Axel Aspholm

HÄIRIÖOPPIMINEN OSANA ORGANISAATION TIE-TOTURVAA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Aspholm, Axel
Häiriöoppiminen osana organisaation tietoturvaa
Jyväskylä: Jyväskylän yliopisto, 2021, 42 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja: Marttiin, Pentti

Häiriöoppimisella tarkoitetaan prosessia, jonka avulla organisaatio hyödyntää häiriötietoa toimintansa ja etenkin tietoturvansa parantamiseen. Tämän kandidaatintutkielman tarkoituksena on integroivan kirjallisuuskatsauksen muodossa selvittää, miten häiriöoppimista toteutetaan osana organisaation tietoturvaa ja mitkä ovat keskeiset esteet tehokkaalle häiriöoppimiselle. Tarkoituksena on myös esittää kirjallisuudesta löydettyjä ratkaisuja ja malleja organisaation häiriöoppimiskyvykkyyden parantamiseen. Tutkielman aikana selvisi, että häiriöoppiminen rajoittuu useassa organisaatiossa lähinnä häiriönhallintaprosessin tekniseen tehostamiseen. Organisaatioiden häiriöoppiminen on suurilta osin epäjärjestelmällistä ja menetelmät epämuodollisia varsinkin matalan prioriteetin häiriöiden osalta. Korkean prioriteetin häiriöt tutkitaan pääsääntöisesti tarkasti, mutta tutkinnan tuloksia ei hyödynnetä järjestelmällisesti hallinnollisten tietoturvakäytäntöjen arvioimiseen ja kehittämiseen. Tutkielmassa löydettiin kolme häiriöoppimismallia, joita esitettiin ratkaisuiksi organisaatioiden häiriöoppimisessa ilmenneisiin ongelmiin. Mallit korostavat häiriönhallinnan ja muiden organisaation sisäisten sidosryhmien välisen tiiviin yhteistyön ja viestinnän tärkeyttä häiriöoppimisen tehokkaassa toteutuksessa. Mallit liittävät häiriöoppimisen häiriönhallinnan teknisen tehostamisen lisäksi koskemaan organisaation tietoturvakäytänteiden ja strategian arvioimista ja kehittämistä.

Asiasanat: tietoturva, häiriönhallinta, organisaation oppiminen, häiriöoppiminen

ABSTRACT

Aspholm, Axel
Incident learning as a part of an organization information security
Jyväskylä: University of Jyväskylä, 2021, 42 pp.
Information Systems, Bachelor's thesis
Supervisor: Marttiin, Pentti

Incident learning refers to the process by which an organization utilizes incident information to improve its operations and, in particular, its information security. The purpose of this bachelor's thesis is to find out, in the form of an integrative literature review, how incident learning is implemented as part of an organization's information security and what are the main obstacles to effective incident learning. It is also intended to present solutions and models found in the literature for improving an organization's ability to learn from incidents. During the thesis, it became clear that incident learning in several organizations is mainly limited to the technical enhancement of the incident handling process. Organizational incident learning is largely unsystematic and methods informal, especially for low-priority incidents. High-priority incidents are generally investigated closely, but the results of the investigation are not systematically used to assess and develop administrative security practices. In the study, three models of incident learning were found, which were presented as solutions to the problems encountered in incident learning in organizations. The models emphasize the importance of close cooperation and communication between incident response team and other internal stakeholders in the effective implementation of incident learning. In addition to the technical enhancement of incident handling, the models link incident learning to the evaluation and development of an organization's security policies and strategy.

Keywords: information security, incident handling, organizational learning, incident learning

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Liiketoimintatiedon hyödyntäminen yritysten liiketoimintaprosessien kehittämisessä ja päätöksenteon nopeuttamisessa on kasvanut merkittävästi 90-luvulta lähtien. Tiedon tallentamiseen ja käsittelyyn liittyvien kustannusten lasku on antanut yrityksille mahdollisuuden kerätä valtavia määriä toimintaansa liittyvää dataa useista eri lähteistä. (Chaudhuri, Dayal & Narasayya, 2011.) Erilaisia business intelligence (BI) ratkaisuja hyödyntämällä organisaatiot pystyvät valjastamaan keräämäänsä liiketoimintatietoa liiketoimintaprosessiensa tehostamiseen esimerkiksi kilpailuedun tai kustannussäästöjen tavoittelemiseksi (Harrison, Parker, Brosas, Chiong & Tian, 2015). Liiketoimintatiedon käsittelyyn käytettyjen järjestelmien ja tietoteknisen infrastruktuurin suojaamisesta ja asianmukaisen toiminnan varmistamisesta onkin tullut merkittävä perusedellytys liiketoiminnan jatkuvuuden turvaamiseksi. Erilaiset kyberhyökkäykset, kuten tietomurrot, tietojen kalasteluhyökkäykset ja kiristyshaittaohjelmat ovat viime vuosina yleistyneet ja esimerkiksi erilaiset haittaohjelmatartunnat kasvoivat vuosien 2015 ja 2018 välillä noin 453 miljoonasta jopa 812 miljoonaan vuosittaiseen tartuntaan (Purplesec, 2021). Vuonna 2020 havaittiin noin 138 miljoonaa uutta haittaohjelmaa ja vuoden 2021 kesäkuuhun mennessä uusia haittaohjelmia oli havaittu noin 93 miljoonaa vuoden alusta lähtien. Cyber edge groupin laatimassa raportissa kyberhyökkäyksen uhriksi oli vuonna 2021 joutunut 86,2 % haastatelluista yrityksistä. (Zaharia, 2021.) Vuonna 2020 keskimääräinen tietomurron havaitsemiseen kulunut aika yrityksessä oli 207 päivää ja aiheutuneet kustannukset $3,86 miljoonaa (Sobers, 2021).

Tilastot auttavat hahmottamaan tieto- ja kyberturvakyvykkyyden tärkeyttä organisaation liiketoiminnan jatkuvuuden turvaajana. Tietoturvatoiminnon tarkoituksena on erilaisten teknisten ja hallinnollisten suojaustoimenpiteiden avulla suojata organisaatiota sen tieto- ja tietoteknisiä resursseja uhkaavilta hyökkäyksiltä ja häiriöiltä. Organisaation tietoturvaan liittyvä keskeinen osatoiminto on häiriönhallinta. Häiriönhallinnan tehtävänä on varautua ja vastata organisaation kohtaamiin tietoturvahyökkäyksiin ja -häiriöihin lievittäen niistä organisaation toiminnalle koituvia haittoja. (Ahmad, Desouza, Maynard, Naseer & Baskerville, 2020.) Häiriönhallintaprosessin aikana kerätään ja käsitel-

lään häiriötietoa, jota voidaan hyödyntää organisaation tietoturvan kehittämisessä. Häiriöoppimisella tarkoitetaan prosessia, jonka avulla organisaatio hyödyntää häiriötietoa toimintansa ja etenkin tietoturvansa parantamiseen. (Ahmad, Maynard & Shanks, 2015.) Tehokkaan häiriöoppimisen hyödyiksi on esitetty muun muassa häiriönhallintaprosessin nopeuden, joustavuuden ja tehokkuuden kasvua, laajempaa ymmärrystä häiriöistä, päätöksenteon tarkkuuden kasvua sekä tietoturvatoimintoa ohjaavien käytäntöjen ja strategian huomioimista, arvioimista ja muokkaamista osana tietoturvatoiminnon parantamista. (Ahmad ym., 2020; Shedden, Ahmad & Ruighaver, 2010.)

Tämän tutkielman tarkoituksena on tutustua häiriöoppimiseen osana organisaation tietoturvatoimintoa ja selvittää mitä ongelmia organisaatioiden häiriöoppimiseen liittyy. Tarkoituksena on myös esitellä erilaisia malleja häiriöoppimiskyvykkyyden parantamiseen. Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

1) Mitkä ovat keskeisiä esteitä tehokkaalle häiriöoppimiselle organisaatiossa?
2) Millaisia malleja tutkimuskirjallisuus tarjoaa organisaation häiriöoppimiskyvykkyyden parantamiseen?

Tutkielman sisältö koostuu johdannosta, kolmesta sisältöluvusta ja yhteenvedosta. Toisessa ja kolmannessa luvussa esitellään ja määritellään tutkielman kannalta oleellinen tietoturvaan, häiriönhallintaan ja organisaation oppimiseen liittyvä käsitteistö. Neljännessä luvussa analysoidaan kirjallisuuskatsauksessa löydettyä aineistoa ja pyritään vastaamaan tutkimuskysymyksiin. Kirjallisuudesta löydetyt organisaation häiriöoppimiseen liittyvät ongelmat voidaan pääpiirteissään jakaa kolmeen kategoriaan: kommunikaatioon ja viestintään liittyviin ongelmiin, häiriöiden tutkintaan ja raportointiin liittyviin ongelmiin ja tutkinnan tulosten ja häiriötiedon hyödyntämiseen liittyviin ongelmiin. Kirjallisuudesta löydettiin myös kolme häiriöoppimismallia organisaation häiriöoppimiskyvykkyyden parantamiseen.

Tutkielma toteutettiin integroivana kirjallisuuskatsauksena. Tutkielman kahdessa ensimmäisessä kappaleessa esitetyn teoreettisen pohjan määrittelyä varten lähteitä etsittiin vapaamuotoisesti useilla tietoturvaan ja häiriönhallintaan liittyvillä hakusanoilla. Tutkimusaineistoa haettiin pääasiassa JYKDOK- ja Google Scholar -hakupalveluista ja hakusanoina käytettiin muun muassa *"security incident learning"*, *"incident response"* ja *"information security"* hakutermejä. Tutkielman neljännessä kappaleessa analysoidut lähdemateriaalit valikoitiin hakutulosten joukosta seuraavien kriteerien perusteella: tutkimusten piti tarkastella organisaation tietoturvahäiriönhallintaprosessia organisaation oppimisen teoriaan pohjautuvan viitekehyksen kautta. Tutkimuksen tuli lisäksi käsitellä häiriöoppimisen haasteita ja/tai esittää suosituksia häiriöoppimisen kehittämiseen organisaatiossa.

2 TIETO- JA KYBERTURVA ORGANISAATIOSSA

Tietoturvaan liittyy monia käsitteitä, joiden tarkempi määrittely helpottaa hahmottamaan tietoturvan roolia organisaation kontekstissa. Seuraavissa alaluvuissa käsitellään keskeisiä tieto- ja kyberturvaan liittyviä käsitteitä ja niiden määritelmiä kansainvälisissä standardeissa ja tutkimuskirjallisuudessa.

2.1 Keskeisiä käsitteitä

Yrityksen resurssien ja voimavarojen (asset) suojaaminen on kaikkien turvatoimenpiteiden keskeinen tavoite. Voimavarat voivat olla aineellisia tai aineettomia. Esimerkkejä aineellisista voimavaroista ovat yrityksen fyysinen tuotantolaitteisto, toimitilat ja tietotekniset laitteet. Aineettomia voimavaroja ovat esimerkiksi data, ohjelmistot ja yrityksen maine. (NIST, 2017; Von Solms & Van Niekerk, 2013; Fenz & Ekelhart, 2009.) Fenz ja Ekelhart (2009) esittävät tutkimuksessaan tietoturvaontologian, jossa he kuvaavat organisaation turvallisuuteen liittyvien konseptien välisiä suhteita. Heidän mukaansa voimavara on konsepti, jonka organisaatio omistaa ja jolle haavoittuvuus luo uhan.

Stallings ja Brown (2018, s. 31) määrittelevät tietoturvauhan tarkoittamaan mahdollista resurssiin tai voimavaraan kohdistuvaa turvallisuushaittaa. Fenzin ja Ekelhartin (2009) ontologiassa uhalla on lähde ja alkuperä. Uhan alkuperä voi olla ihmislähtöinen (esim. haittaohjelma tai palvelunestohyökkäys jne.) tai luonnollisista syistä johtuva (esim. maanjäristys tai tsunami jne.). Uhan lähde on joko vahinko (esim. laitevika) tai se on aiheutettu tarkoituksellisesti (esim. varkaus tai haittaohjelma). Uhka vaarantaa yrityksen voimavaran käyttämällä hyväksi voimavaraan liittyvää haavoittuvuutta. (Fenz & Ekelhart, 2009.)

NIST (2017) määrittelee haavoittuvuuden sellaiseksi heikkoudeksi järjestelmässä, järjestelmän turvallisuusmenettelyssä, turvallisuudenhallinnassa tai implementaatiossa, jota jokin uhan lähde kykenee hyväksikäyttämään. Fenzin ja Ekelhartin (2009) ontologiassa haavoittuvuus liittyy organisaation voimava-

raan ja sillä on vakavuusaste. Haavoittuvuuteen liittyy myös kontrollitoimenpiteitä, jotka lieventävät siihen liittyvää riskiä (Fenz & Ekelhart, 2009). Tietoturvakontrollit ovat riskejä lieventäviä toimia, laitteita, menettelytapoja tai muunlaisia keinoja, jotka eliminoivat tai ehkäisevät tietoturvarikkomuksia, minimoivat niistä aiheutuvaa haittaa tai havaitsevat ja raportoivat niitä mahdollistaen korjaavat toimenpiteet. Kontrollit voidaan jakaa kolmeen pääluokkaan: hallinnollisiin kontrolleihin (tietoturvakäytännöt ja koulutukset jne.), operatiivisiin kontrolleihin (tietoturvaohjeistusten implementointi jne.) ja teknisiin kontrolleihin (tunkeutumisen tunnistusjärjestelmät jne.). (Stallings & Brown, 2018, s. 512-513.)

Riski on suure, joka kuvaa entiteettiin kohdistuvan tapahtuman uhkaavuuden astetta. Riski määritellään tapahtuman toteutumisesta aiheutuvien haittojen vakavuuden ja tapahtuman todennäköisyyden funktiona. Tieto- ja kyberturvan kontekstissa entiteetit, joihin riski kohdistuu ovat organisaation toiminnot, resurssit ja voimavarat, yksilöt, muut organisaatiot ja laajimmillaan koko yhteiskunta. (NIST, 2017.) Riski voidaan siis nähdä entiteettiin kohdistuvana uhkaskenaariona, jolla on vakavuusaste ja todennäköisyys.

2.1.1 Tietoturva

Tietoturvalla tarkoitetaan yleisesti sellaisia toimia, joiden tarkoituksena on tiedon suojeleminen tapahtumilta, joiden seurauksena tiedon luottamuksellisuus, eheys tai saatavuus vaarantuu. Kun tieto toteuttaa luotettavuuden, eheyden ja saatavuuden periaatteet, voidaan tiedon todeta olevan turvattu. (Whitman & Mattord, 2016; Von Solms & Van Niekerk, 2013.) Myös kansainvälinen ISO/IEC 17799:2005 standardi määrittelee tietoturvan tiedon luottamuksellisuuden, eheyden ja saatavuuden turvaamisena. Määritelmässä tiedon esiintymismuodolla ei ole merkitystä ja se voi esiintyä elektronisen tallennusmuodon lisäksi myös esimerkiksi kirjoitettuna tai puheen muodossa. NIST (2017) määrittelee tietoturvan tarkemmin tiedon ja tietojärjestelmien suojaamiseksi luvattomalta pääsyltä, käytöltä, paljastumiselta, häiriöiltä, muokkaamiselta tai tuhoutumiselta luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi. Nämä kolme tietoturvan määritelmissä toistuvaa tiedon ominaisuutta tunnetaan yleisesti CIA (confidentiality, integrity, availability) kolmiomallina, jota pidetään yleisesti alan standardina tietoturvan määrittelyssä (Von Solms & Van Niekerk, 2013). Fenzin ja Ekelhartin (2009) mallissa luottamuksellisuus, eheys ja saatavuus ovat voimavaran tai resurssin ominaisuuksia, joihin uhka vaikuttaa sen päästyä hyväksikäyttämään jotain heikkoutta.

NIST (2017) määrittelee luottamuksellisuuden tiedon saatavuuden (access) ja paljastumisen (disclosure) rajoittamiseksi valtuutetuille tahoille. Yleisiä tapoja tiedon luotettavuuden varmistamiseen ovat esimerkiksi tiedon salaaminen (encryption), käyttäjän tunnistusdokumentit (user ID), sekä salasanat ja muut autentikointikeinot, kuten sormenjälkitunnistus (Tchernykh, Schwiegelsohn, Talbi, Babenko, 2019).

Tiedon eheydellä tarkoitetaan NIST (2017) mukaan suojautumista tiedon luvattomalta muokkaamiselta tai tuhoamiselta sen kiistämättömyyden ja autenttisuuden varmistamiseksi. Tiedon eheys varmistaa, että tieto on luotettavaa ja tarkkaa (Tchernykh ym., 2019).

NIST (2017) määrittelee saatavuuden siten, että tietoon päästään varmuudella käsiksi silloin kun sitä tarvitaan. Saatavuus takaa valtuutettujen tahojen käyttövarman pääsyn tietoon (Tchernykh ym., 2019).

2.1.2 Kyberturva

Tieto- ja kyberturvallisuuden käsitteitä käytetään usein ristiin huomioimatta niiden merkityseroja (Von Solms & Van Niekerk, 2013). Siinä missä tietoturvan käsite on yleisesti vakiintunut tarkoittamaan tiedon luotettavuuden, eheyden ja saatavuuden suojaamista, kyberturvan merkitys vaihtelee usein kirjallisuudessa tilanteen ja kontekstin mukaan ja termiä myös käytetään usein kaiken kattavana käsitteenä tarkoittamaan yleisesti tietoteknisten resurssien ja järjestelmien suojaamista. (Craigen, Diakun-Thibault & Purse, 2014; Von Solms & Van Niekerk, 2013).

Von Solms ja Van Niekerk (2013) käsittelevät tutkimuksessaan kyberturvan ja tietoturvan käsitteellisiä eroja. Heidän mukaansa kyberturvallisuus laajentaa turvattavien kohteiden joukon koskemaan tiedon ja informaatioteknologiainfrastruktuurin lisäksi myös ihmistä ja yhteiskuntaa. Esimerkiksi kodin IoT-laitteisiin kohdistuneet hyökkäykset voivat saattaa talon asukkaat suoraan vaaraan ja hyökkäykset valtion kriittistä infrastruktuuria, kuten sähköverkkoa tai vedenjakelua kohtaan voivat aiheuttaa merkittävää tuhoa koko yhteiskunnan mittakaavalla. Edellä kuvatut hyökkäykset eivät välttämättä vaaranna tiedon luotettavuutta, eheyttä tai saatavuutta, joten niiltä suojautuminen on määritelmällisesti tietoturvan ulottumattomissa. (Von Solms & Van Niekerk, 2013.)

Yhteenvetona kyberturvallisuuden voidaan katsoa tarkoittavan kaikkien niiden kohteiden ja resurssien suojaamista, jotka voivat vaarantua kyberympäristön kautta toteutetussa hyökkäyksessä pitäen sisällään tiedon lisäksi ICT laitteiston, ihmisen ja laajemmin koko yhteiskunnan (Von Solms & Van Niekerk, 2013). Myös sanastokeskus (2018) tukee tätä näkemystä omalla kyberturvallisuuden määritelmällään: ”*tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan*”. Kybertoimintaympäristöllä viitataan digitaalisten tietojärjestelmien muodostamaan toimintaympäristöön (Sanastokeskus, 2018).

2.2 Tietoturva organisaatiossa

Tietoturvaa organisaation toimintona on sen alkuaikoina käsitelty yrityksissä lähinnä teknisenä ongelmana, johon on pyritty vastaamaan teknisillä ratkaisuilla. Sittemmin tietoturvan kehitys yrityksen toimintona on laajentunut puhtaasti

teknisestä toiminnosta osaksi organisaation johtotason hallinnollisia toimintoja, jossa sen rooli yrityksen arvontuotannossa tietoteknisten resurssien ja liiketoimintaprosessien toiminnan turvaajana on kasvavissa määrin tunnistettu (Eloff & Da Veiga, 2007; Posthumus & Von Solms, 2004; Narain Singh, Gupta & Ojha, 2014). Tietoturva ei olekaan Von Solmsin ja Van Niekerkin (2013) mukaan yrityksessä mikään yksittäinen teknologia tai tuote vaan pikemminkin jatkuva prosessi. Tämän prosessin tarkoituksena on turvata organisaation liiketoimintaprosesseille elintärkeän liiketoimintatiedon luotettavuus, eheys ja saatavuus (Posthumus & Von Solms, 2004).

Tietoturvaprosessiin sisältyvät tietoturvakäytännöt ja periaatteet voidaan karkeasti jakaa preventiivisiin ja responsiivisiin suojautumiskeinoihin, joiden tarkoituksena on ennalta-ehkäistä ja vastata organisaatioon kohdistuviin tietoturvauhkiin. Organisaatio koostaa tietoturvastrategiansa näistä preventiivisistä ja responsiivisista suojautumiskeinoista, jolloin onnistuneesti luotu strategia vastaa sen uhkaympäristön asettamiin vaatimuksiin (Baskerville, Spagnoletti & Kim, 2014). Whitmanin ja Mattordin (2016, s.47) mukaan tietoturva toteuttaa organisaatiossa neljää tärkeää toimintoa. Nämä toiminnot ovat organisaation toimintakyvyn turvaaminen, organisaation keräämän datan ja informaation turvaaminen, organisaation tietoteknisissä järjestelmissä toimivien ohjelmien turvallisen käytön mahdollistaminen ja organisaation teknologiaresurssien (technology asset) suojaaminen.

2.2.1 Tietoturvan sisäinen organisointi

Tietoturvan sisäinen organisointi on yrityskohtaista ja sen käytännön toteutustavat saattavat erota toisistaan paljonkin yritysten välillä. Kansainväliset standardit ja viitekehykset kuten ISO 27001, COBIT, ITIL ja NIST SP 800-12 sekä akateeminen kirjallisuus tarjoavat erilaisia malleja tietoturvan organisointiin yrityksessä.

Yritysjohdon tuki tietoturvalle ja tietoturvan sisäinen organisointi osaksi yrityksen johtavan tason kokonaisvaltaista strategista hallinnointia (Corporate Governance) nähdään kirjallisuudessa keskeisenä tietoturvan onnistuneen toteutuksen menestystekijänä (AlGhamdi, Win & Vlahu-Gjorgievska, 2020; Soomro, Mahmood & Ahmed, 2016). Tähän tietoturvan strategisen tason hallinnointiin viitataan yleisesti termillä ISG (information security governance). Tietoturvasäännösten ja käytäntöjen käytännön johtamiseen viitataan sen sijaan termillä ISM (information security management). Nämä kaksi toimintoa mahdollistavat tietoturvatoiminnon johdonmukaisen ja kokonaisvaltaisen, eri osastot yhdistävän suunnittelun ja toteutuksen organisaatiossa.

2.2.2 Tietoturvan johtotason hallinnointi

Posthumus ja von Solms (2004) määrittelevät ISG:n prosesseiksi, joiden kautta tietoturva otetaan huomioon yrityksen johtavalla strategisella tasolla. ISG on siis yrityksen johtoportaan toteuttamaa strategista politiikkaa, jonka tehtävänä

on varmistaa, että tietoturva tunnustetaan osana yrityksen perustavanlaatuisia toimintoja. ISG:n tarkoituksena on varmistaa, että tietoturva on strategisella tasolla linjassa yrityksen mission ja liiketoiminnan tavoitteiden kanssa (Posthumus & Von Solms, 2004).

AlGhamdin ym. (2020) toteuttamassa kirjallisuuskatsauksessa analysoitiin ISG:ä käsitteleviä tutkimusartikkeleita ja jaettiin löydetyt ISG:n toteutukseen liittyvät kriittiset menestystekijät seitsemään aihepiiriin. Tunnistetut aihepiirit olivat vastuu ja velvollisuus, tietoisuus, noudattaminen, arviointi, mittaaminen, raportointi ja monitorointi. Analysoiduissa artikkeleissa korostui yritysjohdon roolin merkittävyys sekä organisaatiokulttuurin ja tietoturvakulttuurin vaikutus ISG:n onnistumisessa. Analysoiduissa tutkimuksissa korostui myös tunnettujen viitekehysten, kuten ISO 27001 ja COBIT:n hyödyntäminen ISG-mallien luomisessa. Tutkimuksessa korostetaan tarvetta kokonaisvaltaisen tietoturvan hallinnointimallin kehittämiseen, joka linjaisi yhteen tietoturvan ja yrityksen liiketoiminnan tavoitteet ja ottaisi kattavasti huomioon tutkimuksessa tunnistetut kriittiset menestystekijät. (AlGhamdi ym., 2020.)

2.2.3 Tietoturvan johtaminen

ISM toteuttaa organisaatiossa johdon laatimia tietoturvan strategisia tavoitteita ja määräyksiä (Posthumus & Von Solms, 2004). ISM on osa yrityksen johtamistoimintoja ja sen tarkoituksena on pystyttää, toteuttaa, monitoroida, arvioida, huoltaa ja parantaa organisaation tietoturvaa liiketoimintariskin näkökulmasta. Tarkoituksena on sovittaa organisaation tietoturvatavoitteet yhteen liiketoiminnan tarpeiden kanssa (Narain Singh ym., 2014). Tietoturvaa johdetaan yleensä liiketoimintariskin näkökulmasta, mikä tarkoittaa sitä, että tietoturvakäytäntöjen ja strategian laatiminen alkaa tietoturvariskiympäristön kartoittamisesta. Resurssit ja niihin liittyvät uhat kartoitetaan ja resursseihin liittyvät riskit tunnistetaan arvioimalla niiden toteutumisen todennäköisyyttä ja vaikutuksia. (Ahmad ym., 2020; Narain Singh ym., 2014.)

ISM suojaa organisaation resursseja ja voimavaroja toteuttamalla suojausaktiviteetteja strategisella, taktisella ja operatiivisella tasolla. Näillä tasoilla toteutettavat aktiviteetit voidaan jakaa viiteen johtamiskäytännealueeseen: tietoturvakäytäntöjen ja politiikan hallinta, riskienhallinta, häiriönhallinta, tietoturvakoulutuksen, -harjoitteiden ja -tietoisuuden hallinta sekä tekniikan hallinta. Nämä johtamiskäytänteet institutionalisoidaan kehittämisen, implementoinnin ja ylläpitämisen ja arvioinnin vaiheiden kautta osaksi organisaation tietoturvatoimintoa. (Ahmad ym., 2020.) Narain Singh ym. (2014) tutkivat ISM kirjallisuutta ja löysivät kymmenen käytännealuetta, jotka olivat osittain samoja kuin Ahmad ym. (2020) esittämät viisi pääaluetta. Strategisen tason tekijöiksi tunnistettiin ylätason johdon tuki ja tietoturvakäytäntöjen laatiminen. ISM:n taktisen tason tekijät olivat tietoturvakoulutus, -tietoisuus ja -kulttuuri. Operatiivisen tason tekijät olivat tietoturva auditointi, parhaiden ISM käytänteiden noudattaminen ja resurssien/ voimavarojen hallinta, johon kuuluu resurssien omistajuuden, liiketoimintakriittisyyden ja riskien kartoitus ja hallinta. Häiriöhallinta

ja tietoturvasääntelyn noudattaminen olivat viimeiset kirjallisuudesta löydetyt ISM käytännealueet. Näiden katsottiin olevan yleisluontoisia tekijöitä, jotka eivät kuuluneet millekään tietylle tasolle. (Narain Singh ym., 2014.)

Myös Soomro ym. (2016) toteuttivat systemaattisen kirjallisuuskatsauksen tietoturvan johtamista (ISM) käsittelevästä tutkimuskirjallisuudesta. Myös heidän tutkimustuloksissaan korostui yritysjohdon roolin merkittävyys ja liiketoiminnan tavoitteiden ja tietoturvan yhteensovittaminen. Lisäksi kirjallisuudessa merkittäviksi aiheiksi nousi mm. tietoturvan johtamisen rooli tietoturvakäytänteiden laatimisessa ja käyttöönotossa, tietoturvatietoisuus ja inhimillisten tekijöiden merkittävyys tietomurroissa ja käytänteiden noudattamisessa. Al-Ghamid ym. (2020) tapaan myös Soomro ym. (2016) tunnistavat organisaatioissa tarpeen kokonaisvaltaisen tietoturvan johtamismallin käyttöönottoon. Tietoturvan johtamisessa pitäisi heidän mukaansa ottaa etenkin huomioon ylätason johdon, henkilöstöhallinnon ja stategisten päätöksentekijöiden osallistaminen sekä tietoturvakäytäntöjen laatiminen ja toteuttaminen ja tietoturvatietoisuuskoulutus. (Soomro ym., 2016.)

ISM:n tehtävä voidaan edellä referoitujen lähteiden pohjalta nähdä organisaation resurssien ja voimavarojen suojelemisena eräänlaisen suojauskäytäntöjä ja kontrolleja sisältävän työkalupakin avulla. ISM kehittää, toteuttaa, pitää yllä ja arvioi sisältöä riskienhallinnan toteuttaman riskiympäristön kartoituksen pohjalta. Tunnistettuja resursseihin kohdistuvia riskejä lievennetään strategisella, taktisella ja operatiivisella tasolla toteutettavien suojausaktiviteettien avulla.

2.3 Häiriönhallinta

Organisaatiot tulevat suurella todennäköisyydellä jossain vaiheessa elinkaartaan kärsimään jonkin asteisesta tietoturvahäiriöstä. Tietoturvahäiriön tavallisia seurauksia ovat suorat taloudelliset haitat, kuten tuotannon häiriintyminen, mainehaitat, kuten asiakkaan luottamuksen menetys sekä mahdolliset lailliset ongelmat (Ahmad, Hadgkiss & Ruighaver, 2012).

Yrityksen näkökulmasta tietoturvahäiriönhallinnan tavoitteena on lievittää voimavarojen ja resurssien luotettavuuteen, eheyteen ja saatavuuteen kohdistuvia riskejä ja turvata ja minimoida tietoturvahyökkäyksen aiheuttama taloudellinen, maineellinen ja laillinen vahinko yritykselle. Häiriönhallinta on vastuussa tietoturvahyökkäykseen vastaamisesta erityisesti silloin, kun yrityksen rakentamat tietoturvasuojaukset pettävät (Rahman & Choo, 2015; Ahmad, Maynard, Desouza, Kotsias, Whitty & Baskerville, 2021).

Tässä kappaleessa tutustutaan häiriönhallintaan organisaation toimintona. Aluksi tutustutaan tietoturvahäiriön ja häiriönhallinnan käsitteisiin ja niiden määrittelyyn organisaation kontekstissa. Kappaleen lopussa esitellään tarkemmin NIST SP 800-61 julkaisun mukainen häiriönhallintamalli.

2.3.1 Tietoturvahäiriö

Tietoturvahäiriölle on annettu yksityiskohdiltaan hiukan toisistaan eroavia määritelmiä kansainvälisissä standardeissa ja parhaiden käytäntöjen kokoelmissa. Tarkastellaan seuraavaksi tietoturvahäiriön määritelmiä tällaisissa keskeisissä häiriönhallintaohjeistuksissa sekä alan kirjallisuudessa.

NIST (2012) määrittelee tietoturvahäiriön tietoturvakäytäntöjen, hyväksyttävän käytön ohjeiden tai yleisten turvakäytäntöjen rikkomukseksi tai välittömän rikkomuksen uhaksi: *"A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."* (NIST, 2012). Esimerkkeinä erilaisista häiriöistä mainitaan palvelunestohyökkäys, sähköpostin välityksellä levitettävä haittaohjelma, tietoturvahyökkäyksessä vuotaneen sensitiivisen tiedon avulla kiristäminen ja käyttäjän jakama sensitiivinen tieto.

ISO/IEC 27035:2011 -standardissa tietoturvahäiriö määritellään yhdeksi tai useammaksi toisiinsa liittyväksi odottamattomaksi tai epätoivotuksi tietoturvatapahtumaksi, joka merkittävällä todennäköisyydellä vaarantaa yrityksen liiketoimintaoperaatioita ja uhkaa sen tietoturvaa. Tietoturvatapahtumalla tarkoitetaan sellaista järjestelmässä, verkossa tai palvelussa tunnistettua tapahtumaa, joka viittaa mahdolliseen tietoturvan rikkoutumiseen.

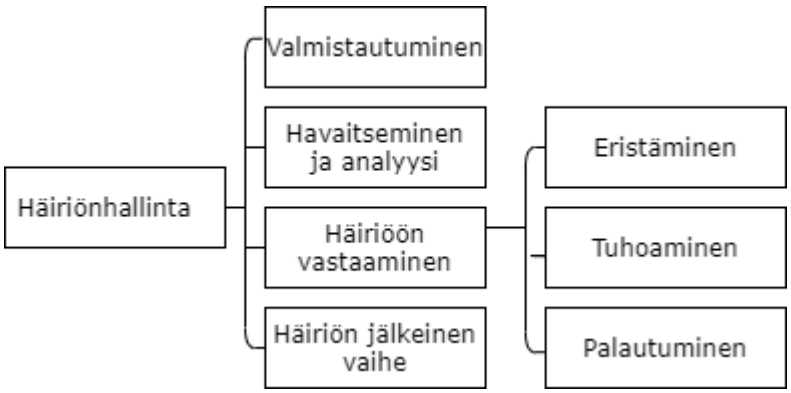
Edellä mainitut viralliset määritelmät ovat melko yleisluontoisia ja niiden yhteys muihin tietoturvaan liittyviin käsitteisiin jää melko epäselväksi. Myös NIST (2012) ohjeessa todetaan, että organisaation tulisi määritellä häiriön käsite organisaatiolle relevantissa kontekstissa. Käytetään edellä esiteltyjä määritelmiä ja ensimmäisessä alaluvussa esitettyjä uhan, haavoittuvuuden ja riskin käsitteitä tietoturvahäiriön määrittelyssä niin, että niiden väliset suhteet tulevat tämän tutkielman kannalta paremmin esille: Uhka on yrityksen resurssin tai voimavaran vaarantaja, joka käyttää hyväkseen resurssin haavoittuvuutta. Tämä uhan ja haavoittuvuuden yhdistelmä luo resurssiin liittyvän riskin, jota kuvataan resurssin luotettavuuden, eheyden tai saatavuuden vaarantumisen todennäköisyytenä ja vaarantumisesta aiheutuvina haittavaikutuksina. Riski on siis tämän päättelyn mukaan resurssin saatavuuden, eheyden tai luotettavuuden vaarantava tapahtumaskenaario. Kun tämä skenaario käytännössä toteutuu, syntyy tietoturvahäiriö. Tietoturvahäiriö on siis organisaation resurssin vaarantava realisoitunut tai suurella todennäköisyydellä realisoituva riski.

2.3.2 Häiriönhallinta organisaatiossa

Häiriönhallinta organisaation toimintona ja sen rajapinnat muihin organisaation toimintoihin voidaan hahmottaa häiriönhallinnan eri osakokonaisuuksiin liittyvien englanninkielisten termien, *incident handling* ja *incident response* kautta. Näistä *incident response* (IR) viittaa reaktiiviseen häiriöön vastaamiseen, joka alkaa, kun organisaation resurssin vaarantava häiriö havaitaan. IR prosessi pi-

tää sisällään häiriön eristämisen (containment), tuhoamisen (eradiction) ja häiriöstä palautumisen (recovery). IR on osa laajempaa proaktiivisen ja reaktiivisen häiriökäsittelyn, *incident handling*:n kokonaisuutta. Häiriönhallinnan yleinen malli pitää sisällään neljä vaihetta 1) valmistautuminen (preparation), 2) havaitseminen ja analysointi (detection and analysis), 3) häiriöön vastaaminen (incident response) ja 4) häiriön jälkeinen vaihe. (Rahman & Choo, 2015.) Nämä vaiheet pohjautuvat kahteen keskeiseen häiriönhallintamalliin/standardiin: NIST SP 800-61 ja ISO/IEC 27035. Häiriönhallinnan yleistä mallia käytetään laajasti häiriönhallinnan vaiheiden jaotteluun myös akateemisessa kirjallisuudessa. Vaiheiden nimityksissä on usein eroavaisuuksia ja vaiheiden määrä saattaa esitysten välillä vaihdella, mutta häiriönhallintaprosessin toiminnallinen sisältö on yhdenmukainen. (Ks. Ahmad ym., 2020; Mitropoulos, Patsos & Douligeris, 2006; Tøndel, Line & Jaatun, 2014.)

Akateemisessa kirjallisuudessa termillä *incident response* saatetaan myös viitata häiriönhallinnan kokonaisuuteen pelkän häiriöön vastaamisen sijaan. Joskus termin *incident handling* tilalla käytetään myös termiä *incident management,* jolla häiriönhallintaprosessiin viittaa esimerkiksi ITIL v3 viitekehys. Toisaalta esimerkiksi Alberts, Dorofee, Killcrece, Ruefle ja Zajicek (2004) viittaavat *incident management:lla* useiden palvelujen kokoelmaan, jossa *incident handling* on yksi palvelukokonaisuus. Muihin palveluihin lukeutuvat esimerkiksi haavoittuvuuksien hallinta ja artifaktien hallinta. Yhdenmukaisen termistön puuttuminen aiheutti tutkimusprosessin alussa lieviä epäselvyyksiä, mutta häiriönhallinnan käsite selkeytyi tämän tutkielman kontekstissa tarkoittamaan edellä esitettyä nelivaiheista proaktiivisen ja reaktiivisen toiminnan kokonaisuutta (ks. kuvio 1).



KUVIO 1 Häiriönhallinnan vaiheet (Rahman & Choo, 2015 mukaan)

Häiriönhallintaprosessissa toimivat usein yhteistyössä useat yrityksen toiminnot kuten riskien hallinta ja ISM (Ahmad ym., 2020). Usein häiriönhallinnan kolmas vaihe, eli häiriöön vastaaminen on organisaatiossa erityisen häiriönhallintaryhmän, CSIRT (Computer Security Response Team) vastuulla. Tiimin toiminta ja vastuualueet ovat organisaatiokohtaisia ja sen toiminta voi vaihdella ad hoc- tyyliin toteutetusta reaktiivisesta häiriöihin vastaamisesta ennakoivaan ja tarkasti organisoituun hierarkkiseen toimintaan, jossa se osallistuu myös häi-

riötilanteisiin valmistautumiseen. (Ahmad, Hadgkiss & Ruighaver, 2012; Ahmad ym., 2021.)

NIST (2012) esittää häiriönhallintaryhmälle kolme toteutusmallia. Ensimmäinen tapa rakentaa häiriönhallintaryhmä on keskitetty häiriönhallintaryhmä (Central Incident Response Team). Tässä mallissa yksi häiriönhallintaryhmä vastaa häiriönhallinnasta koko organisaatiossa. Malli on toimiva ratkaisu pienissä organisaatioissa, jotka ovat maantieteellisen sijaintinsa puolesta keskittyneitä. Toinen malli on jakautettu häiriönhallintaryhmä (Distributed Incident Response Teams). Organisaatiolla on useita häiriönhallintaryhmiä, joiden välillä vastuu on jaettu loogisten ja/tai fyysisten häiriönhallinta-alueiden välillä. Tämä malli toimii suurissa organisaatioissa, joiden toiminta ja IT-resurssit on maantieteellisesti hajautettu. Mallissa tulisi olla yksi muita ryhmiä hallinnoiva ryhmä, joka varmistaa ryhmien toiminnan johdonmukaisuuden ja yhteistyön toimivuuden. Kolmas esitetty malli on koordinoivan ryhmän (Coordinating Team) malli. Edellisen mallin tavoin organisaatiolla on useita häiriönhallintaryhmiä, mutta edellisestä mallista poiketen koordinoiva ryhmä on muiden ryhmien kanssa vertainen, eikä se ole johtohierarkiassa korkeammalla. Koordinoivan ryhmän tehtävänä on auttaa paikallisia ryhmiä.

Organisaation häiriönhallinta voi olla kokonaan organisaation oman henkilöstön toteuttamaa tai puoliksi tai kokonaan ulkoistettua. Häiriönhallintamallin ja ulkoistuksen tason valinta on organisaatiokohtaista ja riippuu monista seikoista, kuten henkilöstön osaamistasosta, häiriönhallinnan ajallisen saatavuuden tarpeesta ja eri toteutustapojen hyödyistä ja kustannuksista kyseiselle organisaatiolle. (NIST, 2012.)

Tiivistettynä edellä esitetyn perusteella tietoturvahäiriönhallinta organisaatiossa voidaan määritellä prosessiksi, jonka tarkoituksena on preventiivisin ja reaktiivisin toimin häiriönhallintaryhmän ja muiden tietoturvaan liittyvien ryhmien yhteistyöllä estää ja minimoida häiriön aiheuttama haitta organisaation resursseille ja voimavaroille ja niiden kautta organisaation toiminnalle.

2.4 Häiriönhallintamallit

Organisaation häiriönhallintatoiminnon suunnittelun ja toteuttamisen tueksi on tarjolla useita ohjeistuksia, standardeja ja parhaiden käytäntöjen kokoelmia. Näistä ISO/IEC 27035 -standardi ja NIST SP 800-61 -ohjeistus ovat kaksi keskeisintä ja käytetyintä (Tøndel ym., 2014). Kumpikin malli lähestyy häiriönhallintaa järjestelmällisesti ja proaktiivisesti sisältäen häiriöön valmistautumisen, siihen vastaamisen ja siitä oppimisen vaiheet. ISO/IEC 27035 -standardissa tämä prosessi on jaettu viiteen ja NIST SP 800-61 -mallissa neljään vaiheeseen. (Rahman & Choo, 2015.) Näiden kahden mallin lisäksi myös IT-palveluiden hallintaan laajasti käytetty ITIL -viitekehys tarjoaa organisaatiolle ohjeistusta häiriönhallinnan toteuttamiseen. Häiriönhallinta on ITIL:ssä yksi viidestä palvelutoimintaprosessista (service operation process), jotka kuvataan palvelutoiminto-

jen kirjassa. ITIL:n mukainen häiriönhallintaprosessi keskittyy palvelutason mahdollisimman nopeaan palauttamiseen eikä yksinään sisällä häiriöihin valmistautumista ja niistä oppimista. Häiriöiden tarkempi tutkinta ja juurisyiden selvittäminen tapahtuu yhteistyössä muiden prosessien, kuten ongelmien hallinnan ja tapahtumien hallinnan kanssa. (ITIL, 2011.)

Tutustutaan tarkemmin NIST SP 800-61 ohjeistuksen mukaiseen häiriönhallintamalliin. Ensimmäisessä vaiheessa, valmistautumisessa ennaltaehkäistään häiriöiden syntymistä ottamalla käyttöön riskianalyysin perusteella valittuja turvakontrolleja. Valmistautumisen aikana organisaation häiriönhallintakyvykkyys asetetaan riittävään häiriönhallintavalmiuteen, jotta häiriöihin vastaaminen onnistuu luotettavasti tositilanteessa. Häiriönhallintavalmiuden valmisteluun liittyvät asiat jaetaan neljään kategoriaan: viestinnän ja toimitilojen valmistelu, häiriöiden analysointiin liittyvän laitteiston ja ohjelmistojen valmistelu, häiriöanalyysin resurssien valmistelu ja häiriöiden lievittämiseen liittyvien ohjelmistojen valmistelu. Kun häiriönhallintavalmius on varmistettu, voidaan aloittaa häiriötilanteita ennaltaehkäisevien toimien suunnittelu ja toimeenpano. Ennaltaehkäisevät suojauskontrollit vähentävät häiriötilanteiden määrää ja estävät häiriönhallintaryhmän ylikuormittumista. Ne pitävät huolen siitä, että jokainen riski ei eskaloidu responsiivisia häiriönhallintatoimenpiteitä vaativaksi häiriöksi. Pääasiallisia suojauskontrolleja ovat esimerkiksi riskien arviointi, palvelinten turvaaminen, tietoverkkojen turvaaminen, haittaohjelmilta suojautuminen ja käyttäjien tietoturvakoulutus. (NIST, 2012.)

Häiriönhallintamallin toisen vaiheen, havaitsemisen ja analysoinnin tarkoituksena on tunnistaa ennakoivia merkkejä tulevista häiriötilanteista ja indikaattoreita parhaillaan käynnissä olevista häiriöistä. Analysoinnin avulla lukuisista vääristä signaaleista tunnistetaan todellisiin häiriöihin liittyvät merkit ja indikaattorit. Havainnoinnin lähteinä käytetään pääasiassa erilaisia tunkeutumisen havainnointijärjestelmiä, viruksentorjuntaohjelmistoja, verkon laitteiden lokitietoja, järjestelmien lokitietoja jne. Analysoinnin helpottamiseen esitetään esimerkiksi seuraavanlaisia suosituksia: häiriönhallintaryhmän tulisi tuntea järjestelmien normaali toiminta, jotta poikkeavuuksien erottaminen ja niiden yhdistäminen mahdollisiin häiriöihin olisi helpompaa, palvelinten kellot tulisi synkronoida, jotta tapahtumien korrelointi olisi helpompaa. Jonkinlaisen häiriötietokannan ylläpitäminen helpottaa häiriöiden tunnistamista ja erilaisten merkkien yhdistämistä tietynlaisiin häiriöihin. (NIST, 2012.)

Häiriöt tulisi myös dokumentoida. Häiriöistä tulisi kerätä ainakin seuraavanlaista tietoa: häiriön nykyinen status, yhteenveto, häiriöön liittyvät indikaattorit, häiriöön liittyvät toiset häiriöt, häiriönhallintaryhmän toteuttamat toimet, vaikutusten arviointi, häiriötutkinnassa löydetty todistusaineisto, liittyvien sidosryhmien yhteystiedot, kommentointi, seuraavaksi tehtävät asiat. (NIST, 2012.)

Yksi häiriönhallintaprosessin kriittisimmistä vaiheista on häiriöiden oikeanlainen priorisointi. Keskeisiä priorisoinnin pohjana käytettäviä tekijöitä ovat häiriön toiminnalliset vaikutukset järjestelmiin, häiriön vaikutukset tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen ja häiriöstä palautumisen hanka-

luus. Toiminnallisten- ja tietoon kohdistuvien vaikutusten yhteisvaikutus määrittää häiriön liiketoiminnalliset vaikutukset. Häiriöstä palautumisen hankaluus auttaa määrittämään oikeanlaisen tavan vastata häiriöön. Helposti korjattava häiriö, jolla on merkittävät vaikutukset järjestelmien toimintaan, on esimerkki häiriöstä, johon tulee vastata nopeasti. Joissakin tapauksissa palautuminen saattaa vaatia suorien ja nopeiden toimenpiteiden lisäksi tarkempaa strategisen tason suunnittelua. Tiivistettynä häiriöihin vastaamista tulisi priorisoida häiriön liiketoimintavaikutusten ja vastaamisen vaikeusasteen perusteella. (NIST, 2012.)

Häiriön analysoinnin ja priorisoinnin jälkeen häiriönhallintaryhmän tulee viestiä asiaankuuluville sidosryhmille, jotta häiriöön vastaamisen aikana eri toimijat tietävät vastuunsa ja roolinsa. Ajan tasalla pidettäviä sidosryhmiä ovat esimerkiksi tietohallintopäällikkö, tietoturvapäällikkö, muut häiriönhallintaryhmät, henkilöstöhallinto, virkavalta, organisaation lakitoiminnot ja julkisesta tiedotuksesta vastaavat ryhmät ja henkilöt. (NIST, 2012.)

Häiriönhallinnan kolmas vaihe koostuu häiriön eristämisestä, tuhoamisesta ja häiriöstä palautumisesta. Häiriön eristämisessä on kyse häiriön aiheuttaman vahingon ja sen hallintaan käytettyjen resurssien rajaamisesta siksi aikaa, kun asianmukainen hallintastrategia kehitetään. Strategian valintaan vaikuttaa häiriön luonne. Esimerkkejä strategian valintaan vaikuttavista tekijöistä ovat tarve todistusaineiston turvaamiselle, palvelujen saatavuuden vaarantuminen, strategisten ratkaisujen pysyvyys ja strategian toteuttamiseen kuluva aika ja resurssit. Hyökkääjän toimintaa voidaan eristämisen jälkeen myös tarkkailla todistusaineiston keräämistä varten. Häiriönhallintaprosessin aikana tapahtuva todistusaineiston kerääminen auttaa paitsi häiriötilanteen ratkaisemisessa, myös mahdollisessa oikeusprosessissa. Jälkimmäisen kannalta on hyvä huolehtia siitä, että todistusaineiston kerääminen toteutetaan siten, että sitä voidaan käyttää hyväksi mahdollisessa oikeudenkäynnissä. Todistusaineiston keräämisen lisäksi voi olla aiheellista pyrkiä selvittämään tarkempia tietoja häiriön takana olevasta hyökkääjästä. Menetelmiä tällaisten tietojen keräämiseen ovat esimerkiksi hyökkääjän IP-osoitteen validointi, julkisesti ylläpidettyjen häiriötietokantojen tarkastelu ja hyökkääjien mahdollisten viestintäkanavien tunnistaminen ja kuuntelu. (NIST, 2012.)

Häiriön eristämisen jälkeen voi olla tarpeen tuhota sen jäänteet, jotta organisaation tietotekninen toimintaympäristö saadaan turvattua. Esimerkiksi vaarantuneet käyttäjätilit ja haittaohjelmien osat on aiheellista poistaa. Myös hyökkäyksessä hyväksikäytetyt haavoittuvuudet tulee paikata. Toimintaympäristön turvaamisen jälkeen häiriön kohteena olleet järjestelmät palautetaan normaalille toimintatasolle. Niiden asianmukainen toiminta varmistetaan ja tarpeen mukaan palautetaan viimeisimmät vakaat varmuuskopiot tai rakennetaan järjestelmät uusiksi. Järjestelmien toiminnan palauttamiseen liittyviä toimintoja voivat olla myös vaarantuneiden tiedostojen korvaaminen, palomuurien uudelleenkonfigurointi, salasanojen vaihtaminen ja järjestelmien korjauspäivitykset. (NIST, 2012.)

Häiriön jälkeinen toiminta käsittää edellisten vaiheiden arvioimisen ja prosessin aikana opittujen asioiden sekä tehtyjen virheiden yhteen vetämisen

tapaamisten ja kokousten muodossa. Tapaamisiin tulisi osallistua henkilöstöä yli organisaation sisäisten tiimirajojen siten, että häiriötilanteesta opitut asiat saadaan viestittyä kaikille niitä tarvitseville sisäisille sidosryhmille. Häiriönhallintaprosessi ja sen aikana tehdyt päätökset tulisi dokumentoida arviointia varten, jotta niitä voitaisiin käyttää uusien häiriönhallintaryhmän jäsenten koulutukseen ja prosessin virheiden tunnistamiseen. Tietoturvakäytäntöjen ja ohjeistusten arvioiminen ja parantaminen tulisikin olla yksi häiriön jälkeisen toiminnan keskeisistä tavoitteista. (NIST, 2012.)

Häiriönhallinnasta ja häiriöistä tulisi kerätä järjestelmällisesti tietoa jonkinlaiseen häiriötietokantaan. Tiedon analysointi voi paljastaa muuten vaikeasti havaittavissa olevia haavoittuvuuksia ja mahdollisia uhkia. Tiedon perusteella voidaan myös mitata häiriönhallinnan tehokkuutta ja tunnistaa muuttuvia uhkatrendejä. Analysoinnin tuloksia voidaan hyödyntää myös häiriönhallinnan parantamisessa käyttämällä niitä riskien arvioinnissa ja sitä kautta uusien suojauskontrollien käyttöönotossa. Kerättävällä häiriötiedolla tulisi olla jokin käyttötarkoitus ja rooli tietoturvan tason mittaamisessa ja parantamisessa. Esimerkkejä hyödyllisistä seurattavista suureista ovat häiriön selvittämiseen käytetty aika, häiriön objektiivinen ja subjektiivinen arviointi ja käsiteltyjen häiriöiden kokonaismäärä tietyllä aikavälillä. (NIST, 2012.)

3 ORGANISAATION OPPIMINEN JA HÄIRIÖNHALLINTA

Yrityksen kohtaamat tietoturvauhat ja hyökkäykset kehittyvät jatkuvasti. Uusien teknologioiden myötä kyberrikollisten hyökkäyspinta-ala laajenee ja syntyy uusia hyväksikäytettäviä haavoittuvuuksia. Tehokkaan oppimisprosessin avulla yritys pystyy mukauttamaan häiriönhallinta- ja tietoturvatoimintonsa vastaamaan muuttuvan ympäristön asettamia vaatimuksia.

Tässä luvussa perehdytään ensin organisaation oppimisen käsitteeseen ja esitellään organisaation oppimisen teoria. Tämän jälkeen tarkastellaan organisaation oppimisen suhdetta häiriönhallintatoimintoon. Perehdytään tutkimukseen organisaation oppimisen tarjoamista hyödyistä ja sen haasteista häiriönhallinnassa ja kerätään tutkimuskirjallisuudesta suosituksia ja esitettyjä hyötyjä oppimismenetelmien käytöstä osana organisaation häiriönhallintaa.

3.1 Organisaation oppiminen

Organisaation oppiminen tutkimusalueena tutkii organisaation kykyä kehittää tietoa ja rutiineja toimintansa ohjaamiseen. Organisaation oppiminen on prosessi, jonka avulla organisaatio pyrkii sisällyttämään ja levittämään tietoa ja kokemusta sen toimintaan ja päivittämään ja vaihtamaan organisaation muistissa olevaa tietoa. Oppimisen tavoitteena on korjata virheitä, kehittää organisaation tietämyskantaa, saada kilpailuetua innovaation kautta ja lyhentää päätöksentekoon vaadittavaa aikaa. Organisaation halukkuus oppia ja sisällyttää uutta tietoa organisaation muistiin johtaa ketterämpään toimimiseen sen kohdatessa uusia haasteita ja pienentää päätöksenteossa ja toiminnassa tehtyjä virheitä. (Shedden, Ahmad & Ruighaver, 2010.)

Organisaation oppimista käsittelevä tutkimus ja kirjallisuus on runsasta ja tutkijat ovat esittäneet useita näkemyksiä organisaation oppimisen määritelmälle (Wang & Ahmed, 2003). Wang ja Ahmed (2003) tunnistivat organisaation oppimista käsittelevästä kirjallisuudesta viisi suuntausta, jotka painottivat eri asi-

oiden tärkeyttä oppimisen tarkastelussa. Suuntaukset olivat: kollektiivisen yksilöoppimisen suuntaus, prosessi- ja systeemisuuntaus, kulttuurin ja metaforan suuntaus, tiedon hallinnan suuntaus ja viimeisenä jatkuvan parantamisen ja asteittaisen innovaation suuntaus.

Kollektiivisen yksilöoppimisen suuntaus korostaa yksilön roolia oppimisessa. Organisaation oppimisen nähdään tapahtuvan yksilöllisen oppimisen kautta yksilöiden toimiessa organisaation oppimisen ”agentteina”. Yksilöoppimisen rinnalla tapahtuu kollektiivista oppimista ja organisaation oppiminen nähdään näiden oppimisten yhtesivaikutuksena. (Wang & Ahmed, 2003.) Yksilöoppimisen suuntausta edustaa esimerkiksi Argyriksen ja Schönin (1978) näkemys organisaation oppimisesta.

Prosessi- ja systeemisuuntauksessa organisaatio nähdään oppimissysteeminä. Tutkimus keskittyy yksilötason sijaan organisaatioon kokonaisuutena ja organisaatio nähdään tietoa käsittelevänä systeeminä, joka kerää, jakaa, tulkitsee ja tallentaa tietoa. Oppiminen nähdään organisaatiossa kolmesta näkökulmasta: kykynä mukautua ympäristöön, oppimisena organisaation jäseniltä ja osallistumisena laajemman yhteisön oppimiseen. Huberin (1991) näkemys organisaation oppimisesta edustaa systeemisuuntausta. (Wang & Ahmed, 2003.)

Kulttuuri- ja metaforasuuntauksen keskiössä on organisaatiokulttuurin pitäminen keskeisenä edellytyksenä organisaation oppimiselle. Kulttuuri on organisaation järkeilymekanismi, joka ohjaa ja määrittää sen arvoja, asenteita ja toimintaa. Suuntauksen mukaan organisaatiokulttuurin täytyy edistää kaikkien jäsentensä osallistamista jatkuvaan oppimisen tuottamiseen, säilömiseen ja hyödyntämiseen. (Wang & Ahmed, 2003.)

Tiedon hallinnan suuntauksessa huomio on organisaation muistissa ja tietämyskannassa. Organisaation muisti on oppimisen perusta ja se huolehtii organisaation tietämyskannan ylläpitämisestä, toimii perustana tiedon kerryttämiselle ja luomiselle ja heijastaa organisaation tiedonkäsittelykykyä. Tiedon hallinnan pääasiallisena tehtävänä nähdään yksilöiden ja organisaation välisen vuorovaikutuksen ja tietämyksen vahvistamisen mahdollistavan oppimisympäristön luominen. (Wang & Ahmed, 2003.)

Viimeinen organisaation oppimisen suuntaus on jatkuvan parantamisen ja asteittaisen innovaation suuntaus. Nimensä mukaisesti suuntauksessa oppivan organisaation tulisi määrätietoisesti pyrkiä yksilöiden oppimisen helpottamiseen jatkuvan muutoksen aikaansaamiseksi. Organisaation tulisi jatkuvasti laajentaa jäsentensä kykyä tuottaa haluamiaan tuloksia ja sen tulisi vaalia uusien ajattelutapojen luomista. Organisaation jäsenten tulisi jatkuvasti voida oppia oppimaan toisiltaan. Tällaisen jatkuvan parantamisen kautta tapahtuvan oppimisen nähdään suuntauksessa johtavan asteittaiseen innovointiin. (Wang & Ahmed, 2003.)

Tutkimuksessa tunnistetut suuntaukset eivät ole toisiaan poissulkevia, vaan osittain samoja näkemyksiä jakavia erilaisia näkökulmia organisaation oppimisen konseptiin. Tehokkaan oppimisen toteuttaminen organisaatiossa vaatii tilanteeseen ja ympäristöön sopivan sekoituksen eri näkökulmien tarjoamista periaatteista. (Wang & Ahmed, 2003.) Tutustutaan seuraavaksi tarkem-

min Argyriksen ja Schönin (1978) ja Huberin (1991) näkemyksiin organisaation oppimisesta.

Organisationaalisen oppimisen tutkimuksen juuret ovat Argyriksen (1976) ja Argyriksen ja Schönin (1978) esittelemissä yksi- (single-loop) ja kaksikehäisen (double loop) oppimisen malleissa, jotka ovat vahvasti esillä ja tunnustettuja myös nykypäivän organisaation oppimisen tutkimuksessa. Argyris ja Schön (1996) tarkastelevat organisaation oppimista toimintatieteen näkökulmasta. Heidän näkemyksensä perustuu organisaation omaksutun toimintalogiikan (espoused theory) ja käytännön toimintalogiikan (theory-in-use) sekä organisaation toiminnan taustalla vaikuttavien normien käsitteisiin. (Argyris & Schön, 1996, s. 13-14.)

Organisaation toimintalogiikka/teoria on käsite, jolla viitataan toimintaan ja päätöksiin, jotka perustuvat organisaation tietämykseen tallennettuihin toimintamalleihin, joita yksilöt toteuttavat organisaation nimissä heille jaettujen valtuutusten mahdollistamana. Yksilöt toimivat ja tekevät päätöksiä organisaation nimissä, kun toimintaa ja päätöksiä sekä näihin valtuutettuja ihmisiä hallinnoidaan organisaation yhteisten sääntöjen kautta. (Argyris & Schön, 1996, s. 8-13.)

Omaksuttu toimintalogiikka on organisaation käytännöissä ja dokumenteissa virallisesti tunnustettu toimintalogiikka, kun taas käytännön toimintalogiikka on organisaation toimintaa tarkastelemalla saatu kuva sen toiminnasta. Toisin sanoen se mitä organisaatio käytännössä tekee. (Argyris & Schön, 1996, s. 13-14.)

Yksikehäinen ja kaksikehäinen oppiminen perustuvat Argyriksen ja Schönin (1996, s. 20-22) mukaan organisaation käytännön toimintalogiikan jatkuvaan arvioimiseen ja muuttamiseen. Toteuttaessaan organisaation käytännön toimintalogiikkaa organisaation jäsenet arvioivat toiminnan odotettuja tuloksia ja toteutuneita tuloksia. Tulos joko vahvistaa tai kumoaa käytännön toimintalogiikan. Mikäli tulos eroaa toimintalogiikan odotetusta tuloksesta pyrkivät jäsenet löytämään ristiriidan syyn tai ”virheen” toimintalogiikassa ja korjaamaan sen. Argyriksen ja Schönin (1996, s. 16-17) mukaan organisaation oppimista tapahtuu kuitenkin vain, mikäli tieto virheenkorjausprosessista koodataan kuvina ja malleina käytännön toimintalogiikasta organisaation yhteiseen muistiin, jonka mukaan organisaation jäsenet toimivat.

Huber (1991) tarkastelee ja arvioi tutkimuksessaan organisaation oppimiseen liittyvää neljää oppimisen konstruktiota: Suoraa tiedon keräämistä, tiedon leviämistä, tiedon tulkintaa ja organisaation muistia. Tutkimuksessa esitetyn määritelmän mukaan organisaation oppiminen kuvataan neljän ominaisuuden: olemassaolon (existence), leveyden (breadth), yksityiskohtaisuuden (elaborateness) ja perusteellisuuden (thoroughness) kautta. Jokaiseen ominaisuuteeen liittyy oppimista kuvaava oletus, joiden yhteenvetona oppiminen määritellään. Nämä oletukset ovat (järjestyksessä edellä mainittujen ominaisuuksien kanssa): Organisaatio oppii, mikäli joku sen yksiköistä saa haltuunsa tietoa, jonka se tunnistaa hyödylliseksi organisaatiolle. Organisaatio oppii sitä enemmän, mitä useampi sen yksiköistä kerää tietoa ja tunnistaa sen hyödylliseksi. Mitä moni-

puolisempaa tiedon tulkinta on, sitä enemmän organisaatio oppii ja organisaatio oppii sitä enemmän, mitä useampi organisaation yksikkö kehittää yhtenäisen ymmärryksen erilaisista tulkinnoista. (Huber, 1991.)

Organisaatio oppii siis yksiköidensä kautta keräten itselleen hyödyllistä tietoa ja kehittäen erilaisista tulkinnoista organisaation yhteistä ymmärrystä.

Tämän oppimisen määritelmän kautta Huber (1991) arvioi edellä mainittuja neljää oppimisen konstruktiota. Suora tiedon kerääminen tapahtuu esimerkiksi erilaisten kyselyiden, tuotekehitysprosessin tai kilpailuanalyysin kautta. Tiedon leviäminen edistää organisaation oppimista organisaation eri yksiköiden kehittäessä uutta tietoa toisiltaan saaman tiedon perusteella. Organisaation eri yksiköt tekevät tiedosta erilaisia tulkintoja ja näin ollen edistävät oppimista. Organisaation muistissa yksiköiden tulkinnat kerätään talteen yhteisön kollektiiviseen tietovarastoon.

Huber (1991) ja Argyris & Schön (1996) näkemyksille yhteistä on, että molemmat näkevät organisaation entiteettinä, joka oppii jäsentensä omaksuessa ja tulkitessa uutta tietoa lopulta tallentaen sen organisaation muistiin yhteiseksi ymmärrykseksi. Argyris ja Schön (1996) näkevät tämän prosessin organisaation käytännön toimintalogiikan muutoksena ja kehittymisenä Yksi- ja kaksikehäisen oppimisen kautta. Heidän näkemyksensä painottaa myös yksilön roolia organisaation oppimisen agenttina.

3.2 Häiriöoppiminen

Organisaation häiriönhallintaprosessiin osallistuvat ryhmät ja erityisesti häiriönhallintatiimi IRT (Incident Response Team) käsittelevät häiriönhallintaprosessin aikana arvokasta tietoturvahäiriöihin ja -hyökkäyksiin liittyvää tietoa, jonka keräämisestä ja hyödyntämisestä on hyötyä organisaation tietoturvan parantamisessa. (Ahmad ym., 2015) Tähän häiriöön liittyvän tiedon keräämiseen ja jakamiseen organisaation muille yksiköille analysointia varten viitataan useissa tutkimuksissa termillä häiriöoppiminen (incident learning, post-incident learning) (Shedden, Ahmad & Ruighaver, 2010; Ahmad ym., 2012).

Häiriöoppiminen häiriönhallinnan ja tietoturvan tutkimussuuntauksena on yleisesti jäänyt vähäiselle huomiolle verrattuna tutkimukseen, joka keskittyy häiriönhallintaan teknisestä näkökulmasta (Shedden ym., 2010) Organisaatioiden häiriönhallintatoiminnon pääasiallinen tavoite on usein liiketoiminnan jatkuvuuden turvaaminen ja häiriöiden nopea ja kustannustehokas selvittäminen liiketoiminnalle aiheutuvan haitan minimoimiseksi, jolloin häiriöoppimisen saama huomio jää yleensä vähäiseksi. (Ahmad ym. 2015; Ahmad ym., 2012)

Häiriöoppiminen tapahtuu yleisten häiriönhallintamallien viimeisessä, häiriön jälkeisessä (lessons learned/post-incident) vaiheessa. Häiriöoppimista toteutetaan yleisesti dokumentoimalla häiriönhallintaprosessin aikana häiriöstä kerätty tieto virallisen raportin muotoon, analysoimalla kerättyä tietoa, ja viestimällä tätä tietoa johdolle kokouksien ja esitelmien muodossa (Shedden ym., 2010). Ahmad ym. (2015) mukaan häiriönhallinnan parhaiden käytäntöjen mal-

lit eivät kuitenkaan tunnista tai korosta tarvetta käyttää tätä tietoa laajemmin organisaation tietoturvan ja tietoturvakäytäntöjen arviointiin ja kehittämiseen. Mahdollisuudet tietoturvan parantamiseen ovat heidän mukaansa heikot ilman tällaista laajempaa oppimisen mallia.

Häiriöoppimiseen liittyvät keskeisesti aiemmin mainitut yksi- ja kaksikehäisen oppimisen käsitteet. Näistä yksikehäinen oppiminen tarkoittaa yksinkertaista virheenkorjausta, jossa poikkeukset organisaation tavoitteista, käytännöistä ja rutiineista korjataan. Yksikehäinen oppiminen häiriönhallinnassa liittyy turvatoimien suoraan muuttamiseen ja käytäntöjen ja toimien muokkaamiseen yksinkertaisen virheenkorjauksen muodossa. Kaksikehäinen oppiminen sisältää käytäntöjä ja strategiaa ohjaavien normien kyseenalaistamisen. Kaksikehäiseen häiriöoppimiseen sisältyy tietoturvakäytäntöjen ja toimien taustalla olevan hallinnoinnin ja yleisten olettamusten arvioiminen ja muuttaminen osana ongelmanratkaisua. (Ahmad ym., 2020; Baskerville, Spagnoletti & Kim, 2014.)

Baskerville ym. (2014) esittävät yritysten häiriöpainotteisten tietoturvastrategioiden koostuvan ennalta-ehkäisevistä ja häiriöön reagoivista suojaustoimista. He nimittävät näitä kahta lähestymistapaa organisaation tietoturvaan prevetiiviseksi (preventive) ja responsiiviseksi (responsive) paradigmaksi, joihin kuuluvista suojaustoimista organisaatio koostaa tietoturvastrategiansa. Heidän mukaansa organisaation toimintaympäristö määrittää sopivan suhteen preventiivisille ja responsiivisille toimille yrityksen tietoturvastrategiassa. Yleisesti ottaen preventiivinen paradigma ja siihen liittyvän yksikehäisen oppimisen tarjoama lähestymistapa tietoturvaan toimii samankaltaisina toistuvien ja vähemmän kehittyneiden, yksinkertaisten tietoturvahyökkäysten torjunnassa, kun taas responsiivisesti painottunut strategia ja siihen kuuluva kaksikehäinen oppiminen toimivat paremmin muuttuvassa ja ennalta arvaamattomassa uhkaympäristössä, jossa tietoturvahyökkäykset ovat yhä pidemmälle kehittyneitä ja kohdistuvat organisaation yksilöllisten haavoittuvuuksien hyväksikäyttöön. (Baskerville ym., 2014.)

4 ORGANISAATION HÄIRIÖOPPIMISEN ESTEET JA HÄIRIÖOPPIMISEN PARANTAMINEN

Tässä luvussa tutustutaan häiriöoppimista käsitteleviin tutkimuksiin ja selvitetään tutkimusten perusteella keskeiset organisaation häiriöoppimiseen liittyvät ongelmat sekä mallit organisaation häiriöoppimiskyvykkyyden parantamiseksi.

Kirjallisuuskatsauksessa löydettiin viisi häiriöoppimista käsittelevää tutkimusta, jotka valittiin tarkempaan käsittelyyn seuraavien kriteerien perusteella: tutkimuksen piti tarkastella organisaation tietoturvahäiriönhallintaprosessia organisaation oppimisen teoriaan pohjautuvan viitekehyksen kautta ja tutkimuksen tuli käsitellä häiriöoppimisen haasteita ja/tai esittää suosituksia häiriöoppimisen kehittämiseen organisaatiossa. Häiriöoppimisen haasteita käsittelevät case-tutkimukset, ja niissä tunnistetut häiriöoppimisen haasteet on kuvattu taulukossa 1 (taulukko 1). Kirjallisuuskatsauksessa löydettiin kolme häiriöoppimismallia, jotka tarjoavat oman ratkaisunsa häiriöoppimisen toteuttamiseen vastaten myös havaittuihin häiriöoppimisongelmiin.

4.1 Häiriöoppimisen esteet

Esitellään seuraavaksi neljä case-tutkimusta, joissa tutkittiin häiriöoppimista neljässä eri organisaatiossa. Huomionarvoista on, että kaikkien yritysten häiriöoppimisessa esiintyi hyvin samankaltaisia ongelmia. Tutkimuksissa havaittuja yrityksille yhteisiä häiriöoppimista estäviä ongelmia oli pääpiirteissään kolme:

1. Virallisten viestintäkäytäntöjen puuttuminen häiriönhallintaryhmän ja tietoturvan hallinnoinnin välillä. Häiriötiedon tehoton viestintä häiriönhallintaryhmän ulkopuoliseen käyttöön.
2. Häiriötutkinnan toteuttaminen ja häiriöraportin laatiminen vain korkean prioriteetin häiriöistä.

3. Teknisen näkökulman painottuminen häiriötutkinnassa ja -raportissa. Tutkinnan tulosten hyödyntämisen rajoittuminen häiriönhallintaprosessin tehostamiseen teknisestä näkökulmasta.

TAULUKKO 1 Tutkimuksissa tunnistetut häiriöoppimisen ongelmat

	Ahmad ym. 2012	**Ahmad ym. 2015**	**Webb ym. 2017**	**He & Johnson. 2017**
Kommunikaation ja viestinnän ongelmat	Virallisten häiriötiedon viestintäkäytäntöjen puuttuminen häiriönhallinnan ja tietoturvan hallinnoinnin ja riskienhallinnan sekä käytäntöjen laadinnan väliltä.	Virallisten häiriötiedon viestintäkäytäntöjen puuttuminen häiriönhallinnan ulkopuolisille sidosryhmille. (Häiriönhallinnan koordinaatioryhmä kuitenkin kommunikoi tietoturvan hallinnoinnin kanssa häiriön jälkeisten kokousten ja raportin muodossa)	Virallisten häiriötiedon viestintäkäytäntöjen puuttuminen häiriönhallinnan ulkopuolisille sidosryhmille.	Tekninen henkilöstö piti osaston sisäisissä tapaamisissa esitelmiä häiriöistä, mutta ne olivat vaikeaselkoisia muulle henkilöstölle. Raporttien hankala saatavuus häiriönhallinnan ulkopuolisille osastoille.
Häiriötutkinnan ja raportoinnin ongelmat (matalan prioriteetin häiriöt)	Ei juurisyyanalyysiä. Ainoa virallinen käytäntö on teknisten statistiikkaraporttien laatiminen johdolle.	Ei virallisia käytäntöjä, raporttia tai juurisyyanalyysiä.	Ei virallisia käytäntöjä, raporttia tai juurisyyanalyysiä.	Ei virallisia käytäntöjä, raporttia tai juurisyyanalyysiä.
Häiriötutkinnan ja raportoinnin ongelmat (korkean prioriteetin häiriöt)	Riskienhallinnan ja liiketoiminnan henkilöstön sulkeminen ulkopuolelle ensimmäisistä häiriön jälkeisistä kokouksista.	Ensimmäiseen häiriön jälkeiseen tapaamiseen osallistuu vain häiriönhallintaryhmä. Riskienhallinnan ja liiketoiminnan henkilöstö suljetaan ulkopuolelle.	Ensimmäiseen häiriön jälkeiseen tapaamiseen osallistuu vain häiriönhallintaryhmä. Muut sidosryhmät suljetaan ulkopuolelle.	Ei mainintaa. Sairaalahenkilökunta osallistui häiriötutkintaan.

(Jatkuu)

Taulukko 1 (jatkuu)

Häiriötiedon hyödyntämiseen ja oppimiseen liittyvät ongelmat (matalan prioriteetin häiriöt)	Kerätty tieto lähes täysin teknistä. Ainoa virallinen kerätty tieto on merkinnät häiriönkirjausjärjestelmään. Häiriöistä opitaan epävirallisilla menetelmillä häiriönhallintatiimin sisällä.	Merkintä selvitetystä häiriöstä häiriönkirjausjärjestelmään. Ei virallisia menettelyjä häiriötiedon hyödyntämiseen oppimisessa. Keskittyminen palvelujen nopeaan palauttamiseen.	Tietoa kerätään ainoastaan häiriökirjausjärjestelmään. Ei merkkejä häiriötiedon hyödyntämisestä oppimisessa. Keskittyminen palvelujen nopeaan palauttamiseen.	Ei virallisia menetelmiä tiedon keräämiseen tai hallintaan. Jonkin verran henkilöstön omaaloitteisia muistiinpanoja. Ei virallisia menettelyjä häiriötiedon hyödyntämiseen oppimisessa. Keskittyminen palvelujen nopeaan palauttamiseen.
Häiriötiedon hyödyntämiseen ja oppimiseen liittyvät ongelmat (korkean prioriteetin häiriöt)	Oppimisen rajoittuminen häiriönhallintaprosessiin. Tietoturvariskienhallinnan ja käytänteiden laadinnan jääminen oppimisen ulkopuolelle.	Järjestelmällisten ja virallisten häiriötiedon hyödyntämiskäytäntöjen puuttuminen kokonaisvaltaisen tietoturvan parantamiseksi. Häiriöraportteja ei välitetä automaattisesti niihin liittyville sidosryhmille. Oppiminen keskittyy häiriönhallinnan tekniseen parantamiseen.	Häiriöraportin ja tutkinnan tarkoituksena parantaa vain häiriönhallintaprosessia lähinnä teknisestä näkökulmasta. Häiriötiedon käyttämisestä tietoturvan kokonaisvaltaiseen parantamiseen virallisten käytäntöjen kautta ei ollut viitteitä. Keskittyminen palvelujen nopeaan palauttamiseen.	Häiriötietoa ja raportteja ei käytetty järjestelmälliseen oppimiseen ja tietoturvan parantamiseen. Raporteissa ei esitetty toimia tietoturvatoimenpiteiden parantamiseen.

4.1.1 Ensimmäinen case-tutkimus

Ahmad ym. (2012) case-tutkimuksen kohteena oli suuri kansainvälinen finanssialan yritys, johon tutkimuksessa viitattiin nimellä FinanceOrg. FinanceOrg työllisti yli 20 000 työntekijää ja sillä oli toimipisteitä neljällä eri mantereella. Yrityksen häiriönhallinnasta vastasi kaksi häiriönhallintaryhmää: NIRT (Network Incident Response Team) ja HIRCT (High-impact Incident Response Coordination Team). NIRT oli vastuussa yrityksen globaalin ydinverkon suojaamisesta preventiivisin ja responsiivisin keinoin. NIRT osallistui sekä korkean, että matalan tason häiriöihin vastaamiseen ja sen toiminta perustui ITIL ja ISO

17799 viitekehyksiin. HIRCT vastasi häiriönhallinnan koordinoinnista korkean tason häiriöihin vastaamisen aikana. HIRCT hallinnoi korkean tason häiriöihin vastaamista viestien NIRT:n ja muiden oleellisten sidosryhmien kanssa häiriön aikana. HIRCT:n vastuulla oli myös häiriöraporttien laatiminen korkean tason häiriöistä.

Yrityksen häiriönhallinta oli yleisesti ottaen kypsää ja se noudatti tarkasti alan keskeisiä standardeja. Erityisesti matalan prioriteetin häiriöihin vastaaminen on tehokasta. Tutkimuksessa tunnistettiin kuitenkin useita ongelmia liittyen häiriötiedon hyödyntämiseen tietoturvan parantamisessa.

Yrityksestä puuttui viralliset käytännöt häiriötiedon ja raporttien jakamiseen sisäisten sidosryhmien käyttöön. Tiedonkulku oli siiloutunutta, eikä häiriötieto siirtynyt tehokkaasti häiriönhallintaryhmän sisältä organisaation tietoturvan kokonaisvaltaiseen kehittämiseen. Tutkimuksessa tunnistettu häiriöoppiminen liittyikin vahvasti itse häiriönhallintaprosessin kehittämiseen.

Häiriön jälkeisissä kokouksissa ja tutkinnassa pääpaino oli teknisessä oppimisessa käytäntöjen ja riskien arvioimisen sijaan. Tekninen henkilökunta oli mukana kaikissa tapaamisissa, mutta liiketoiminnan ja riskienhallinnan kanssa työskentelevä henkilöstö jätettiin pois varsinkin ensimmäisistä tapaamisista. Matalan tason häiriöitä ei tutkittu, eikä niiden jälkitoimenpiteisiin kuulunut raportin laadintaa tai kokouksia. Matalan tason häiriöistä viestittiin johdolle häiriökirjausjärjestelmän teknisillä statistiikkaraporteilla. (Ahmad ym., 2012.)

4.1.2 Toinen case-tutkimus

Ahmad ym. (2015) toteuttaman tutkimuksen tulokset olivat hyvin samankaltaisia edellä kuvaillun tutkimuksen kanssa. Tutkimuksen kohteena oli tässäkin tapauksessa finanssialan yritys, josta käytettiin nimitystä OzFinance. OzFinancen häiriönhallintaprosessi noudatti alan yleisiä standardeja ja sen häiriönhallinta oli organisoitu kahteen häiriönhallintaryhmään: NIRT ja koordinaatioryhmään samoin kuin FinanceOrgilla. Erottavana tekijänä oli koordinaatioryhmän aktivoituminen OzFinancella vain korkean prioriteetin häiriöiden yhteydessä, kun taas FinanceOrgin koordinaatioryhmä oli pysyvä. Myös OzFinancella häiriönhallintaryhmien ja tietoturvan hallinnoinnin väliltä puuttuivat viralliset viestintäkäytännöt. Korkean prioriteetin häiriöistä laadittiin raportit, jotka lähetettiin johdon käytettäväksi, mutta tutkimuksessa ei löydetty viittauksia siihen, että tätä tietoa olisi käytetty esimerkiksi tietoturvakäytäntöjen kehittämiseen. Siiloutunut organisaatiorakenne ja ristiriita häiriönhallinnan ja tietoturvan hallinnoinnin tavoitteiden välillä arvioitiin syiksi huonoon kommunikaatioon. Häiriönhallinnan tavoitteena oli palveluiden nopea palauttaminen, kun taas tietoturvan hallinnointi keskittyi tietoturvatoiminnan kehittämiseen ja hallinointiin. Häiriöoppiminen OzFinancella keskittyi FinanceOrgin tapaan häiriönhallintaprosessin parantamiseen teknisestä näkökulmasta. Ensimmäisiin häiriön jälkeisiin kokouksiin ja tapaamisiin osallistui myös OzFinancella vain häiriönhallintaryhmän teknistä henkilöstöä ja tietoturvahallinnoinnin henkilöstö jätettiin tarkoituksella ulkopuolelle. (Ahmad ym., 2015.)

4.1.3 Kolmas case-tutkimus

Webbin, Ahmadin, Maynardin, Baskervillen ja Shanksin (2017) toteuttama kolmas case-tutkimus käsitteli suurta australialaista finanssialan yritystä, josta käytettiin nimitystä OzAccounts. OzAccountsin häiriönhallinnasta vastasi FinanceOrgin ja OzFinancen tapaan kaksi häiriönhallintaryhmää: matalan prioriteetin häiriöihin keskittyvä NIRT ja korkean prioriteetin häiriön aikaan aktivoituva koordinaatioryhmä. Yrityksen häiriöoppimista koskevat ongelmat olivat pääosin samoja kuin FinanceOrgilla ja OzFinancella. Häiriönhallinnan ja liiketoiminnan välillä oli viestintäyhteydet, mutta tietoturvahallinnoinnin ja käytäntöjen suunnittelun toiminnot eivät kommunikoineet häiriönhallinnan kanssa, eivätkä osallistuneet millään tavalla häiriönhallintaprosessiin. OzAccountsin häiriöraportointi ja häiriöiden tarkempi tutkinta keskittyi FinanceOrgin ja OzFinancen tapaan vain korkean prioriteetin häiriöihin. Häiriön jälkeen tutkintaan kuului häiriön käsittely kolmessa kokouksessa, joista ensimmäiseen osallistuu vain tekninen henkilökunta. Kolmannessa kokouksessa häiriötilanteesta tehdään kokonaisvaltainen arvio ja riskiarvio, joiden pohjalta tehdään parannuksia häiriönhallintaprosessiin. Lopulta kummatkin häiriönhallintaryhmät tuottavat omat raporttinsa yritysjohdolle, jotka tarpeen mukaan yhdistetään yhdeksi raportiksi. (Webb ym., 2017.)

4.1.4 Neljäs case-tutkimus

He & Johnson (2017) toteuttaman case-tutkimuksen kohteena oli kiinalainen terveydenhuollon organisaatio. Organisaation häiriönhallinnasta vastasi sen tietotekniikkaosasto, eikä sillä ollut erillisiä häiriönhallintaryhmiä. Tietotekniikasta vastaava henkilöstö muodosti häiriönhallintaryhmän tarpeen mukaan. Matalan prioriteetin häiriöille ei ollut selkeää virallista menettelyohjeistusta ja häiriöstä huolehti yksi tietotekniikkaosaston työntekijä tavoitteenaan palauttaa palvelut mahdollisimman nopeasti. Korkean prioriteetin häiriöiden hallintaan muodostettiin tarpeen mukaan häiriönhallintaryhmä, jonka toiminta noudatti virallisia menettelytapoja. Korkean prioriteetin häiriöistä suoritettiin tutkinta, johon kuului teknisen henkilökunnan ja häiriön raportoineen hoitohenkilökunnan välisiä tapaamisia ja häiriöraportin laatiminen. Raportin ja häiriötiedon viestiminen häiriönhallintaryhmän ulkopuolelle oli kuitenkin puutteellista. Häiriöraporttien laatimisessa ei kiinnitetty huomiota niiden ymmärrettävyyteen ja hyödynnettävyyteen muiden sidosryhmien näkökulmasta ja niiden saatavuus häiriönhallintaryhmän ulkopuolisille osastoille oli heikkoa. Tutkimuksessa ei havaittu viitteitä häiriötiedon hyödyntämisestä tietoturvan kokonaisvaltaiseen parantamiseen. (He & Johnson, 2017.)

4.1.5 Yhteenveto häiriöoppimisen esteistä

Kaikkien tutkittujen yritysten viestintään ja kommunikaatioon liittyvät ongelmat liittyivät häiriötiedon tehottomaan jakamiseen häiriönhallintaryhmän ulkopuolelle. Ainoastaan He ja Johnson (2017) raportoivat häiriönhallinnan pitämistä esitelmistä organisaation muille osastoille. Ongelmaksi kuitenkin tunnistettiin esitysten vaikeaselkoisuus teknisen henkilöstön ulkopuolisille osastoille.

Yksikään yritys ei käynnistänyt tutkintaa tai laatinut raportteja matalan prioriteetin häiriöistä. Ahmad ym. (2012) kuitenkin panivat merkille ajoittaiset yritysjohdolle laaditut suppeat statistiikkaraportit. Korkean prioriteetin häiriöihin liittyi jokaisessa yrityksessä jälkitutkinta ja raportin laatiminen. Häiriönhallintaryhmän ulkopuoliset sidosryhmät suljettiin kuitenkin järjestelmällisesti ulos ensimmäisistä häiriötutkintatapaamisista kaikissa yrityksissä lukuun ottamatta Hen ja Johnsonin (2017) tutkimaa sairaanhoito-organisaatiota. Tämän seurauksena tutkintaan ja sen tuloksiin arvioitiin vaikuttavan teknistä näkökulmaa painottava vinouma (Ahmad ym. 2012).

Yhdessäkään tutkitussa yrityksessä ei ollut virallisia käytäntöjä järjestelmälliseen oppimiseen matalan prioriteetin häiriöistä. Havaittu oppiminen tapahtui epävirallisesti häiriönhallintaryhmän omasta aloitteesta (Ahmad ym., 2012; He & Johnson, 2017). Lisäksi matalan prioriteetin häiriöihin vastaamisessa keskityttiin pääasiassa palvelujen toiminnan mahdollisimman nopeaan palauttamiseen (Ahmad ym., 2015; Webb ym., 2017; He & Johnson, 2017). Korkean prioriteetin häiriöistä tehtyjen tutkimusten tuloksien ja laadittujen raporttien hyödyntämiseksi ja jakamiseksi häiriönhallinnan ulkopuolisten sidosryhmien käyttöön ei ollut virallisia käytäntöjä yhdessäkään tutkitussa yrityksessä. Tapahtunut häiriöistä oppiminen rajoittui häiriönhallintaprosessin tehostamiseen (Ahmad ym., 2012; Ahmad ym., 2015; Webb ym., 2017).

Tiivistettynä voidaan todeta, että tutkimuksissa ei löydetty viitteitä tietoturvan kokonaisvaltaiseen parantamiseen tähtäävästä järjestelmällisestä kaksikehäisen oppimisen periaatteita noudattavasta häiriöoppimisesta. Tietoturvan parantaminen teknisen näkökulman lisäksi myös hallinnollisesta näkökulmasta esimerkiksi tietoturvakäytänteiden ja riskienhallinnan toimivuuden arvioimisen ja parantamisen kautta jäi häiriöoppimisen ulkopuolelle.

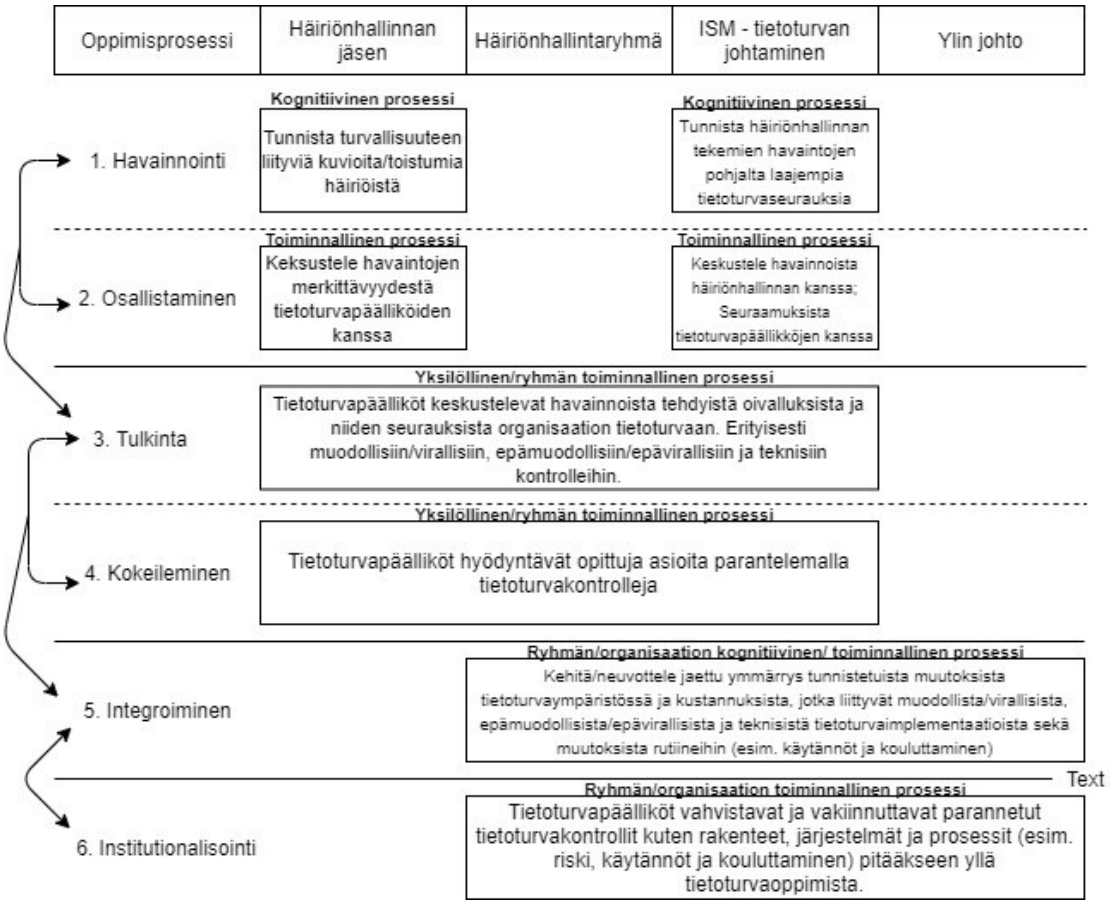
4.2 Häiriöoppimisen parantaminen

Katsaukseen valikoiduissa tutkimuksissa esitettiin useita suosituksia organisaation häiriöoppimiskyvykkyyden parantamiseen ja järjestelmällisen oppimisprosessin käyttöönottoon. Seuraavissa alaluvuissa käsitellään tarkemmin kolme lähestymistapaa organisaation häiriöoppimisen tehostamiseen: DSL (Dynamic Security Learning) -malli (Ahmad ym., 2015; Webb ym., 2017), Häiriönhallinnan

ja tietoturvan hallinnan välisen integraation malli (Ahmad ym., 2020) ja SAMF (Security Assurance Modeling Framework) -malli (He & Johnson, 2017).

4.2.1 DSL-malli

Ahmad ym. (2015) ja Webb ym. (2017) esittävät ratkaisuksi häiriöoppimisen tehostamiseen DSL– mallin. Mallissa kuvataan, kuinka häiriötietoa voidaan hyödyntää organisaation tietoturvakäytäntöjen systemaattiseen parantamiseen. DSL- malli sisältää kuusi prosessia, joiden kautta häiriönhallintaryhmän keräämää häiriötietoa käytetään organisaation tietoturvakäytäntöjen ja kontrollien luomiseen ja parantamiseen. Oppiminen tapahtuu yksilö-, ryhmä- ja organisaatiotasolla kognitiivisten ja toiminnallisten prosessien kautta. Prosesseja toteutetaan kolmessa avainryhmässä: häiriönhallintaryhmässä, tietoturvajohdossa ja yritysjohdossa. (Webb ym., 2017.) Mallin kuusi vaihetta ovat: 1) Havainnointi (Intuiting) 2) Osallistaminen (Attending) 3) Tulkitseminen (Interpreting) 4) Kokeileminen (Experimenting) 5) Integrointi (Integrating) ja 6) Institutionalisointi (Institutionalizing). Havainnoinnin ja osallistamisen vaiheisiin kuuluvat kognitiiviset prosessit ovat toistuvien kuvioiden löytäminen kerätystä häiriötiedosta ja näiden kuvioiden liittäminen laajempaan tietoturvakontekstiin mahdollisten riskien tunnistamiseksi. Esimerkiksi palvelimen lokitietojen poistaminen voi olla merkki mahdollisesta hyökkäystoiminnasta. (Ahmad ym., 2015.) Osallistamisen aikana tapahtuvat toiminnalliset prosessit ovat häiriönhallintaryhmän yksilön ja tietoturvajohdon välillä tapahtuva keskustelu, tiedonjako ja yhteistyö havainnoinnissa tehtyjen löydösten pohjalta. Tulkintaan liittyy toiminnallinen prosessi, jossa häiriönhallinta ja tietoturvajohto tulkitsee ja arvioi tilannetta yhteistyössä tavoitteena luoda jaettu yhteinen näkemys tilanteesta ja tarpeellisista toimista. Kokeileminen tapahtuu myös häiriönhallinnan ja tietoturvajohdon välisenä toiminnallisena prosessina, jossa tulkinnan tuloksena tunnistettuja toimia kokeillaan käytännössä. Integraatioon kuuluu kaikkien kolmen sidosryhmän välinen kognitiivinen ja toiminnallinen prosessi, jonka tarkoituksena on päästä yhteisymmärrykseen tietoturvakäytäntöihin ja toimiin tehtävistä muutoksista sidosryhmien mahdollisista ristiriitaisista ja kilpailevista prioriteeteista huolimatta. Tietoturvajohto voi esimerkiksi haluta häiriönhallinnalta tiiviimpää osallistumista juurisyyanalyyseihin, mutta häiriönhallinnan mielestä tämä veisi liikaa aikaa sen palveluiden nopeaan palauttamiseen keskittyvältä pääasialliselta toiminnalta. Institutionalisointi on mallin viimeinen prosessi, jossa integroinnin aikana päätetyt muutokset tietoturvakäytäntöihin virallistetaan yritysjohdon toimesta. Prosessi voi sisältää esimerkiksi uusien riskiarvioiden tekemistä ja henkilöstön tietoturvakoulutusta. (Ahmad ym., 2015.) DSL-oppimismalli prosesseineen ja sidosryhmineen on kuvattu alapuolella (kuvio 2).



KUVIO 2 Dynamic Security Learning (DSL) -malli (Webb ym., 2017 mukaan)

4.2.2 Integraatiomalli

Ahmad ym. (2020) esittävät, että organisaation häiriöoppimiskyky riippuu siitä, kuinka vahvasti sen ISM ja häiriönhallinnan toiminnot toimivat yhteistyössä. Vahva linkki toimintojen välillä auttaa kumpaakin kehittämään toimintaansa organisaation tietosuojauksen parantamiseksi. Häiriönhallinnan ja ISM:n välinen vahva taktisen tason integraatio kasvattaa organisaation oppimismahdollisuuksia, mikä johtaa tietoturvan parantumiseen. Organisaatiot voivat hyödyntää mallia siinä esitettyjen strategisella, taktisella ja operatiivisella tasolla sijaitsevien integraatiokatkosten tunnistamiseen ja korjaamiseen. Tutkimuksessa esitetään viisi integraation tarjoamaa hyötyä organisaation tietoturvalle. Lisäksi esitellään jokaiseen hyötyyn liittyvät yksi- ja kaksikehäisen oppimisen mahdollisuudet sekä integraation hyödyt organisaation muille tietoturvatoiminnoille (riskien hallinta, käytäntöjen laatiminen ym.).

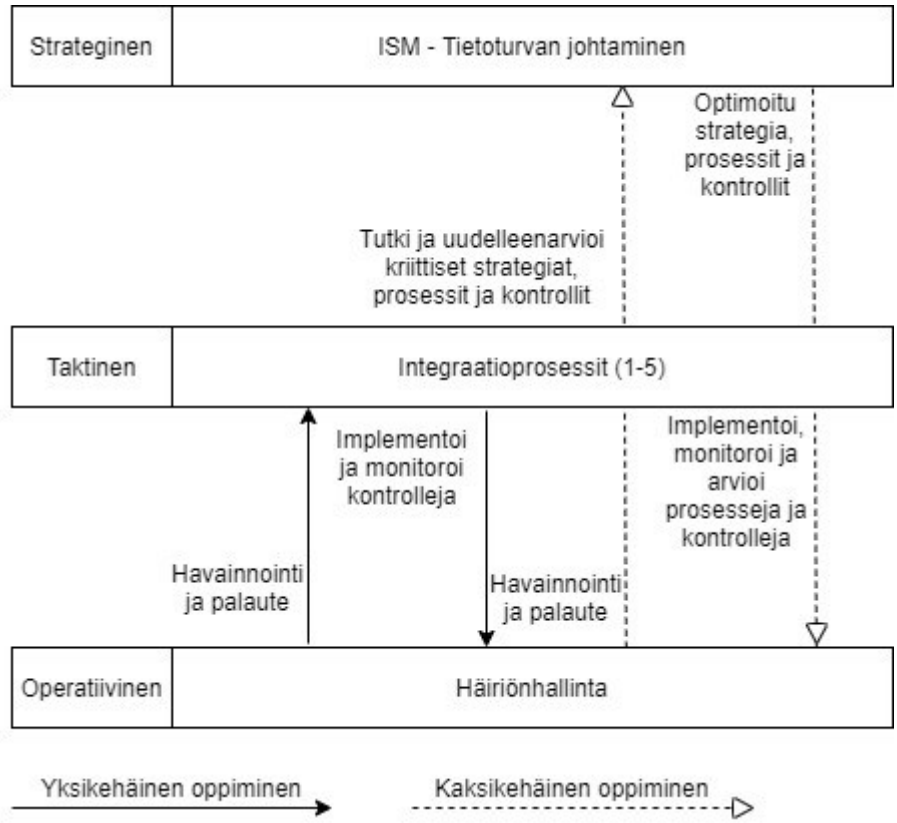
Ensimmäinen esitetty hyöty on kasvanut tietoisuus tietoturvariskeistä. Häiriönhallintatiimin toimittaessa häiriöihin liittyvää tietoa ISM:lle riskien arviointiin ja analysointiin paranee organisaation kokonaisvaltaisen riskiympäristön tuntemus.

Toinen hyöty on uhkatiedon kokoaminen. ISM voi käyttää häiriönhallintatiimin keräämää uhkatietoa erilaisten hyökkääjäprofiilien ja hyökkäystyyppien määrittelyyn ja tietoturvastrategian muuttamiseen tämän tiedon pohjalta.

Kolmas tutkimuksessa esitetty integraatiohyöty on tietoturvasuojauksen heikkouksien paikkaaminen. Häiriönhallintatiimin tulisi kerätä tietoa myös vähemmän kriittisistä häiriöistä ja läheltä-piti-tilanteista sekä tietoturvajärjestelmien häiriöistä. Nämä lähteet voivat sisältää arvokasta tietoa organisaation voimavaroihin ja resursseihin liittyvistä haavoittuvuuksista, joita analysoimalla ISM voi vuorostaan tarjota häiriönhallinnalle tiedon kriittisistä tietoresursseista ja niihin liittyvistä riski-indikaattoreista, jotta häiriönhallinta osaa vuorostaan valita oikeat häiriöt oppimisprosessiin.

Neljäs hyöty on organisaation tietoturvalogiikan arvioiminen. Häiriönhallinnan tulisi tarjota ISM:lle palautetta nykyisten tietoturvakäytäntöjen toimivuudesta ja häiriöissä ja hyökkäyksissä hyväksikäytetyistä haavoittuvuuksista, jotta ISM pystyy arvioimaan ja korjaamaan nykyistä tietoturvastrategiaa.

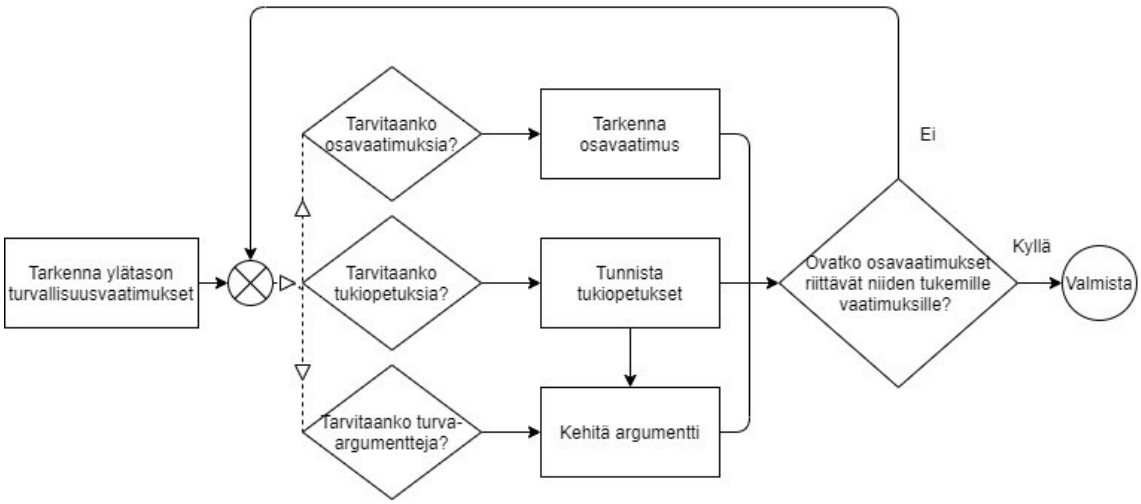
Viimeinen tutkimuksessa esitetty integraatiohyöty on häiriönhallintatiimin toiminnan parantuminen ISM:n tarjoaman strategisen ja taktisen ohjauksen myötä. Tämän ohjauksen muotoja ovat käytäntöihin liittyvä ohjaus. Esimerkiksi millaista häiriötietoa ja todistusaineistoa tulisi kerätä. ISM voi tarjota ohjausta myös koulutusten, harjoitusten ja tietoisuuden muodossa. Kolmas ISM:n tapa tarjota häiriönhallinnalle ohjausta on teknologisen tuen tarjoaminen esimerkiksi prosessointitehon ja rutiininomaisten tehtävien automaation myötä. (Ahmad ym., 2020.) Oheinen kuvio esittää taktisen tason integraatioprosessien mahdollistamat yksi- ja kaksikehäisen oppimisen mahdollisuudet (kuvio 3).



KUVIO 3 Yksi- ja kaksikehäisen oppimisen mahdollisuudet häiriönhallinnan ja tietoturvan johtamisen välisen taktisen integraation kautta (Ahmad ym., 2020 mukaan)

4.2.3 SAMF-malli

Hen ja Johnsonin (2017) esittelemän SAMF-mallin avulla organisaatio pystyy liittämään häiriönhallintatiedosta johdetut tietoturvan parannusideat niitä vastaaviin tietoturvavaatimuksiin ja tavoitteisiin, jotka on dokumentoitu organisaation noudattamiin tietoturvakäytäntöihin ja standardeihin. Ylätason tietoturvavaatimukset jaetaan osavaatimuksiin, joihin liitetään mahdollisia niitä tukevia opittuja tietoturvaparannuksia. Vaatimusten ja opittujen parannusten lisäksi malliin kuuluvat argumentit, joiden avulla ratkaistaan käytössä olevien tietoturvakäytänteiden ja parannusehdotusten väliset ristiriidat ja arvioidaan eri toteutuksia. Kartoittamalla häiriötiedosta johdetut tietoturvaparannusehdotukset tietoturvavaatimuksiin ja niitä vastaaviin käytäntöihin, malli auttaa arvioimaan muutoksen tarvetta käytäntöihin, jotta asetetut tietoturvavaatimukset täyttyvät. (He & Johnson, 2017.) Malli on yleisluontoinen eikä tarjoa yksityiskohtaista vaiheittaista ohjeistusta häiriötiedon keräämiseen ja sen hyödyntämiseen oppimisessa. Se auttaa kuitenkin organisaatiota hahmottamaan mahdollisia puutteita sen tietoturvakäytännöissä korjaten yleensä yleisten standardien pohjalta laadittua tietoturvastrategiaa vastaamaan paremmin organisaation yksilöllistä toimintaympäristöä. SAMF-mallin tarkoituksena ei ole tarjota kaiken kattavaa ratkaisua häiriöoppimiseen, vaan sitä täytyisi käyttää yhdessä esimerkiksi kaksikehäisen oppimismallin periaatteiden tai DSL-mallin kanssa. (He & Johnson, 2017.) SAMF – mallin mukainen toimintakaavio on esitetty alapuolella kuviossa (kuvio 4).



KUVIO 4 Toimintakaavio SAMF -mallin mukaiseen häiriöoppimiseen (He & Johnson, 2017 mukaan)

4.2.4 Yhteenveto esitetyistä ratkaisuista

Sekä DSL-malli, että integraatiomalli painottavat organisaation osastojen välistä yhteistyötä ja integraatiota. DSL- malli tarjosi tarkan vaiheittaisen prosessimallin tämän yhteistyön toteuttamiseen, kun taas integraatiomalli keskittyi kuvaamaan häiriönhallinnan ja tietoturvan johtamisen välisen yhteistyön hyötyjä tie-

toturvan eri osa-alueille. SAMF-mallissa keskeisenä ominaisuutena voidaan myös nähdä häiriönhallinnan tiiviimpi yhteistyö ja kommunikaatio muiden tietoturvaan liittyvien sidosryhmien kanssa. Mallissa ei suoraan korosteta häiriönhallinnan ja tietoturvan johtamisen välisen integraation tärkeyttä, mutta häiriötiedon yhdistäminen siihen liittyviin tietoturvakäytäntöihin ja kontrolleihin voidaan nähdä vaativan tiivistä osastojen välistä yhteistyötä.

Organisaation tietoturvatoimintaan liittyvien sidosryhmien välisen yhteistyön ja kommunikaation tiivistäminen voidaan nähdä kaikkien kolmen mallin perustana. Tästä huolimatta mallit lähestyvät häiriöoppimista hiukan eri näkökulmista: DSL-malli esittää yksityiskohtaisen vaiheittaisen mallin, jossa organisaation sisäisten sidosryhmien roolit ja toiminta oppimisprosessin eri vaiheissa on tarkasti määritelty. Integraatiomalli esittää viisi häiriönhallinnan ja tietoturvan johtamisen yhteistyön aluetta, joilla oppimista tulisi tapahtua. SAMF-mallin voidaan katsoa täydentävän näitä malleja auttamalla yhdistämään opitut asiat käytössä oleviin tietoturvakäytäntöihin.

Mallit vastaavat case-tutkimuksista löydettyihin häiriöoppimisen ongelmiin ottamalla huomioon osastojen välisen virallisten viestintäkäytäntöjen tärkeyden ja ulottamalla häiriöoppimisen yksikehäisen häiriönhallinnan parantamiseen tähtäävän teknisen oppimisen lisäksi tietoturvastrategian ja -käytäntöjen arvioimiseen ja kehittämiseen. Mallit auttavat toteuttamaan häiriöoppimista kokonaisvaltaisesta näkökulmasta, jossa oppiminen otetaan järjestelmällisesti osaksi riskienhallintaa, uhkatiedustelua, haavoittuvuuksien kartoitusta ja käytäntöjen arvioimista tietoturvan parantamiseksi organisaation osastojen rajat ylittävän kommunikaation ja yhteistyön kautta. DSL-malli ja integraatiomalli noudattavat molemmat sekä yksi- että kaksikehäisen oppimismallin periaatteita. DSL-mallin viimeisessä vaiheessa sekä hallinnolliset, että tekniset muutokset tietoturvakontrolleihin implementoidaan osaksi organisaation tietoturvakäytäntöjä. Muutokset pitävät sisällään niin yksinkertaista virheenkorjausta olemassa olevien käytäntöjen sisällä, kuin näiden käytäntöjen arviointia ja muuttamista esimerkiksi uusien riskiarvioiden pohjalta. Integraatiomallissa kummatkin oppimismallit otetaan huomioon kaikissa viidessä integraatioprosessissa.

5 POHDINTA JA YHTEENVETO

Tutkielman tarkoituksena oli tutustua häiriönhallintaan ja häiriöoppimiseen ja niiden toteuttamiseen osana organisaation tietoturvaa. Tarkoituksena oli löytää häiriöoppimisen toteutukseen liittyvät keskeiset ongelmat ja esitellä kirjallisuudesta löydettyjä ratkaisuja näihin ongelmiin. Tutkielman alussa määriteltiin organisaation tieto- ja kyberturvaan keskeisesti liittyvät **voimavaran/resurssin, uhan**, **haavoittuvuuden** ja **riskin** käsitteet. Tämän jälkeen käsiteltiin **tietoturvaa** ja **häiriönhallintaa** organisaation toimintoina ja esiteltiin kolme keskeistä ja yleisesti käytettyä häiriönhallintamallia.

Seuraavaksi esiteltiin tutkielman kannalta toinen oleellinen teema: **organisaation oppiminen** tutkielman kannalta oleelliselta laajuudelta. Lopulta tuotiin yhteen häiriönhallinnan ja organisaation oppimisen käsitteet **häiriöoppimisen** määrittelyn muodossa.

Tutkielman teoreettisen pohjan ja oleellisten käsitteiden määrittelyn jälkeen esiteltiin kirjallisuuskatsauksen tulokset. Tutkielmassa pyrittiin löytämään vastaus kahteen tutkimuskysymykseen: 1) Mitkä ovat keskeisiä esteitä tehokkaalle häiriöoppimiselle organisaatiossa? ja 2) Millaisia malleja tutkimuskirjallisuus tarjoaa organisaation häiriöoppimiskyvykkyyden parantamiseen?

Tehokkaan häiriöoppimisen toteutusta estäviä keskeisiä ongelmia löydettiin kirjallisuuskatsaukseen valikoiduista case-tutkimuksista pääpiirteissään kolme: 1) Virallisten viestintäkäytäntöjen puuttuminen häiriönhallintaryhmän ja tietoturvan hallinnoinnin välillä ja häiriötiedon tehoton viestintä häiriönhallintaryhmän ulkopuoliseen käyttöön. 2) Häiriötutkinnan toteuttaminen ja häiriöraportin laatiminen vain korkean prioriteetin häiriöistä. 3) Teknisen näkökulman painottuminen häiriötutkinnassa ja häiriöraportissa ja tutkinnan tulosten hyödyntämisen rajoittuminen häiriönhallintaprosessin tehostamiseen teknisestä näkökulmasta.

Löydettyjen ongelmien perusteella voidaan todeta organisaatioiden häiriöoppimisen keskittyvän usein häiriönhallintaprosessin tekniseen tehostamiseen ja jättävän suurilta osin huomiotta häiriönhallinnan ulkopuolisten sidosryhmien toiminnan kehittämisen häiriötiedon pohjalta. Organisaatioiden häiriöoppimisen tasossa on myös merkittävä ero matalan prioriteetin ja korkean

prioriteetin häiriöiden välillä. Matalan prioriteetin häiriöistä oppimiseen ei ollut virallisia menettelytapoja yhdessäkään yrityksessä. Jos oppimista tapahtui, oli se häiriönhallintaryhmän sisälle rajoittunutta omaehtoista muistiinpanojen tekemistä ja jakamista. Tästä huolimatta matalan prioriteetin häiriöt kuitenkin kirjattiin usein vähintään selvitetyiksi jonkinlaiseen häiriökirjausjärjestelmään.

Korkean prioriteetin häiriöistä toteutettiin kaikissa yrityksissä tutkinta, jonka tuloksena laadittiin häiriöraportti. Tutkinnasta vastasi kuitenkin usein teknistä näkökulmaa korostava häiriönhallintaryhmä, minkä vuoksi myös tutkinnan tuloksissa ja häiriöraportissa painottui tekninen näkökulma. Oppiminen rajoittuikin suurilta osin häiriönhallinnan tekniseen tehostamiseen.

Organisaation häiriöoppimiskyvykkyyden parantamiseksi löydettiin tutkimuskirjallisuudesta kolme häiriöoppimismallia. Oppimismallien yhteisiä ominaisuuksia olivat häiriönhallintaryhmän ja muiden organisaation tietoturvatoimintaan liittyvien osastojen välisen yhteistyön ja viestinnän tehostaminen, selkeyttäminen ja tiivistäminen. Lisäksi sekä integraatiomalli, että DSL-malli toteuttavat yksikehäisen oppimisen lisäksi kaksikehäisen oppimisen periaatteita ja pyrkivät liittämään oppimisen teknisten ja suoraviivaisten parannusten lisäksi tietoturvastrategian taustalla vaikuttavien ja sitä ohjaavien olettamusten ja uskomusten arviointiin ja muuttamiseen organisaation tietoturvan kehittämiseksi kokonaisvaltaisesta näkökulmasta.

Malleista DSL-malli tarjoaa vaiheittaisen ja käytännön toiminnan kannalta selkeimmän ohjeistuksen häiriöoppimisen käytännön toteutukseen ja vastaa löydetyistä malleista ehkä parhaiten kysymykseen siitä, miten häiriöoppimista tulisi käytännössä toteuttaa. Integraatiomalli esittelee häiriönhallinnan ja tietoturvan johtamisen välisen yhteistyön luomia oppimismahdollisuuksia ja hyötyjä esittäen vastauksen kysymykseen siitä, mitä hyötyä häiriöoppimisesta on organisaatiolle. SAMF-mallin voidaan katsoa täydentävän kahta muuta mallia tarjoten ratkaisun tietoturvavaatimusten ja niihin liittyvien parannusten ja käytäntöjen kartoittamiseen ja arvioimiseen.

Tutkielma kokoaa usean tutkimuksen tulokset organisaation häiriöoppimiseen liittyvistä esteistä ja ongelmista ja niihin esitetyistä ratkaisuista antaen kuvan häiriöoppimisen nykytilasta organisaatioissa. Tutkielman tuloksista on oletetusti hyötyä niin aiheen akateemisen jatkotutkimuksen kuin tietoturvan käytännön harjoittamisen näkökulmasta. Tulokset auttavat niin tutkijoita kuin tietoturvan parissa työskenteleviä ymmärtämään paremmin häiriöoppimisen potentiaalista roolia tietoturvan parantamisessa ja ottamaan huomioon keskeiset ongelmat ja olemassa olevat ratkaisumallit tehokkaan häiriöoppimistoiminnon kehittämisessä.

Tutkielman tekemisen aikana kävi selväksi, että häiriöoppiminen on tutkimusalueena jäänyt suhteellisen vähäiselle huomiolle häiriönhallinnan tekniseen näkökulmaan painottuvaan tutkimukseen verrattuna. Tähän liittyvä huomionarvoinen seikka kirjallisuuskatsaukseen valikoituihin tutkimuksiin liittyen oli, että analysointiin valikoituneiden tutkimusten tutkimusryhmissä esiintyi suurilta osin samoja henkilöitä. Tutkimukset olivat kuitenkin suurilta osin pal-

jon viitattuja, vertaisarvioituja ja laadukkaissa tieteellisissä julkaisuissa julkaistuja.

Tämä tutkielma keskittyi tutkimaan organisaation tietoturvan kehittämistä organisaation oppimisen teorian tarjoamasta häiriöoppimisen viitekehyksestä. Tutkielman ulkopuolelle jäivät muut vaihtoehtoiset lähestymistavat häiriönhallinnan ja tietoturvan kehittämiseen. Yksi esimerkki tutkielman ulkopuolelle jätetystä lähestymistavasta on tilannetietoisuuden (situation awareness) näkökulma organisaation häiriönhallintaan.

Mielenkiintoinen jatkotutkimusaihe olisi häiriöoppimismallien käyttöönoton havainnointi organisaatiossa. Tutkielmassa löydettyjen häiriöoppimismallien käytännön toimivuudesta ja hyödyistä ei tutkielman tekohetkellä ollut vielä löydettävissä laadukkaita tutkimuksia.

LÄHTEET

Ahmad, A., Desouza, C. K., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020) How integration of cyber security management and incident response enables organizational learning. *Journal of the association for information science and technology, 71(8)*, 939-953.

Ahmad, A., Hadgkiss, J., & Ruighaver, A.-B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security, 31(5),* 643-652.

Ahmad, A., Maynard, S. P., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security, 101,* 102122.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015) A case analysis of information systems and security incident responses. *International journal of information management. 35,* 717-723.

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004) Defining incident management processes for CSIRTs: A work in progress. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020) Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99,* 102030.

Argyris, C. (1976) Single-loop and double-loop models in research on decision making. *Administrative science quarterly, 21(3),* 363-375.

Argyris, C., & Schön, D. A. (1978). *Organizational learning : A theory of action perspective.* Reading: Addison-Wesley publishing company.

Argyris, C., & Schön, D. A. (1996). *Organizational learning II.* Addison-Wesley publishing company.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014) Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management, 51(1),* 138-151.

Chaudhuri, S., Dayal, U & Narasayya, V. (2011). An overview of business intelligence technology. *Communications of the ACM. 54(8),* 88-98.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014) Defining cybersecurity. *Technology innovation management review*

Eloff, J. H. P., & Da Veiga, A. (2007) *An information security governance framework. Information systems management, 23,* 361-372.

Fenz, S., & Ekelhart, A. (2009) Formalizing information security knowledge. *ASIACCS'09*, Sydney: NSW, Australia.

He, Y., & Johnson, C. (2017) Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. *Informatics for health and social care, 42(4),* 393-408.

Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management, 27(5),* 644-667.

Harrison, R., Parker, A., Brosas, G., Chiong, R & Tian, X. (2015). The role of technology in the management and exploitation of internal business intelligence. *Journal of systems and information technology. 17(3),* 247-262.

Huber, G. P. (1991) Organizational learning: the contributing processes and the literatures. *Organization science. 2(1),* 88-115.

ISO/IEC. (2005). ISO/IEC 17799: Code of practice for information security management.

ITIL. (2011). *ITIL Service operation.* UK: TSO.

BS ISO/IEC. (2011). ISO/IEC 27035: *Information technology – Security Techniques – Information security incident management.*

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006) On incident handling and response: a state-of-the-art approach. *Computers & security, 25,* 351-370.

NIST. (2017). *An introduction to information security.*

NIST. (2012). *Computer security incident handling guide.*

Posthumus, S., & Von Solms, R. (2004) A framework for the governance of information security. *Computers & security, 23,* 638-646.

Purplesec. 2021 cyber security statistics – the ultimate list of stats, data & trends. Haettu 3.7.2021 osoitteesta https://purplesec.us/resources/cyber-security-statistics/

Rahman, N. H. A., & Choo, K. R. (2015) A survey of information security incident handling in the cloud. *Computers & Security, 49,* 45-69.

Sanastokeskus. (2018). *Kyberturvallisuuden sanasto.*

Shedden, P., Ahmad, A & Ruighaver, A. B. (2010). Organisational learning and incident response: promoting effective learning through the incident response process. *8th australian information security management conference*, Edith Cowan University, Perth Western Australia, 30th November 2010. DOI: https://doi.org/10.4225/75/ 57b6771734788

Sobers, B. (2021, 16. maaliskuuta). 134 cybersecurity statistics and trends for 2021. Haettu 3.7.2021 osoitteesta https://www.varonis.com/blog/cybersecurity-statistics/

Soomro, Z. A., Mahmood, H. S., & Ahmed, J. (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36(2),* 215-225.

Stallings, W., & Brown, L. (2018) *Computer security: Principles and practice.* Harlow.

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36,* 100581.

Tøndel, I. A., Line, M. B. & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security, 45,* 42-57.

Von Solms, R., & Van Niekerk, J. (2013) From Information security to cyber security. *Computers & security 38,* 97-102.

Wang, C. L., & Ahmed, P. K. (2003). Organisational learning: a critical review. *The learning organization, 10(1),* 8-17.

Webb, J., Ahmad, A., Maynard, S., Baskerville, R., & Shanks, G. (2017) Organizational security learning from incident response. *ICIS 2017 Proceedings. 4.*

Whitman, M. E. & Mattord, H.-J. (2016) *Principles of information security*. Boston: Cengage Learning.

Zaharia, A. (2021, 29. kesäkuuta). 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends (2021 EDITION). Haettu 2.7.2021 osoitteesta https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/