Ohjeet. Käyttövarmuuden hallinta. Käytön tietojärjestelmät ja tietoliikenne I. Varautuminen vakaviin ICT-häiriöihin -KI40014. Luettavissa: http://wiki.fingrid.fi. Luettu: 7.3.2016.

Haastattelu 21.12.2015. Tietoturvayksikkö (tietoturvapäällikkö ja kaksi it-asiantuntijaa) Fingrid Oyj. Helsinki.

Haastattelu 20.1.2016a. Tietoturvapäällikkö. Yritys A (identifioiva tieto salattu). Helsinki.

Haastattelu 20.1.2016b. Tietoturvapäällikkö. Yritys B (identifioiva tieto salattu). Espoo.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo. Jyväskylä.

Hartley, J. 2004. Case Study Research. Teoksessa Cassell, C., Syman, G. (toim.). Essential guide to qualitative methods in organizational research. Sage Publications.

Hiltunen, L. Graduaineiston analysointi. Graduryhmä. Jyväskylän Yliopisto. Luettavissa: http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/aineiston_analysointi2.pdf. Luettu: 14.1.2016.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Tammi. Helsinki.

Hirsjärvi, S. & Hurme, H. 2015. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Gaudeamus. Helsinki.

Järvinen, A. & Järvinen, P. 2011. Tutkimustyön metodeista. Opinpajan kirja. Tampere.

Killcrece, G., Kossakowski, K-P., Ruefle, R. & Zajicek, M. 2003. Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University Software Engineering Institute. Luettu: 21.2.2016.

King, N. 2004. Using interviews in qualitative research. Teoksessa Cassell, C. & Syman, G. (toim.). Essential guide to qualitative methods in organizational research. Sage Publications.

Kral, P. 2012. Incident Handler's Handbook. GCIH Gold Certification. SANS Institute InfoSec Reading Room. Luettavissa: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901. Luettu: 21.2.2016.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy. Helsinki.

McMillan, R. & Walls, A. 2012. Seven Steps to Creating an Effective Computer Security Incident Response Team. Gartner. Fingridin lisenssillä. Luettu: 23.2.2016.

Myers, M. D. & Newman, M. 2007. The qualitative interview in IS research: Examining the craft. Information and organization 17. Luettavissa: http://www.pm.lth.se/fileadmin/_migrated/content_uploads/5._Qual_Interview_Texto_Leitura_Atividade_2.pdf. Luettu: 20.11.2015.

Proffitt, T. 2007. Creating and Managing an Incident Response Team for a Large Company. GCIH Gold Certification. SANS Institute InfoSec Reading Room. Luettavissa: https://www.sans.org/reading-room/whitepapers/incident/creating-managing-incident-response-team-large-company-1821. Luettu: 21.2.2016.

Eskola, J. & Saarela-Kinnunen, M. 2015. Tapaus ja tutkimus = tapaustutkimus?. Teoksessa Valli, R. & Aaltola, J. (toim.). Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. PS-kustannus. Jyväskylä.

SFS 2014. ISO/IEC 27000. Information technology - Security techniques - Information security management systems - Overview and vocabulary. Fingridin lisenssillä.

SFS 2011. ISO/IEC 27035. Information technology - Security techniques - Information security incident management. Fingridin lisenssillä.

Sarajärvi, A. & Tuomi, J. 2009. Laadullinen tutkimus ja sisällönanalyysi. Tammi. Helsinki.

Vangelos, M. 2004. Managing the Response to a Computer Security Incident. Teoksessa Krause, M. & Tipton, H. F. (toim.). Information Security Management Handbook. CRC Press LLC.

Wheatman, J. 2010. Five Reasons Why You Need a CSIRT, Even If You Think You Don't. Gartner. Fingridin lisenssillä. Luettu: 21.2.2016.

Yin, R. K. 2009. Case study research. Design and methods. Sage Publications.

Wildemuth, B. M. & Zhang, Y. 2009. Unstructured interviews. Teoksessa Wildemuth, B. M. (toim.). Applications of social research methods to questions in information and library science. Westport. Libraries Unlimited.

Liitteet

Liite 1. Teemahaastattelurunko

Teemahaastattelut 12/2015 - 01/2016		
Teemat	**Pääkysymykset**	**Täydentävät kysymykset**
Johdanto	• Kuinka olette jakaneet it-toimintonne? • Kuinka näette niiden toiminnan olevan sidoksissa keskenään? Miten se näkyy jokapäiväisessä toiminnassanne?	• Kuvaile työtehtäviäsi sekä kuinka kauan olet toiminut nykyisessä tehtävässäsi? • Mistä osa-alueista olet erityisvastuussa ja kenelle raportoit niiden toiminnasta?
Suunnittelu ja valmistautuminen	• Onko tietoturvapolitiikka luotu? Onko sisältö vapaasti koko henkilökuntanne saatavilla, esimerkiksi Intranetissä? • Kuinka ajattelet poikkeamanhallinnan vasteryhmän perustamisesta, tai onko sellainen jo toteutettu? Entä onko sillä aktiivinen rooli liiketoiminnassanne? • Kuinka hyvin johtoryhmässänne ollaan tietoisia poikkeamanhallinnan ja siihen sidonnaisten prosessien tärkeydestä? • Suoritatteko yritystasolla säännöllisiä poikkeamanhallintanne toimintatasoa käytännössä mittaavia harjoituksia? • Noudatatteko mitään tietoturva-alaan liittyvää standardia tai toimintamallia? Onko käytössänne mahdollisesti jokin näiden välimuoto? Miksi valintanne on kohdistunut juuri tähän ratkaisuun?	• Onko henkilöstö tietoinen politiikasta ja millaisia yksityiskohtia siinä käsitellään? • Oletteko ajatelleet itsenäistä politiikkaa tietoturvapoikkeamien hallinnan tueksi? • Minkä osaamisalueiden asiantuntijoista vasteryhmän jäsenet koostuvat, ja millä perusteilla heidät on valittu tehtävään? • Koulutatteko vasteryhmän jäseniä juuri poikkeamanhallinnan prosesseja varten, ja tiedetäänkö, keneen otetaan yhteyttä mahdollisten häiriötilanteiden kuluessa? • Onko poikkeamanhallinnan koulutukset pelkästään tietoturvan asiantuntijoille ja vasteryhmälle, vai onko koulutusta myös suunniteltu koko henkilöstöön nähden? • Koetteko standardit byrokraattisina sekä liian yleistävinä käyttötarkoituksiinne? • Pidättekö sertifioimista mahdollisena?
Tunnistaminen ja raportointi	• Kuinka havaitsemanne poikkeamat on pystytty tunnistamaan ja minkä kautta ne ovat lopulta tulleet teidän tietoon? • Kuvittele mielessäsi pahinta uhkaavaa haavoittuvuutta; millaisia vaikutuksia se voisi aiheuttaa liiketoiminnallenne? • Dokumentoitteko kaikki poikkeamat? • Kuinka huomioitte ydinliiketoiminnan?	• Kuvaile tyypillisesti tavattua poikkeamaa ja mistä tällainen voisi mielestäsi johtua? • Käytättekö valmiita prosesseja ja malleja entuudestaan tunnettujen poikkeamien nopeutetun käsittelyn varmistamiseksi? • Ketkä päättävät mitä dokumentoidaan? • Talletatteko kaikista poikkeamista myös lokitiedot tulevia rikostutkintoja varten?
Torjunta ja palautuminen	• Miten toimitte tilanteessa, jossa oman henkilöstönne osaaminen tai resurssit eivät riitä uhkatilanteen purkamiseen? • Kuinka turvaatte yrityssalaisuuksien ja salassa pidetyn tiedon luotettavuuden ja eheyden, kun yrityksen tietoturvaan ei voida uhkatilanteessa enää luottaa?	• Ketkä toimivat ensisijaisina kontakteina? • Mitä yhteistyötä teette ulkopuolisten tai sisäisten osapuolten kanssa tilanteessa? • Kuinka määrittelette, kenellä on tarvetta käsitellä salassa pidettävää materiaalia? • Käydäänkö vasteryhmässä vakavampien uhkien jälkeen tilannetta läpi yhdessä?
Mitä virheistä on opittu	• Millä tavoin huomioitte kohtaamianne poikkeamanhallinnan ongelmakohtia, ja toisaalta mitä olette osanneet ottaa opiksi näistä? Muutamia esimerkkejä? • Millä keinoilla lähtisitte tehostamaan poikkeamanhallinnan nykytilannetta?	• Onko harjoitusten yhteydessä huomattu selkeitä parannuskohteita, mutta joihin ei ole nyt taloudellisia mahdollisuuksia? • Koetteko selvää tarvetta tämänhetkistä läheisempään yhteistyöhön kolmansien osapuolien kanssa? Mitä tämä voisi olla?
Lopuksi	• Tuleeko sinulla vielä mieleen aiheita, joista voisi olla hyötyä tälle tutkimukselle?	
Ohjaavat kysymykset		
	• Miksi ei/kyllä? • Tarkentaisitko tätä hieman?	• Pystyisitkö kertomaan lisää? • Voisitko antaa tästä esimerkin?

Liite 2: Salassapitosopimus (identifioivat tiedot muutettu)

SALASSAPITOSITOUMUS

Tämän toimeksiantona annetun opinnäytetyön tarkoituksena on kartoittaa Fingrid Oyj:n (jäljempänä Fingrid) poikkeamienhallinnan nykytilaa ja kehittää siihen liittyviä prosesseja. Fingridin ulkopuolisia haastatteluja käytetään tässä päättötyössä vertailupohjana.

Ymmärrän, että Yritys A voi luovuttaa tämän sitoumuksen antajalle tietoturvallisuutta koskevaa aineistoa, joka saattaa sisältää Yritys A:n liiketoimintaan, prosesseihin, tietojärjestelmiin tai asiakkaisiin liittyviä tietoja, mukaan lukien liike- ja ammattisalaisuudet sekä yksityistä henkilöä koskevat luottamukselliset ja salassa pidettävät tiedot. Näiden tietojen luovutus voi tapahtua kirjallisesti, suullisesti tai muussa muodossa.

Sitoudun pitämään salassa kaikki minulle luovutetut luottamukselliset aineistot, olemaan paljastamatta tai luovuttamatta luottamuksellisia tietoja kolmansille osapuolille sekä olemaan käyttämättä luottamuksellisia tietoja muuhun kuin toimeksiantona annetun päättötyön suorittamiseen. Sitoudun myös käsittelemään ja säilyttämään luottamuksellisia tietoja huolellisesti ja säädösten ja määräysten sekä mahdollisesti erikseen sovittavien ohjeiden mukaisesti.

Ymmärrän, että tämän salassapitositoumuksen rikkominen voi aiheuttaa Yritys A:lle, sen henkilöstölle tai sen asiakkaille merkittävää vahinkoa ja johtaa eräissä tapauksissa vahingonkorvaus- ja rikosoikeudellisiin vastuisiin ja seuraamuksiin.

Sitoumus astuu voimaan välittömästi ja jatkuu myös toimeksiantoon liittyvän päättötyön valmistumisen jälkeen. Haastattelun aikana jaetut dokumentit palautetaan tai hävitetään ja haastattelun mahdollinen nauhoitus hävitetään välittömästi toimeksiannon valmistuttua.

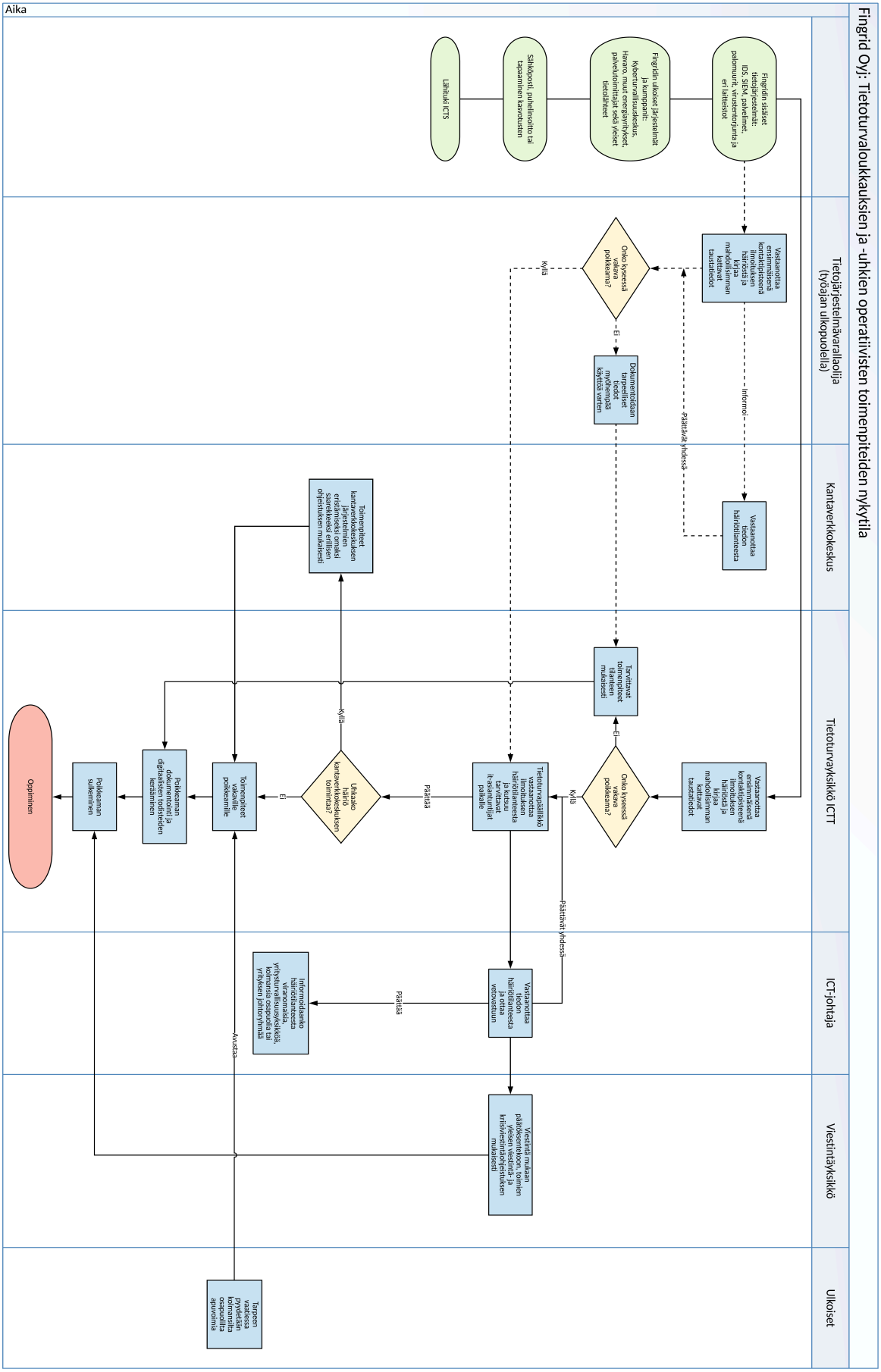
Tätä salassapitosopimusta on laadittu kaksi (2) kappaletta, yksi (1) kullekin osapuolelle.

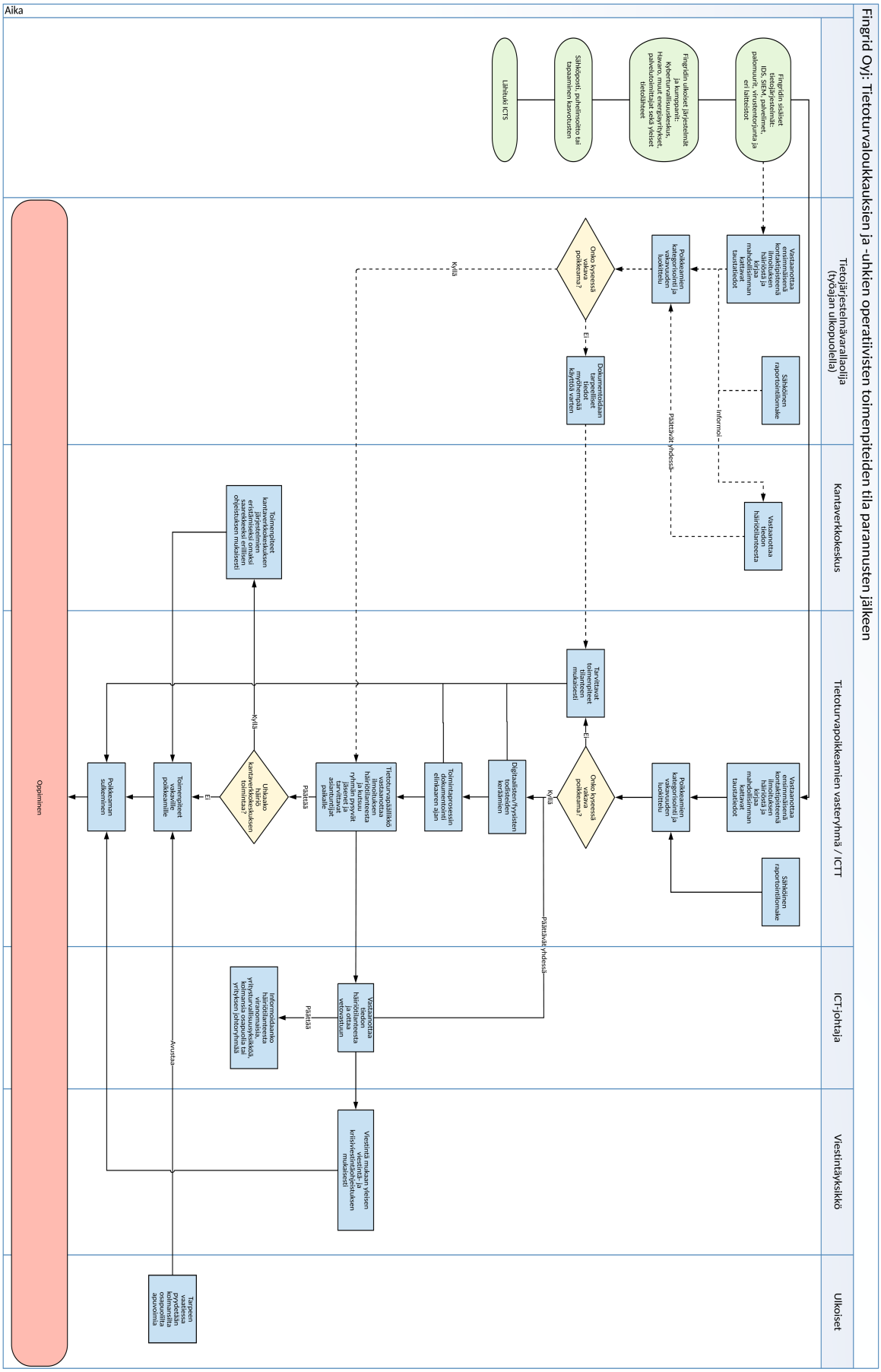
Suostun haastattelun nauhoittamiseen: kyllä ____ ei ____

Helsingissä 20.päivänä tammikuuta 2016.

_____	_____
Matti Tuovinen opinnäytetyöntekijä Fingrid Oyj	tietoturvapäällikkö Yritys A

Liite 3. Fingrid Oyj: Operatiivisten toimenpiteiden nykytila




Fingrid Oyj: Tietoturvaloukkauksien ja -uhkien operatiivisten toimenpiteiden tila parannusten jälkeen
Aika
Tietojärjestelmävarallaolija (työ/ajan ulkopuolella)
Kantaverkkokeskus
Tietoturvapoikkeamien vastevyhmä / ICT
ICT-johtaja
Viestintäyksikkö
Ulkoiset
Fingridin sisäiset tietojärjestelmät: IDS, SIEM, palvelimet, palomuuri, tunnistautuminen eri laitteistot
Fingridin ulkoiset järjestelmät ja kumppanit: Kyberturvallisuuskeskus, Havaintoverkon palvelutoimittajat sekä yleiset tietolähteet
Sähköposti, puhelinsoitto tai tapaaminen kasvotusten
Lähituki ICT
Vastaanottaa ilmoituksen kontaktipisteenä toimien ilmoituksen hyväksyjä ja mahdollisimman kattavat taustatiedot
Sähköinen raportointilomake
Poikkeamien kategorisointi ja vakavuuden luokittelu
Onko kyseessä poikkeama?
Dokumentoidaan tarpeelliset myöhempää käyttöä varten
Tarvittavat toimenpiteet tilanteen mukaisesti
Digitaalisten/fyysisten todisteiden keräämien
Toimintaprosessin dokumentointi ehkäisemi sjan
Tietoturvapäällikkö ilmoituksen häiriötilanteesta ryhmän pyyvät jäsenet ja asiantuntijat paikalle
Uhkaako kantaverkkokeskuksen häiriö kantaverkkokeskuksen toimintaa?
Toimenpiteet vakaroille poikkeamille
Poikkeamaan sulkeminen
Toimenpiteet kantaverkkokeskuksen järjestelmien eristämiseksi omaksi saarekkeeksi ohjeistuksen mukaisesti
Vastaanottaa tietoja häiriötilanteesta
Informoidaanko kantaverkkokeskuksen viranomaisia, yritysturvallisuuspäällikköä, yrityksen johtoryhmää
Viestintää mukaan yleisen viestinnän ja kriisiviestintäohjeistuksen mukaisesti
Tarpeen vaatiessa pyydetään konsultteilta osaporoilta apuvoimia
Oppiminen
Kyllä
Ei
Informoi
Päättävät yhdessä
Päätetää
Avustaa