TURUN YLIOPISTO
Kauppakorkeakoulu

Kokonaisarkkitehtuuri häiriöiden hallinnan työkaluna normaalioloissa

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatija:
Helmi Pelkonen

Ohjaaja:
Professori Jukka Heikkilä

2.11.2025
Turku

Pro gradu -tutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Helmi Pelkonen
Otsikko: Kokonaisarkkitehtuuri häiriöiden hallinnan työkaluna normaalioloissa
Ohjaaja: Professori Jukka Heikkilä
Sivumäärä: 84 sivua + liitteet 5 sivua
Päivämäärä: 2.11.2025

Digitaalisen transformaation myötä häiriöiden määrä organisaatioissa on kasvanut huomattavasti viimeisten vuosien aikana. Lisäksi häiriöiden hallintaan ja kyberturvallisuuteen liittyvät vaatimukset ovat tiukentuneet. Euroopan unionin NIS2-direktiivi laajentaa sen edeltäjän NIS-direktiivin vaatimuksia ja velvoittaa yhä useampia toimialoja. Organisaatioissa on käyty paljon keskustelua siitä, miten uudet vaatimukset voitaisiin täyttää. Laajentuneiden vaatimusten ohella häiriöiden hallintaan tarvitaan parempia ja tehokkaampia ratkaisuja, jotta organisaatiot pystyisivät suojautumaan häiriöiltä ja niiden vaikutuksilta tulevaisuudessa. Kokonaisarkkitehtuuria on ehdotettu toimivaksi työkaluksi muun muassa riskienhallintaan ja kriisienhallintaan, mutta kokonaisarkkitehtuurin ja häiriöiden hallinnan välistä yhteyttä ei ole vielä tutkittu yhtä paljon.

Tämän tutkimuksen tarkoituksena on selvittää, voisiko kokonaisarkkitehtuuri tukea häiriöiden hallintaa. Lisäksi halutaan tarkastella kokonaisarkkitehtuuria suhteessa NIS2-direktiiviin ja selvittää, mikäli kokonaisarkkitehtuurin avulla voidaan vastata direktiivin vaatimuksiin. Tutkimuksen toimeksiantajaorganisaatio lukeutuu NIS2-direktiivin määrittelemäksi kriittisen sektorin toimijaksi ja heihin kohdistuvat direktiivin velvoitteet. Lisäksi he ovat mallintaneet jo useamman vuoden ajan kokonaisarkkitehtuuriaan ja seuranneet organisaatiossa tapahtuneita häiriöitä raportointijärjestelmänsä avulla.

Tutkielman viitekehys on luotu yhdistämällä Kotusevin (2017) kahdeksan kokonaisarkkitehtuurin artefaktia ja NIST kyberturvallisuusviitekehys (2024). Viitekehyksessä yhdistyvät kyberturvallisuusviitekehyksen häiriöiden hallinnan toiminnot ja kokonaisarkkitehtuurin artefaktit, minkä avulla on tutkittu häiriöiden hallinnan ja kokonaisarkkitehtuurin välistä yhteyttä. Tutkimus on toteutettu laadullisena tutkimuksena, jossa yhdistyvät suunnittelutieteellinen tutkimusote ja tapaustutkimus. Suunnittelutieteellisessä tutkimusotteessa testataan ja arvioidaan luotua artefaktia, joka tässä tutkielmassa on tutkielman viitekehys. Tapaustutkimus toteutettiin tutkimalla toimeksiantajaorganisaation kokonaisarkkitehtuurin mallinnuksia ja häiriöraportteja tutkielman viitekehyksen avulla. Tämän jälkeen tutkielman viitekehystä arviointiin NIS2-direktiivin vaatimuksiin peilaten.

Kahdessa tutkitussa häiriössä tunnistettiin seitsemän tapaa, joilla kokonaisarkkitehtuuri tukee kyberturvallisuusviitekehyksen mukaista häiriöiden hallintaprosessia. Kokonaisarkkitehtuurin avulla pystyttiin erityisesti tukemaan häiriöiden ja niiden vaikutusten laajuuden kartoittamista sekä yhtenäistämään ja selkeyttämään häiriöiden hallintaprosessia. Tutkielman viitekehyksen ja kokonaisarkkitehtuurin avulla pystyttiin vastaamaan neljään kuudesta tunnistetusta NIS2-direktiivin vaatimuksesta ja osittain viidenteen. Kokonaisarkkitehtuuri toteutti erityisesti toimitusketjuihin, häiriöiden hallintaan ja riskienhallintaan liittyviä vaatimuksia. Tutkimus osoittaa, että kokonaisarkkitehtuurilla voidaan tukea häiriöiden hallintaa ja tehostaa siihen liittyviä toimintoja. Lisäksi kokonaisarkkitehtuuria hyödyntämällä voidaan vastata useampaan NIS2-direktiivin vaatimukseen. Jatkotutkimusta olisi hyvä tehdä aiheesta laajemmin, jotta erilaisten häiriöiden ja toimialojen erot tulisivat tarkasteltua.

Avainsanat: kokonaisarkkitehtuuri, häiriöiden hallinta, NIS2-direktiivi, kyberturvallisuus

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

1.1 Tutkimuksen tausta ja motivointi

Digitalisaatio on vaikuttanut siihen, miten nopeasti liiketoimintaympäristö muuttuu ja kehittyy (Urbach & Ahlemann, 2019). Liiketoimintaprosessit ovat yhä useammin aineettomia ja ne tapahtuvat digitaalisesti erilaisilla teknologia-alustoilla. Uudet teknologiat vaativat monimutkaisten tietojärjestelmä kokonaisuuksien hallintaa. (Laudon & Laudon, 2004.) Organisaatioiden on pyrittävä pysymään mukana muutoksessa, jotta ne voivat kilpailla markkinoilla (Ahlemann ym., 2012). Saman aikaisesti organisaatioiden kohtaamien riskien ja uhkien määrä on ollut jatkuvassa kasvussa ja uudenlaisten digitalisaation tuomien haasteiden hallitseminen vaikeutuu (Dokuchaev ym., 2020). Kyberturvallisuudesta ja tietoturvasta huolehtiminen organisaatioissa on aina vain tärkeämpää, sillä niihin kohdistuvien häiriöiden vaikutukset leviävät muihin liiketoiminnan osa-alueisiin (Diefenbach ym., 2019).

Suomessa tietomurtoja ja palvelunestohyökkäyksiä tapahtuu yhä useammin. Yksi Suomen suurimmista tietomurroista uhrien määrällä mitattuna tapahtui 2018, kun suomalaisen Psykoterapiakeskus Vastaamon tietojärjestelmiin tunkeuduttiin ja noin 33 000 potilastietokannassa olleen henkilön tietoja julkaistiin internetissä. (Yle, 25.10.2024.) Toinen Suomessa laajasti vaikuttanut tietomurto kohdistui Helsingin kaupungin kasvatuksen ja koulutuksen toimialaan toukokuussa 2024, jolloin jopa 120 000 oppijan, huoltajan ja kaupungin työntekijän tiedot vuosivat (Yle, 14.5.2024). Vuoden 2024 syksyllä Nordeaan kohdistui yhtäjaksoisesti kuukauden ajan palvelunestohyökkäyksiä, minkä vuoksi pankin palveluihin kirjautuminen oli usein estetty. Ensimmäisellä vuosipuoliskolla Nordeaan kohdistui 20 palvelunestohyökkäystä, kun taas syksyllä hyökkäysten määrä oli päässyt nousemaan jo yli 360. (Helsingin Sanomat, 15.10.2024.) Ohjelmistoyhtiö Tietoevry totesi viimeisessä raportissaan, että vuoden 2024 aikana vakavaa haittaa aiheuttaneita kyberhyökkäyksiä oli kohdistunut yli puoleen pohjoismaalaisista yrityksistä ja lähes 90 prosenttia yrityksistä arvioi hyökkäysten yleistyvän (Tietoevry.com, 2024). Tietoturvayhtiö Nixunin kyselyn tuloksien mukaan lähes kolmannes pohjoismaisista yrityksistä on kokenut tietomurron viimeisen vuoden aikana (Yle, 1.11.2024).

Organisaatiot ovat alttiita kohtaamaan häiriöitä jatkuvasti esiintyvien sisäisten sekä ulkoisten uhkien ja riskien vuoksi. Nämä uhat johtuvat usein hallinnan puutteesta tai epäjohdonmukaisuudesta. (Bundy ym., 2017.) Yrityksen kyky ennakoida ja reagoida häiriöihin on keskeisessä asemassa sen tulevaisuuden kehityksen ja sietokyvyn kannalta (Phelps, 1986). Useimmiten yritykset eivät ole

ennakoineet tai odottaneet häiriön tapahtumista, minkä vuoksi sen vaikutukset ovat merkittävät ja palautuminen hitaampaa. Tähän syynä on mahdollisesti se, että häiriöt ovat aina erilaisia, minkä vuoksi niiden ehkäiseminen, havaitseminen ja hallinta vaatii paljon resursseja. (Ahlemann ym., 2012.)

Yritysten kohtaamat uhat ja riskit koskevat yhä useammin teknologiaan ja digitaalisiin palveluihin liittyviä osa-alueita (Thakur, 2024). Näiden uhkien ja riskien seuraukset ovat tänä päivänä yhä vakavampia, sillä tietoturva on muuttunut erottamattomaksi osaksi ydinliiketoimintaa (Diefenbach ym., 2019). Useissa organisaatioissa on tunnistettu haastavaksi hyödyntää kaikkia erilaisia digitaalisia ratkaisuja, mutta samalla kuvitellaan teknologian sulautuvan automaattisesti osaksi omia toimintoja. Tässä muutoksessa kokonaisarkkitehtuurilla (engl. enterprise architecture) on keskeinen rooli organisaatioiden sopeutumiskyvyn tukemisessa. (Ross ym., 2019.) Se keskittyy hahmottamaan organisaatiota kokonaisvaltaisesti ja tunnistamaan liiketoiminnan sekä teknologian muutosvaikutukset (Bernard, 2012). Kokonaisarkkitehtuurin merkitys liiketoiminnassa on kasvanut jatkuvasti digitalisaation edetessä ja sen avulla voidaan löytää vastauksia digitalisaatiohankkeiden haasteisiin (Bossert, 2016; Goerzig & Bauernhansl, 2018; Hafsi & Assar, 2020). IT-ammattilaisuus kehittyy ja digitaalisten portfolioiden merkitys kasvaa, minkä vuoksi kiinnostus dataan perustuvaan päätöksentekoon lisääntyy jatkuvasti. Lisäksi tarve järjestelmätason sietokyvylle on kasvanut teknologisten kehitysaskeleiden myötä, mikä korostui entisestään COVID-19-pandemian myötä (Aldea ym., 2020). Näiden muutosten edessä kokonaisarkkitehtuurilla on merkittävä rooli. (Betz, 2024.)

Digitalisaation mukana tulleiden häiriöiden, uhkien ja riskien havaitsemiseen ja hallintaan on tullut vaatimuksia lisäksi Euroopan unionilta. NIS2-direktiivi on EU:n yhtenäinen oikeudellinen kehys kyberturvallisuuden ylläpitämiseksi 18 kriittisellä sektorilla. Jäsenvaltioiden tulee itse määritellä kansallinen kyberturvallisuusstrategia ja toimia yhdessä EU:n kanssa rajat ylittävässä reagoinnissa ja valvonnassa. (Euroopan komissio, 2025a.) NIS2-direktiivin piti tulla voimaan jäsenvaltioissa lokakuussa 2024, mutta Suomi myöhästyi aikataulusta, sillä hallituksen lakiesitys direktiivin täytäntöönpanemisesta ei edistynyt riittävällä nopeudella eduskunnassa (Kolehmainen, 2024).

Monet häiriöt johtuvat laitteistoista ja ohjelmistoista, mutta tahallisesti aiheutettujen häiriöiden määrä on jatkuvassa kasvussa. Kiristyshaittaohjelmahyökkäyksiä (engl. ransomware attacks) oli vuonna 2022 41 % enemmän kuin edellisvuonna (IBM, 2022) ja sähköpostihyökkäyksien kuten tietojenkalastelun määrä kasvoi vuodessa 48 % (Security Staff, 2022). Lisäksi häiriöt kohdistuvat entistä enemmän toimitusketjuihin (Bulletproof, 2022). Viimeisten vuosien aikana

kyberturvallisuudessa on tapahtunut muutos, joka on koskettanut niin uhkien ja riskien määrää kuin yhä moninaisempia kohteita. Kyberturvallisuuden muutos entistä laaja-alaisemmaksi vaatii EU-tason hallintaa (Gao & Chen, 2022). Tämän myötä myös siihen liittyvät riskit ja uhat ovat yhä monimutkaisempia, ja ne kohdistuvat paitsi tietojärjestelmiin ja ICT-infrastruktuuriin myös talouden ja yhteiskunnan kriittisiin alueisiin (Krzykowski, 2021; Liebetrau, 2024). Kyberturvallisuuden kokonaisuuden hallinta vaatii jatkuvaa uudelleenarviointia digitaalisten teknologioiden kehittyessä (Daugulis, 2023).

Bizzdesignin (2024) State of Enterprise Architecture -raportissa on todettu, että organisaatiot priorisoivat tällä hetkellä innovaatioissaan kyberturvallisuutta. Raportissa nostetaan esille, että kokonaisarkkitehtuuria käytetään yhä enemmän turvallisuuteen, riskienhallintaan ja vaatimustenmukaisuuteen liittyvissä toiminnoissa sekä johtajien keskuudessa. Organisaatioiden tarve kehittää riskienhallintaa ja turvallisuutta kasvaa ja kokonaisarkkitehtuuri nähdään hyödyllisenä työkaluna tämän toteuttamisessa.

Tämän päivän organisaatioille merkittävä haaste ovat digitalisaation liittyvät häiriöt ja niiden vaikutusten hallitseminen. Suomessakin yleistyneet tietomurrot ja palvelunestohyökkäykset osoittavat, että organisaatiot ovat haavoittuvaisia kyberuhille ja häiriöihin varautumisessa on ollut puutteita. Euroopan unioni on myös asettanut vaatimuksia kyberturvallisuuden varmistamiselle uudistetulla NIS2-direktiivillä. Tämä velvoittaa organisaatioita kehittämään niiden häiriöiden hallintaa ja korostaa digitalisaation aiheuttamiin uhkiin ja riskeihin varautumisen merkitystä entisestään. Kyberturvallisuus ei ole enää erillinen turvallisuuden muoto, joka koskisi vain IT-toimintoja vaan merkittävä koko liiketoiminnan turvallisuuden kannalta. Kokonaisarkkitehtuurin menetelmien avulla voidaan tunnistaa organisaation muutosvaikutukset ja tukea teknologian hallintaa ja siksi sen hyödyntämisellä voi olla merkittävä rooli digitalisaation tuomien uhkien ja häiriöiden hallinnassa.

Tutkimusaihe on ajankohtainen, ja sen tarkastelu tuottaa hyödyllistä tietoa kokonaisarkkitehtuurin käytöstä erityisesti häiriöiden hallinnassa ja ratkaisussa. Tutkielmassa perehdytään sekä kokonaisarkkitehtuurin ja häiriöiden hallinnan väliseen yhteyteen että NIS2-direktiivin häiriöiden hallintaan kohdistuviin vaatimuksiin. Tutkimuksessa halutaan selvittää, voisiko kokonaisarkkitehtuuri tukea häiriöiden hallintaa ja samalla olla ratkaisu NIS2-direktiivin vaatimusten toteuttamiseen. Aihe on merkittävä ja ajankohtainen, sillä sitä ei ole käsitelty vastaavasti aikaisemmassa tutkimuksessa. Tutkielman aihe on valittu myös siksi, että kokonaisarkkitehtuurin ja häiriöiden hallinnan tutkiminen on ajankohtaista tutkielman

toimeksiantajaorganisaation kannalta ja heitä koskevat NIS2-direktiivin velvoitteet. Tutkielman tavoitteena on lisätä ymmärrystä siitä, miten kokonaisarkkitehtuuria voidaan hyödyntää entistä tehokkaammin organisaatioissa. Tutkimuksen tuloksista hyötyy erityisesti toimeksiantaja, mutta niiden tavoitteena on tarjota tietoa myös muille kriittisen sektorin toimijoille. Lisäksi tutkimus voi edistää yleisempää ymmärrystä kokonaisarkkitehtuurin mahdollisuuksista ja hyödyistä.

Tutkielman johdannon jälkeen käsitellään seuraavassa luvussa tarkemmin tutkielman aiheeseen liittyvää aikaisempaa tutkimusta. Tämän jälkeen seuraa kaksi teorialukua, joista ensimmäinen käsittelee kokonaisarkkitehtuuria ja toinen NIS2-direktiiviä. Viidennessä luvussa esitellään tutkielman viitekehys, joka on muodostettu yhdistämällä Kotusevin kahdeksan artefaktia ja NIST Kyberturvallisuusviitekehys 2.0. Tämän jälkeen käydään läpi tutkimusmenetelmät ja -prosessi. Seitsemännessä luvussa on esitelty tutkimuksen tulokset. Viimeinen luku sisältää johtopäätökset, jossa tutkimuksen tuloksia pohditaan tutkimuskysymysten ja kirjallisuuskatsauksen avulla sekä annetaan käytännön suosituksia toimeksiantajan kokonaisarkkitehtuurityötä ja häiriöiden hallintaa varten. Lisäksi käydään läpi tutkimuksen rajoitukset ja annetaan jatkotutkimusehdotuksia.

1.2 Tutkimuskysymykset

Tutkimuksen tavoitteena on selvittää kokonaisarkkitehtuurin rooli osana organisaation häiriöiden hallintaa normaalioloissa. Tarkastelu rajataan normaalioloihin, eikä tutkimus käsittele poikkeusoloissa esiintyviä häiriöitä. Tutkielmassa normaaliolo käsittää pääosin vallitsevan tilan ja poikkeusolot tarkoittavat harvinaisempia hetkiä, jotka poikkeavat merkittävästi normaalioloista. Poikkeusolot on määritelty Suomen valmiuslaissa (Finlex, 2011) ja määritelmän on täyttänyt esimerkiksi koronapandemia.

Tutkielmassa pyritään erityisesti ymmärtämään, miten kokonaisarkkitehtuurin hyödyntäminen voi vähentää häiriöiden aiheuttamia haittoja sekä edistää nopeampaa ja tehokkaampaa palautumista häiriötilanteista. Lisäksi halutaan tutkia kyberturvallisuuden näkökulmaa NIS2-direktiivin avulla ja selvittää, miten kokonaisarkkitehtuuri voi auttaa organisaatioita vastaamaan direktiivin asettamiin vaatimuksiin. Tutkimuskysymykset ovat seuraavat:

1. *Miten kokonaisarkkitehtuuri tukee häiriöiden hallintaa organisaatioissa?*
2. *Voidaanko kokonaisarkkitehtuurin avulla vastata NIS2-direktiivin asettamiin vaatimuksiin?*

Ensimmäisen tutkimuskysymyksen avulla on tarkoitus selvittää, onko kokonaisarkkitehtuurista hyötyä organisaatioiden häiriöiden hallinnassa ja miten kokonaisarkkitehtuuri voisi tukea tätä

prosessia. Toisen tutkimuskysymyksen myötä pyritään selvittämään, olisiko kokonaisarkkitehtuuri riittävä menetelmä toteuttamaan NIS2-direktiivin vaatimuksia kriittisen sektorin organisaatioissa ja täten menetelmä, joka parantaisi organisaatioiden kyberturvallisuutta ja sietokykyä. Kysymysten tavoitteena on selvittää, kuinka kokonaisarkkitehtuurin avulla voidaan tunnistaa ja analysoida häiriöihin liittyviä riskejä ja riippuvuuksia ja sen myötä ymmärtää, millä tavoin prosessien ja toimintojen hallintaa voisi parantaa.

Tutkimuskysymyksiin tullaan vastaamaan kirjallisuuskatsauksen ja tutkimuksen avulla. Kirjallisuuskatsauksissa perehdytään kokonaisarkkitehtuuriin ja häiriöiden hallintaan kyberturvallisuuden näkökulmasta, minkä avulla luodaan perusta tutkimuskysymykseen vastaamiselle. Lisäksi tarkastellaan NIS2-direktiiviä ja sitä suhteessa häiriöiden hallintaan. Empiirinen data tullaan saamaan toimeksiantajaorganisaation häiriöiden raportointijärjestelmästä sekä kokonaisarkkitehtuurimallinnusten muodossa. Teoriaosuuden ja empirian avulla luodaan käsitys kokonaisarkkitehtuurin roolista häiriöiden hallinnassa sekä vastataan tutkimuksen ja toimeksiantajaorganisaation kannalta olennaisiin tutkimuskysymyksiin.

1.3 Generatiivisen tekoälyn käyttö (Declaration on the Use of Generative Artificial Intelligence)

Täten ilmoitan, että generatiivista tekoälyä on käytetty työkaluna tässä tutkielmassa tukemaan työskentelyä. Turun kauppakorkeakoulun linjausten mukaisesti yksityiskohtainen selvitys hyödynnetyistä työkaluista ja niiden käyttötarkoituksista tässä tutkielmassa on saatavilla liitteenä 2.

2 Aiempi tutkimus

Kokonaisarkkitehtuurilla on pidempi historia kuin usein ajatellaan. Ensimmäisiä menetelmiä, jotka voidaan jäljittää kokonaisarkkitehtuurin käsitteeseen, oli IBM:n 1960-luvulla käynnistämä Business Systems Planning (BSP) -menetelmä. (Kotusev, 1986.) Vuonna 1975 julkaistu ensimmäinen painos BSP:stä sisälsi monia kokonaisarkkitehtuurille tärkeitä osia, kuten suunnittelua varta vasten valittu ryhmä asiantuntijoita, liiketoiminnan ja IT välinen yhteys sekä prosessien, järjestelmien ja tiedon mallintamiseen liittyvät tekniikat (IBM Corporation, 1975). Informaation ja siihen liittyvien teknologioiden strategisen roolin merkityksestä on alettu puhumaan 1990-luvulla. Silloin esille nostettiin informaation hallinta ja informaation arviointi (engl. information audit), joilla voitaisiin realisoida yhä paremmin informaatioteknologian hyödyt. (Buchanan & Gibb, 1998.) Näillä lähestymistavoilla on ollut vaikutusta kokonaisarkkitehtuurin ja sen kaltaisten käsitteiden muodostumiselle.

Alkunsa kokonaisarkkitehtuurin käsite on saanut Business Systems Planning (BSP) -menetelmän lisäksi tunnetumpien viitekehysten myötä, kuten FEAF (Federal Enterprise Architecture Framework), Zachman Framework ja TOGAF (The Open Group Architecture Framework) (Kotusev, 2016). Zachmanin kehittämä viitekehys on yksi ensimmäisistä kokonaisarkkitehtuurin mallintamiseen laadituista viitekehyksistä ja se tarjoaa kokonaisvaltaisen näkymän organisaatioon. Sen tarkoituksena on muodostaa looginen rakenne, jonka avulla yrityksen eri osa-alueita voidaan jäsentää ja tarkastella eri näkökulmista sekä kuvata yrityksen liiketoimintatarpeita IT-ympäristössä. (Zachman, 1987). FEAF on suunniteltu liittovaltiotason käyttöön ja sen tarkoituksena on edistää liittovaltion tiedon jakamista koko liittovaltion hallituksessa. Liittovaltion kokonaisarkkitehtuurin alle muodostuu suuntaviivojen mukaisesti, mutta erikseen kehitettyjä arkkitehtuurisia segmenttejä, joita käsitellään omakohtaisina yrityksinä. (Goethals, 2005.) TOGAF on organisaatioiden keskuudessa suosituin kokonaisarkkitehtuurin metodologia (Cameron & McMillan, 2013) ja se koostuu kahdesta pääelementistä: Arkkitehtuurin kehitysmenetelmä (ADM) ja arkkitehtuurin sisällön viitekehys (ACF) (TOGAF, 2011). Se sisältää kokonaisarkkitehtuurityön vaiheet ja niistä oletetut tuotokset (TOGAF, 2009). Eri viitekehykset ovat saaneet paljon vaikutteita toisistaan ja edustavat erilaisia lähestymistapoja kokonaisarkkitehtuurille. Kaikkien yhteisiä tavoitteita ovat kuitenkin organisaation liiketoimintastrategian ja IT-infrastruktuurin yhteyden muodostaminen ja yrityksen analysointi yhtenäisenä kokonaisuutena, jossa liiketoiminnan eri osa-alueet ovat linkittyneitä toisiinsa. (Kotusev, 2016.)

Kokonaisarkkitehtuurista on tehty tutkimusta osana riskienhallintaa, jossa esille on nostettu nykyisen toiminnan ongelmallisuus, kun riskienhallintatoimet toteutetaan täysin erillään organisaation muusta toiminnasta, eikä selkeää kartoitusta olla tehty siitä, mihin osa-alueisiin organisaatiossa mahdolliset riskit voisivat vaikuttaa. Tutkimuksessa ehdotetaankin, että riskienhallinta toimet ulottuisivat kokonaisarkkitehtuurin komponentteihin, mikä mahdollistaisi laaja-alaisen analysoinnin siitä, millä tavalla riski vaikuttaa ja leviää organisaation eri osa-alueisiin. Samalla riskienhallintaa päivitetään sitä mukaa, kun muutoksia tapahtuu organisaation kokonaisarkkitehtuurissa. (Barateiro ym., 2012)

Diefenbach ym. (2019) tutkivat 46 julkaisua, jotka keskittyivät riskienhallinnan ja tietoturvanhallinnan tukemiseen kokonaisarkkitehtuurin hallinnan (engl. enterprise architecture management) avulla. Näissä julkaisuissa nousi esille, miten kokonaisarkkitehtuuri tukee tietoturvaa tarjoamalla tietoa organisaation rakenteesta ja IT-järjestelmistä. Sen avulla voidaan myös jäljittää ja yhdistää tunnistetut riskit suoraan organisaation resursseihin, mikä auttaa riskienhallinnassa. Tutkimuksessa nostetaan lisäksi esille, että tietoturvavaatimusten tuomia haasteita suhteessa kokonaisarkkitehtuuriin tulisi tutkia. Tämä korostaa myös tämän tutkielman aihetta kokonaisarkkitehtuurin ja häiriöiden hallinnan osalta.

Al-Turkistani ym. (2021) kävivät läpi tutkimuksessaan eri kokonaisarkkitehtuuriviitekehyksiä ja niiden liiketoimintakyvykkyyksiä keskittyen kyberturvallisuusvaatimusten täyttymiseen. Tutkimus toteutettiin vertaamalla TOGAF:in, SABSA:n ja COBIT 2019:sta sietokykyyn keskittyviä prosesseja. Tutkimuksessa nousi esiin liiketoimintastrategioita tukevien kyberturvallisuusohjeiden välttämättömyys osana kokonaisarkkitehtuuriviitekehyksiä. Digitalisaation myötä yritykset tehostavat toimintaansa IT-ratkaisuilla, mutta samanaikaisesti turvallisuusuhat lisääntyvät. Sietokyvyn merkitys on entistä suurempi organisaatioissa, sillä kyberhyökkäyksen havaitseminen, suojaavat toimenpiteet ja estäminen eivät enää riitä. Organisaatioiden pitää pystyä selviytyä ja palautua hyökkäyksistä entistä tehokkaammin, jotta ne säilyvät toimintakykyisinä. Toteutus tulisi perustaa turvalliseen ja sietokykyiseen kokonaisarkkitehtuuriviitekehykseen, joka integroidaan kehitystyöhön jo varhaisessa vaiheessa.

Sietokykyä ja kokonaisarkkitehtuuria on myös käsitelty osana aikaisempaa tutkimusta, missä on painotettu organisaation kykyä varautua ennakoimattomiin häiriöihin. Tärkeiksi elementeiksi kokonaisarkkitehtuurin suunnittelussa nousivat paikallinen autonomia ja keskitetyt toimintaperiaatteet. Nämä elementit mahdollistaisivat häiriöiden varhaisen tunnistamisen ja tehokkaan hallinnan, mikä johtaisi organisaation sietokyvyn vahvistumiseen. Häiriöiden

sietokyvyllä on vaikutuksia myös muihin organisaation toimintoihin, kuten toimitusketjujen kestävyyteen. (Bemthuis ym., 2020)

Tutkimukset, joissa on perehdytty kokonaisarkkitehtuurin sietokykyyn, pystyvät osittain hyödyntämään tutkiessaan kokonaisarkkitehtuurin roolia häiriötilanteiden hallinnassa. Näissä tutkimuksissa on perehdytty sietokykyyn tiedon tyyppiin (kvalitatiivinen/kvantitatiivinen), häiriön alkuperään (sisäinen/ulkoinen) ja sietokyvyn kestoon (pitkäaikainen/lyhytaikainen) (Aldea ym., 2020), mitkä ovat oleellisia osa-alueita myös häiriötilanteiden hallinnan tutkimisessa.

Tutkimusta on tehty kokonaisarkkitehtuurin hyödyntämisestä osana kriisinhallintaa, mistä löytyy myös häiriötilanteiden hallintaan rinnastettavia elementtejä. Breithaupt ym. (2021) keskittyivät tutkimuksessaan analysoimaan kokonaisarkkitehtuuria yhtenä kriisinhallinnan asiantuntijana. Kokonaisarkkitehtuurin merkitys organisaatioiden kriisitilanteiden hallinnassa on ilmeinen, koska niissä keskitytään jo entuudestaan jatkuvuudenhallintaan, riskienhallintaan, IT-turvallisuuteen, liiketoimintaprosessien hallintaan ja IT-strategiaan. Kokonaisarkkitehtuurin roolia kriisinhallinnassa on tutkittu lisäksi siitä näkökulmasta, miten kriisiarkkitehtuuri hyödyttää myös ”riskialttiiden” tai ”korkean riskin” projektien onnistumisen arvioinnissa (Anthopoulos, 2009).

NIS2-direktiivi on Euroopan parlamentin ja neuvoston 14. joulukuuta 2022 hyväksymä päivitetty säädös, joka laajentaa ja tarkentaa edeltäjänsä NIS-direktiivin soveltamisalaa (Direktiivi (EU) 2022/2555, 2022). Tutkimuskohteena se on edelleen kehittyvä ja suhteellisen vähän käsitelty aihe. Aiheesta tehty tutkimus on usein tarkastellut ja analysoinut direktiiviä yhdessä muiden EU:n kyberturvallisuuslakien kanssa. Tutkimus on keskittynyt lisäksi moniin eri konteksteihin, kuten teollisuuden ohjausjärjestelmiin, telekommunikaatioon, energia- ja vesihuoltosektoreihin sekä tiedonjakoon ja tilannekuvaan liittyviin infrastruktuureihin. NIS2-direktiivin osalta on silti vielä merkittäviä tutkimusaukkoja ja teemoja, joita tulisi käsitellä jatkotutkimusten avulla. (Ruohonen, 2024.)

3 Kokonaisarkkitehtuuri

Tässä luvussa keskitytään kokonaisarkkitehtuurin käsitteeseen ja mitä kokonaisarkkitehtuurin hyödyntäminen yrityksissä tarkoittaa. Luvussa lähdetään selvittämään, miten kokonaisarkkitehtuuri soveltuu kyberturvallisuuden vaatimusten toteuttamiseen ja miten se toimii suhteessa häiriöiden hallintaan. Alaluku 3.1 määrittelee kokonaisarkkitehtuurin käsitteen ja esittelee siihen liittyvät keskeisimmät termit. Kohdassa 3.2 kokonaisarkkitehtuuria tarkastellaan suhteessa kyberturvallisuuteen. Lopussa kohdassa 3.3 syvennytään tutkimaan kokonaisarkkitehtuurin ja häiriönhallinnan (engl. incident management) välistä yhteyttä.

3.1 Määritelmä ja keskeiset käsitteet

Kuehn (2023) määrittelee kokonaisarkkitehtuurin (engl. Enterprise Architecture) viitekehykseksi, jonka avulla voidaan paremmin ymmärtää ja hallita organisaation strategiaa ja kokonaisrakennetta. Se ohjaa suunnittelemaan organisaation tarkoituksenmukaisesti tehokkaaksi, ketteräksi ja arvoa tuottavaksi sekä vähentää monimutkaisuutta ja auttaa liiketoiminnan päätöksenteossa. Kuehn nimittää kokonaisarkkitehtuuria ”usein puuttuvaksi sillaksi strategian ja toimeenpanon välillä”. (Kuehn, 2023.) *”Kokonaisarkkitehtuuri on toiminnan, prosessien, tiedon sekä tietojärjestelmien ja niiden tuottamien palvelujen muodostaman kokonaisuuden rakenne. Sen avulla siis kuvataan organisaation kokonaiskuvaa”* (Arter Oy, haettu 21.02.2025).

Aikaisemmin kokonaisarkkitehtuuria on kuvattu periaatteiden, metodien ja mallien muodostamana yhtenäisenä kokonaisuutena, jota hyödynnetään yrityksen organisaatiorakenteen, liiketoiminta prosessien, tietojärjestelmien ja infrastruktuurin suunnittelussa ja toteutuksessa. Tarkoituksena on hahmottaa kokonaisarkkitehtuurin avulla tärkeimmät osa-alueet liiketoiminnasta, IT:stä ja sen kehityksestä. (Jonkers ym., 2006.) Tamm ym. (2011) mukaan kokonaisarkkitehtuuri muodostaa yhtenäisen rakenteen organisaatiosta, sen IT-infrastruktuurista ja näiden keskinäisistä riippuvuuksista. Kokonaisarkkitehtuuria käytetään organisaation strategisten tavoitteiden tunnistamiseen ja tukemaan ylimmän johdon päätöksentekoa. Se keskittyy hahmottamaan organisaatiota kokonaisvaltaisesti ja tunnistamaan liiketoiminnan sekä teknologian muutosvaikutukset. (Bernard, 2012.)

Kokonaisarkkitehtuuria on nimitetty myös holistisena tapana hallita monimutkaisuutta (Armour ym., 1999; Ross ym., 2006; Winter & Fischer, 2006). Gartnerin (2021) määritelmässä kokonaisarkkitehtuurille korostetaan sen roolia ennakoivana ja kokonaisvaltaisena lähestymistapana häiriötekijöihin. Kokonaisarkkitehtuuri auttaa tunnistamaan ja analysoimaan, miten voidaan

toteuttaa liiketoiminnantavoitteiden mukainen muutos (Gartner, 2021). Kokonaisarkkitehtuurin avulla voidaan suunnitella kestäviä muutoksia sekä tutkia organisaatiota kokonaisvaltaisesti ja läpinäkyvästi (Sousa ym., 2007).

Keskeinen tarkoitus kokonaisarkkitehtuurissa on tukea strategista suunnittelua (Simon ym., 2014). Gartner (2021) mukaan kokonaisarkkitehtuurin arvo piilee sen liiketoiminta- ja IT-johtajille tarjoamissa valmiissa suosituksissa, joiden avulla päätöksenteko toimintaperiaatteiden ja projektien mukauttamisesta hyödyntää liiketoimintaympäristön muutoksia tehokkaasti. Kokonaisarkkitehtuuri luo mahdollisuuden tietoon perustuvaan päätöksentekoon (Närman ym., 2013) ja helpottaa IT-järjestelmien käyttöönoton ohjaamista (Bernard, 2020). Kokonaisarkkitehtuuri tarjoaa yrityksille kokonaiskuvan ja päätöksenteon perustan, joiden avulla voidaan tukea päätöksiä esimerkiksi kustannusten ja monimutkaisuuden vähentämisessä, liiketoiminnan ja prosessien joustavuuden lisäämisessä sekä liiketoiminnan ja IT:n yhteensovittamisen parantamisessa (Tamm ym., 2011). Lisäksi sitä voidaan hyödyntää organisaation muutosprosessien koordinoinnissa (Radake, 2011) sekä sidosryhmien välisen kommunikaation edistämisessä (Lankhorst, 2009).

3.1.1 Rakenne: artefaktit, tuotokset, kyvykkyydet ja viitekehykset

Kokonaisarkkitehtuurin luoma kokonaiskuva organisaatiosta koostuu useista eri osa-alueista, kuten tieto-, prosessi-, tuote-, palvelu-, sovellus- ja IT-arkkitehtuurista. Nämä osa-alueet ovat omia pienempiä kokonaisuuksiaan yrityksen sisällä ja niiden arkkitehtuurikäytännöt kypsyystasoineen eroavat toisistaan. Kokonaisarkkitehtuurin avulla tavoitellaan osa-alueiden muodostamaa yhtenäistä kokonaisuutta, joka mahdollistaa tarvittavan ymmärryksen kysynnän priorisointiin ja keskittyy strategian sovittamiseen päivittäiseen toimintaan. (Jonkers ym., 2006.) Kokonaisarkkitehtuuria voidaan tarkastella näiden osa-alueiden avulla eri taustanäkökulmista, joissa keskiössä on joko IT, liiketoiminta tai hallinto (Dragstra, 2005).

Kokonaisarkkitehtuuri muodostuu komponenteista eli artefakteista (engl. Enterprise Architecture artifacts), jotka ovat erillisiä kokonaisarkkitehtuurin dokumentteja (Winter & Fischer, 2006). Toinen oleellinen komponentti on kokonaisarkkitehtuurin tuotokset (engl. Enterprise Architecture deliverables) (Kurnia ym., 2020). Kokonaisarkkitehtuurin artefaktit antavat erilaisia kuvauksia organisaatiosta, jotta ne olisivat hyödynnettävissä osana päätöksentekoa sekä IT-järjestelmien toteutusta (Abraham, 2013). Listauksia kokonaisarkkitehtuurin artefakteista löytyy useita, minkä vuoksi Kotusev (2017) keskittyi tutkimaan kahdeksaa, jotka ovat käytössä kaikista menestyneimmissä kokonaisarkkitehtuureissa: periaatteet, liiketoimintakyvykkyysmallit, tiekartat, ratkaisukuvaukset, teknologian viitemallit, ohjeistukset, arkkitehtuurin maisemakaaviot ja

ratkaisusuunnitelmat. Kotusev kuitenkin toteaa, että hänen analyysiensa perusteella kohtuullisen kypsät kokonaisarkkitehtuurikäytännöt hyödyntävät yleensä noin 10–15 erilaista kokonaisarkkitehtuurin artefaktia. (Kotusev, 2017.) Kokonaisarkkitehtuurin tuotokset ovat puolestaan artefaktien konkreettisia toteutuksia. Näitä ovat muun muassa liiketoimintakyvykkyydet, liiketoimintapalvelut ja tietojärjestelmäkomponentit (TOGAF, 2009; Winter & Fischer, 2006).

Kokonaisarkkitehtuurissa puhutaan usein kyvykkyyksistä, joilla viitataan arkkitehtuurin aktiivisten rakenteellisten elementtien eli organisaation, henkilön tai järjestelmän hallitsemiin kykyihin. Kyvykkyyksillä ei saada vielä vastausta siihen, miten joku toiminto tulisi suorittaa tai kuka sen suorittaa, ainoastaan mikä toiminto on kyseessä. Muihin kysymyksiin on tarkoitus löytää vastaus kokonaisarkkitehtuurin kautta. (Lankhorst, 2017)

Kokonaisarkkitehtuuriviitekehysten avulla organisaatiot pystyvät hallitsemaan monimutkaisia järjestelmiä ja mahdollistamaan yhteistyön yrityksen sisällä (Al-Turkistani ym., 2021). Ne tarjoavat tarvittavan hallinnan ja kokonaisvaltaisen rakenteen organisaation tietotekniikan ja liiketoiminnan yhdenmukaistamiseen, mikä auttaa tukemaan organisaation strategioita ja liiketoimintatavoitteita (Alshammari, 2017). Sen myötä voidaan alentaa järjestelmän käyttöönoton ja ylläpidon kokonaiskustannuksia vähentämällä monimutkaisuutta yritysjärjestelmän ja liiketoiminnan välillä (Havaluddin, 2012). Erilaisia kokonaisarkkitehtuuriviitekehyksiä on kehitetty useita, joiden tavoitteena on auttaa organisaatioita saavuttamaan tavoitteensa vähentämällä kustannuksia ja monimutkaisuutta eri osa-alueilla (Al-Turkistani ym., 2021). Suosituimpia kokonaisarkkitehtuuriviitekehyksiä ovat muun muassa GERAM, FEAF, DoDAF, DYA, TOGAF, IAF, MIT, ja Gartner. Koska kokonaisarkkitehtuuriviitekehyksiä on tarjolla runsaasti, organisaatioiden voi olla vaikea valita niistä omiin tarpeisiin sopivin. (Bui, 2017.)

TOGAFin mukaan kokonaisarkkitehtuuri viitekehyksessä tulisi olla kaksi pääelementtiä. Nämä ovat kuvaus metodista, jolla arkkitehtuuri aktiviteetti tulisi tehdä sekä määritelmä tuotoksista, jotka aktiviteetti tuottaa. Monet viitekehykset kuitenkin keskittyvät pääasiallisesti näistä vain jälkimmäiseen. (TOGAF, 2002.) Kokonaisarkkitehtuuriviitekehyksellä pyritään tuottamaan organisaatiolle vakiintuneet säännöt, jotka auttavat mukautumaan muuttuviin teknologioihin, lainsäädäntöön ja markkinoiden odotuksiin (TOGAF, 2022). Viitekehyksen tulisi olla helppokäyttöinen, liiketoimintatarpeisiin räätälöity ja mahdollisimman yksinkertainen sekä turvallinen (Al-Turkistani ym., 2021).

3.1.2 Kokonaisarkkitehtuurin hallinta

Kokonaisarkkitehtuurista voidaan puhua tuotteena tai prosessina. Tuote koostuu artefakteista ja tuotoksista, kun taas prosessi kuvaa sitä, miten tuotteet valmistetaan, ylläpidetään, uudelleen sijoitetaan/otetaan uudelleen käyttöön ja poistetaan käytöstä. (Jonkers ym., 2006.) Kokonaisarkkitehtuurin hallinta (engl. Enterprise Architecture Management, EAM) on prosessimuotoista kokonaisarkkitehtuuria. Kokonaisarkkitehtuurin hallinta on tapa hahmottaa ja jäsentää organisaatiojärjestelmää ja sen keskinäisiä riippuvuuksia. Se auttaa organisaation kokonaisuuden monimutkaisuuden hallinnassa ja sen selkeyttämisessä. (Lange & Mendling, 2011.)

Kokonaisarkkitehtuurin mallinnukset voivat keskittyä sekä tiettyyn alueeseen tai näkökulmaan että eri aikaulottuvuuksiin (Tamm ym., 2011). On mahdollista, että kokonaisarkkitehtuuri koostuu jopa tuhansista erilaisista liiketoimintasovelluksista (Buckl ym., 2009). Kokonaisarkkitehtuurin hallinta onkin luonteeltaan monitahoista, mikä johtuu kokonaisarkkitehtuurin elementtien välisten suhteiden ja integraatioiden monimutkaisesta rakennelmasta (Jugel & Schweda, 2014). Kokonaisarkkitehtuurin hallinta luo keskitetyt, ylhäältä johdetut ja koko organisaation kattavat hallintamekanismit, joiden avulla halutaan ylläpitää kokonaisarkkitehtuurin läpinäkyvyyttä, johdonmukaisuutta ja lopulta joustavuutta (Winter, 2016). Kokonaisarkkitehtuurin hallinnan avulla voidaan yhdistää strategia sekä organisaation rakenne, prosessit ja toiminnot (Breithaupt ym., 2021).

Kokonaisarkkitehtuurin hallintaa voidaan käyttää johtamismenetelmänä, jonka avulla voidaan ohjata kokonaisvaltaisten ja kestävien muutosten toteuttamista. Muutokset voivat olla strategisia tai operatiivisia. Kokonaisarkkitehtuurin hallinta mahdollistaa liiketoimintakyvykkyyksien ja organisaation resurssien huomioimisen osana muutosten suunnittelua. Kokonaisarkkitehtuurin hallintaan liittyvissä johtamistoiminnoissa keskitytään integroimaan strategia osaksi kokonaisarkkitehtuurin toteutusta ja sen avulla tavoiteltavia tuloksia. (Ahlemann ym., 2012.)

3.1.3 Haasteet ja kritiikki

Monista hyödyistään huolimatta kokonaisarkkitehtuurin ajatellaan usein vaativan merkittäviä investointeja, mistä ei kuitenkaan synny tarpeeksi konkreettista apua esimerkiksi päätöksentekoon. Kokonaisarkkitehtuuri koetaan abstraktiksi käsitteeksi, eikä sen aikaansaamia tuloksia ole helppo osoittaa käytännössä. (Lange ym., 2016.) Vaikka kokonaisarkkitehtuurista on tehty jo merkittävästi tutkimusta ja mielenkiinto aihetta kohtaan kasvaa, yleinen ymmärrys kokonaisarkkitehtuurista ja sen hyödyntämisestä on edelleen heikkoa. Mainittuja syitä tuntemuksen heikkoudelle ovat

kokonaisarkkitehtuurin monitieteiset piirteet, kielelliset haasteet, aiheeseen liittyvän tutkimuksen rakenne sekä havainnointitapaan liittyvät tekijät. Tähän haasteeseen liittyen ei vielä ole tehty merkittävää määrää tutkimusta. (Saint-Louis & Lapalme, 2016.) Lisäksi haasteeksi kokonaisarkkitehtuuriprosessille muodostuu sidosryhmien erilaiset tarpeet ja tietämys aiheesta sekä organisaation kokonaisarkkitehtuurista (Rehring ym., 2019).

Tutkimusten mukaan kokonaisarkkitehtuurin hyödyntäminen päätöksenteossa jää usein alhaiseksi, sen todetuista hyödyistä huolimatta (Hiekkanen ym., 2013; Löhe & Legner, 2014). Yksi esitetty syy tälle on kokonaisarkkitehtuurin visualisointien ja mallinnusten laatu sekä niiden ymmärryksentaso (Buckl ym., 2009; Löhe & Legner, 2014). Kokonaisarkkitehtuuriprosessiin liittyy myös ylläpidollisia ongelmia, joissa kokonaisarkkitehdit eivät ehdi tai pysty päivittämään ja dokumentoimaan kaikkia muutoksia puutteellisen työkalutuen takia (Kleehaus & Matthes, 2021).

3.2 Kokonaisarkkitehtuuri ja kyberturvallisuus

Organisaatiot kohtaavat järjestelmien käyttöönotossa haasteita teknologioihin liittyvien kyberuhkien vuoksi. Kyberuhat kehittyvät ja muuttuvat jatkuvasti, mikä tekee turvallisen ja tarkoituksenmukaisen järjestelmän käyttöönotosta monimutkaista. Siksi kyberturvallisuus tulisi integroida kokonaisarkkitehtuurin suunnitteluun jo varhaisessa vaiheessa. Turvallisuusnäkökulmien huomioiminen vahvistaa organisaatioiden kykyä puolustautua kehittyneitä kyberuhkia vastaan. Kyberuhkia voidaan lieventää hyväksyttävälle tasolle, kun turvallisuus ja järjestelmän palautumiskyky otetaan huomioon jo järjestelmän kehityksen alkuvaiheessa. (Al-Turkistani ym., 2021.)

On olemassa kokonaisarkkitehtuuriviitekehyksiä, jotka ottavat huomioon turvallisuuteen liittyviä näkökohtia, kuten SABSA (The SABSA Institute, ei pvm.), mutta viitekehystä, joka pystyisi vastaamaan kattavasti eri sidosryhmien turvallisuusvaatimuksiin, ei tällä hetkellä vielä ole (Al-Turkistani ym., 2021). Viitekehyksen on katettava koko organisaation rakenteet ja prosessit huomioiden olennaiset tietoturvavaatimukset. Koko organisaation tulee sitoutua viitekehyksen mukaisten tietoturvavaatimusten toteuttamiseen, jotta saadaan muodostettua kokonaisvaltaisesti turvallinen kokonaisarkkitehtuuri, joka heijastaa eri osastojen ja toimijoiden tarpeita. (Alonso ym., 2010.)

Monet kokonaisarkkitehtuuriviitekehykset ovat vielä puutteellisia turvallisuustoimenpiteiden osalta, mikä jättää organisaatiot entistä haavoittuvammaksi uhille ja riskeille. Viitekehysten tulisi liiketoiminta vaatimusten lisäksi sisällyttää kyberturvallisuuteen liittyviä ohjeistuksia, jotka ovat

linjassa kokonaisarkkitehtuurin liiketoimintastrategioiden kanssa. Organisaatioiden laatu- ja turvallisuusvaatimukset ovat entistä korkeammalla, mikä tekee vakaiden ja luotettavien kokonaisarkkitehtuuriviitekehysten rakentamisesta entistä haastavampaa. Myös ulkoiset sidosryhmät, kuten toimittajat ja kumppanit, jotka ovat yhteydessä yrityksen sisäisiin ja/tai ulkoisiin verkkoihin, tarvitsevat turvallisesti integroidun järjestelmän päivittäisten tehtäviensä hoitamiseen. (Al-Turkistani ym., 2021)

Organisaatioille on erittäin tärkeää sisällyttää kokonaisvaltaiset ja integroidut tietoturvakäytännöt osaksi kokonaisarkkitehtuuriviitekehystä. Tämä on olennaista, jotta järjestelmät voidaan suojata tehokkaasti, liiketoiminnan tavoitteita tukea ja kyberturvallisuusriskejä hallita. Koska tietoturva vaikuttaa koko organisaatioon, on tietoturvan oltava linjassa organisaation strategian kanssa, eikä sitä tule nähdä vain jälkikäteen lisättävänä osana. Tietoturvariskien hallinta tulisi yhdistää tiiviisti koko organisaation riskienhallintaan. On tärkeää määritellä selkeästi tietoturvan vastuut ja roolit. Lisäksi tietoturvan on vastattava sekä sisäisten että ulkoisten sidosryhmien odotuksiin, mikä vaikuttaa luottamukseen ja sääntöjen noudattamiseen. Organisaatioiden tulisi keskittyä pelkän puolustautumisen sijaan myös kykyyn palautua häiriöistä, sillä kyberturvallisuusuhkien jatkuvan kehityksen myötä niitä ei voida täysin välttää. (Ghaznavi-Zadeh, 2017; Truyen, 2018)

3.3 Kokonaisarkkitehtuuri ja häiriöiden hallinta

Häiriötilanne tarkoittaa odottamatonta tapahtumaa, häiriötä tai poikkeamaa, joka vaikuttaa järjestelmän normaaliin toimintaan, prosesseihin tai vakauteen. Organisaation näkökulmasta tilanne voi edetä kriisiksi, kun tapahtumalla on johtajien ja sidosryhmien mielestä merkittävä, odottamaton ja haitallinen vaikutus organisaation toimintaan (Bundy ym., 2017). Myöhemmin tutkielmassa käsiteltävässä NIS2-direktiivissä häiriö on määritelty ”tapahtumaksi, joka vaarantaa tallennettujen, siirrettyjen tai käsiteltyjen tietojen tai verkko- ja tietojärjestelmien tarjoamien tai niiden kautta saatavilla olevien palveluiden saatavuuden, aitouden, eheyden tai luottamuksellisuuden”. (Direktiivi (EU) 2022/2555, 2022.)

Organisaatioiden on entistäkin tärkeämpää kehittää kykyään toimia häiriötilanteissa ja sietää niiden vaikutuksia, sillä niihin kohdistuvat uhat liittyvät yhä useammin turvallisuuteen. Kyse ei ole pelkästään häiriöiden hallinnasta vaan lisäksi jatkuvuudenhallinnan ja palautumiskyvyn kehittämisestä. Näiden sisällyttäminen organisaation kokonaisarkkitehtuuriin parantaa merkittävästi organisaation kykyä toimia kyberturvallisuuteen liittyvissä häiriötilanteissa ja mahdollistaa nopean palautumisen niiden jälkeen. (Al-Turkistani ym., 2021.)

Organisaatioiden tulisi huomioida monenlaisia osa-alueita suunnitellessaan oman sietokykynsä toteutusta ja kehittämistä. Yksi tapa on häiriöiden hallintasuunnitelman (engl. incident response plan) kehittäminen, jolla pyritään lieventämään, rajaamaan ja hallitsemaan häiriön aiheuttamia vaikutuksia. Sitä seurataan häiriön sattuessa, jotta häiriöön voidaan reagoida mahdollisimman nopeasti ja tehokkaasti. Tämä vähentää myös häiriön vaikutuksia, sillä hallintasuunnitelmaan kuuluvissa toimenpiteissä keskitytään poistamaan uhkia, minimoimaan vahingot ja edistämään palautumista. (Al-Turkistani ym., 2021)

Organisaatioille on entistäkin tärkeämpää rakentaa sietokykyyn perustuvia lähestymistapoja, jotka ulottuvat pelkkää suojautumista, havaitsemista ja estämistä pidemmälle. Tärkeässä osassa on organisaation kyky hallita uhkia ja riskejä sekä toimia suunnitelmallisesti häiriön toteutuessa. Kybersietokyky muodostuu tällöin osaksi kokonaisvaltaista turvallisuusstrategiaa. (Al-Turkistani ym., 2021.) Häiriöiden hallinnassa organisaation sietokyky on keskeinen tekijä. Tämän varmistamiseksi sietokyky tulisi suunnitella ja rakentaa osaksi organisaation kokonaisarkkitehtuuria. Nykyisessä epävarmassa toimintaympäristössä korostuu entisestään kyky arvioida ja kehittää arkkitehtuurin sietokykyä osana riskienhallintaa. (Aldea ym., 2020.)

4 Network and Information Security Directive 2 (NIS2)

Tässä osiossa käsitellään Euroopan unionin kyberturvallisuusdirektiiviä NIS2, jonka tarkoituksena on suojata kriittisten sektoreiden verkko- ja tietojärjestelmiä sekä saavuttaa korkea ja yhteinen kyberturvallisuustaso Euroopan unionissa. Alaluvussa 4.1 kerrotaan NIS2-direktiivistä tarkemmin ja käydään läpi sen tausta sekä tavoitteet. Tämän jälkeen osiossa 4.2 keskitytään selvittämään NIS2-direktiivin asettamat vaatimukset organisaatioille. Alaluku 4.3 käsittelee NIS2-direktiiviä ja sen vaikutuksia kyberturvallisuuteen. Viimeisessä alaluvussa 4.4 käsitellään NIS2-direktiivin yhteyttä häiriöiden hallintaan.

4.1 NIS2-direktiivin tausta ja tavoitteet

NIS2-direktiiviä edeltänyt NIS-direktiivi hyväksyttiin vuonna 2016. Sen tavoitteena oli asettaa yhteinen kyberturvallisuuden taso EU:ssa tietyille olennaisten palvelujen toimijoille ja digitaalisten palvelujen tarjoajille. (Eckhardt & Kotovskaia, 2023.) NIS-direktiivi oli ensimmäinen kattava EU-lainsäädäntö, jonka tavoitteena oli vahvistaa verkko- ja tietojärjestelmien kyberturvallisuutta turvaten EU:n taloudelle ja yhteiskunnalle elintärkeät palvelut (Euroopan komissio, 2025a). Direktiivi asetti digitaalisille palveluntarjoajille vaatimukset, jotka tulisi huomioida kyberturvallisuuteen liittyvien riskien hallinnassa, sekä parametrit sen arvioimiseksi, onko kyberturvallisuustapahtumalla tai -häiriöllä merkittävä vaikutus (Direktiivi (EU) 2016/1148, 2016).

Direktiivin toimeenpano sai jäsenvaltioissa nostettua kyberturvallisuuden esille aikana, jolloin sen käsittelyä ei olisi aloitettu vielä omatoimisesti. Kyberturvallisuus ei käsitä alueellisia rajoja, minkä vuoksi direktiivin tuloksena syntyneet yhteistyö- ja koordinaatiomekanismit jäsenvaltioiden välille olivat erityisen merkityksellisiä. Direktiivin myötä määriteltiin yhteiskunnallisesti ja taloudellisesti keskeiset palvelualat, joiden turvallisuuden parantamiseen tulisi keskittyä sekä asetettiin eri sääntelytasot olennaisten palvelujen tarjoajille ja digitaalisten palvelujen tarjoajille. Direktiiviin kirjattiin myös, miten sääntöjä sovelletaan käytännössä. (Vandezande, 2024)

NIS-direktiivin antoi EU:n jäsenvaltioille merkittävästi päätäntävaltaa siitä, miten direktiivin täytäntöönpano toteutettiin, mikä johti selkeisiin eroihin jäsenvaltioiden välillä. Tämä johti siihen, että NIS-direktiivi oli käytössä EU:n sisällä eri tavoilla. (Biasin & Kamenjašević, 2022.) Kun jäsenvaltiot toteuttivat direktiivin vaatimuksia eri tavoilla, syntyi myös eroja toimintavalmiudessa ja direktiiviin liittyvissä kustannuksissa (Euroopan komissio, 2020). Merkittävä puute NIS-direktiivissä oli se, ettei siinä huomioitu eri alojen välisiä riippuvuuksia ja yhteyksiä (Euroopan komissio, 2020; Schmitz-Berndt, 2023). Kyberturvallisuuteen liittyvät uhkat ja riskit kasvoivat ja

samalla tunnistettiin NIS-direktiiviin liittyvät puutteet, minkä seurauksena alkuperäinen direktiivi kumottiin ja luotiin uusi kattavampi NIS2-direktiivi (Euroopan komissio, 2020).

Direktiivin uudistaminen käynnistyi joulukuussa 2020, uusi NIS2-direktiivi tuli voimaan 2023 ja jäsenmaiden oli saatettava direktiivi osaksi kansallista lainsäädäntöä 17. lokakuuta 2024 mennessä (Euroopan komissio, 2025a). Näistä vaatimuksista huolimatta Suomi ei onnistunut saattamaan direktiiviä ajoissa osaksi lainsäädäntöä, sillä lakiesitys jumittui eduskunnassa (Kolehmainen, 2024). Euroopan komissio ilmoitti 28. marraskuuta 2024 lähettäneensä 23 jäsenvaltiolle, mukaan lukien Suomelle, virallisen huomautuskirjeen epäonnistumisesta saattaa NIS2-direktiivi ajallaan täysin voimaan. Suomen lisäksi huomautuskirjeen saajia olivat Alankomaat, Bulgaria, Espanja, Irlanti, Itävalta, Kreikka, Kypros, Latvia, Luxemburg, Malta, Portugali, Puola, Ranska, Romania, Ruotsi, Saksa, Slovakia, Slovenia, Tanska, Tšekki, Unkari ja Viro. Jäsenvaltioille annettiin kaksi kuukautta aikaa vastata, saattaa täytäntöönpano päätökseen ja ilmoittaa toimenpiteistään komissiolle. (Euroopan komissio, 2024.) Vielä 4. maaliskuuta 2025, kolme kuukautta huomautuskirjeestä, Suomi ei ollut saattanut täytäntöönpanoa loppuun täydellisesti (Euroopan komissio, 2025b).

NIS2-direktiivi laajensi edeltäjänsä NIS-direktiivin soveltamisalaa ja velvoitteita huomattavasti. Tavoitteena direktiiville on parantaa EU:n kriittisen infrastruktuurin ja digitaalisten palveluiden sietokykyä. (Ferguson, 2023; Rehbohm & Moses, 2023.) Merkittävä ero edelliseen direktiiviin on tärkeiden toimijoiden lisääminen, mikä kattaa muun muassa posti- ja kuriiripalvelut, jätehuollon, kemianteollisuuden, tuotannon ja jakelun sekä elintarvikkeiden tuotannon, jalostuksen ja jakelun sekä digitaaliset palveluntarjoajat (Direktiivi (EU) 2022/2555, 2022). NIS2-direktiivi keskittyy kriittisten sektoreiden verkko- ja tietojärjestelmien turvallisuuden lisäksi laajemmin kyberturvallisuuteen eli kyseisten järjestelmien käyttäjien ja muiden kyberuhkien vaikutusten alaiseksi joutuneiden henkilöiden suojaamiseen (Biasin & Kamenjašević, 2022; Chiara, 2022). NIS2-direktiivin tarkoituksena on parantaa sekä kansallisia että kansainvälisiä tiedonjakokäytäntöjä laajentamalla tietoturvapoikkeamien ilmoitusvelvollisuutta alkuperäisestä NIS-direktiivistä. Alkuperäiseen NIS-direktiiviin kuuluivat kansalliset CSIRT-tiimit (Computer Security Incident Response Team), joille tietoturvapoikkeamista, uhista ja läheltä piti -tilanteiden tuli ilmoittaa, mutta uudessa direktiivissä ilmoitusaika on yhä tiukempi. (Direktiivi (EU) 2022/2555, 2022; Scheelen ym., 2023.) EU:n tavoite on torjua laajamittaisia kyberhäiriöitä, kyberrikollisuutta, tukea sietokykyä ja hallinnoida rahoitusta asettamalla yhtenäistämisstrategian kyberturvallisuuden hallintaan (Jacuch, 2021).

4.2 NIS2:n vaatimukset organisaatioille

EU:n tavoite saavuttaa korkea kyberturvallisuuden taso koko Euroopassa toteutetaan asettamalla vähimmäisvaatimukset, jotka organisaatioiden on täytettävä NIS2-direktiivin mukaisesti (Ferguson, 2023; Rehbohm & Moses, 2023). NIS2-direktiivi asettaa tiukempia vaatimuksia kansallisten viranomaisten valvonnalle ja sääntöjen täytäntöönpanolle. Direktiivi ei jätä jäsenvaltioille liikkumavaraa eli mahdollisuutta säätää omia, kevyempiä sääntöjä (Valtioneuvosto, 2023). NIS2-direktiivin velvoitteisiin kuuluu riskienhallinta, kyberturvallisuuden hallinta ja EU:n jäsenvaltioiden välinen koordinointi ja raportointi. Direktiivi laajentaa soveltamisalaansa kattamaan uusia sektoreita, lisää vastuuta toimitusketjuista, vahvistaa häiriöiden hallintaa ja tiukentaa aikarajoja tapahtumien ja häiriöiden raportoinnille. Lisäksi se velvoittaa jäsenvaltiot määräämään sakkoja asetusten rikkomisesta. (Direktiivi (EU) 2022/2555, 2022.)

Direktiivi koskee sekä yksityisen että julkisen sektorin toimijoita (Direktiivi (EU) 2022/2555, 2022). Toimialat, jotka kuuluvat kriittisiin sektoreihin ovat NIS2-direktiivissä laajemmat kuin sen edeltäjässä NIS1-direktiivissä (Veigurs ym., 2024). Kriittisyyttä on arvioitu uusia sektoreita niiden taloudellisen ja sosiaalisen kriittisyyden, keskinäisriippuvuuden ja digitalisaation perusteella. Lisäksi toimialojen välillä tehdään jako erittäin kriittisiin ja kriittisiin sektoreihin. Erittäin kriittisiin sektoreihin kuuluvat avaruus, energia, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveydenhuolto, liikenne, juoma- ja jätevesi, julkishallinto, tietoturva- ja hallintapalveluita tarjoavat ICT-toimijat sekä digitaalinen infrastruktuuri. Kriittisiin sektoreihin lukeutuvat elintarvikeala, jätehuolto, posti- ja kuriiripalvelut, kemikaaliala, tutkimustoiminta, digitaalisten palvelujen tarjoajat sekä tietyt alat valmistavassa teollisuudessa, kuten lääkinnällisten laitteiden valmistajat ja autoteollisuus. (Direktiivi (EU) 2022/2555, 2022.)

Toimijoiden luokittelussa on tehty päätöksiä lisäksi koon perusteella. NIS2-direktiivi on suunnattu keskikokoisille ja suurille julkisille tai yksityisille kriittisten sektorien toimijoille. Direktiivi ei lähtökohtaisesti velvoita pieniä tai mikroyrityksiä, mutta tiettyjen alojen toimijat sisältyvät soveltamisalaan koosta riippumatta. Näitä ovat toimijat, jotka:

- tarjoavat julkisia sähköisiä viestintäverkkoja tai -palveluja, luottamuspalveluja tai verkkotunnusrekisteröintiä
- ovat ainoa palveluntarjoaja jäsenvaltiossa kriittisille yhteiskunnallisille tai taloudellisille toiminnoille

- palvelun häiriö voisi merkittävästi vaikuttaa julkiseen turvallisuuteen, terveyteen tai aiheuttaa järjestelmäriskejä
- ovat kriittisiä tietyn toimialan tai keskinäisten riippuvuuksien vuoksi
- ovat valtion tai aluehallinnon viranomaisia – jäsenvaltiot voivat laajentaa tämän myös paikallishallintoon ja oppilaitoksiin. (Direktiivi (EU) 2022/2555, 2022)

On kuitenkin huomioitava, että direktiivi ei velvoita pelkästään kriittisen sektorin toimijaa vaan lisäksi sen toimitusketjuun kuuluvia sidosryhmiä, joiden kanssa toimijalla on riippuvuussuhde (Direktiivi (EU) 2022/2555, 2022). Direktiivin toimitusketjujen turvallisuuteen ja toimittajasuhteisiin liittyvillä organisaatiovaatimuksilla halutaan puuttua toimitusketjujen kyberturvallisuusriskeihin (Euroopan komissio, 2023). Organisaatioon voi siis kohdistua velvoitteita NIS2-direktiivin osalta, joko suoraan tai välillisesti (Direktiivi (EU) 2022/2555, 2022). Kyberturvallisuus suositellaan sisällytettäväksi osaksi sopimusjärjestelyjä toimitusketjuun kuuluvien organisaatioiden kanssa. Toimija on sopimuksesta huolimatta velvoitettu varmistamaan, että toimitusketjussa noudatetaan asianmukaisia ja oikeasuhteisia turvatoimia. (Eckhardt & Kotovskaia, 2023.)

EU:n jäsenvaltioissa on herännyt keskustelua siitä, direktiivissä mainittujen alojen hallintoa ja sääntelyä tulisi lähestyä. Päätökseen siitä, miten NIS2-direktiivi saatetaan osaksi kansallista lainsäädäntöä ja miten sen vaatimuksia käytännössä sovelletaan, vaikuttavat monet tekijät, kuten maan koko, toimijoiden määrä ja kansallinen lainsäädäntö. (Veigurs ym., 2024.) Lisäksi kriittisen infrastruktuurin määritelmä vaihtelee maiden välillä, minkä vuoksi eroja syntyy NIS2-direktiivin soveltamisalan osalta (Vandezande, 2024).

NIS2-direktiivi asettaa pakollisia vaatimuksia, joilla pyritään varautumaan kyberturvallisuusriskeihin ja parantamaan niiden hallitsemista. Direktiivin vaatimukset koskevat sekä erittäin kriittisten sektorien toimijoita että kriittisten sektorien toimijoita. Vaatimukset voidaan jakaa neljään osa-alueeseen, jotka ovat riskienhallinta, yritysjohdon vastuu, raportointivaatimukset ja jatkuvuuden hallinta. Erittäin kriittisten sektorien toimialoilla sekä kriittisten sektorien toimialoilla pitää vaatimusten lisäksi toteuttaa turvallisuustoimenpiteitä, jotka jaetaan teknisiin, operatiivisiin ja organisatorisiin. Direktiiviin on listattu, että toimenpiteiden tulee sisältää vähintään seuraavat osa-alueet:

- linjaukset riskianalyyseihin ja tietojärjestelmien turvallisuuteen

- häiriöiden käsittely
- jatkuvuudenhallinta, johon sisältyy muun muassa kriisinhallinta ja toipumissuunnitelma
- toimitusketjujen turvallisuus
- verkko- ja tietojärjestelmien koko elinkaareen turvallisuus
- linjaukset ja arviointitoimenpiteet kyberturvallisuuden riskienhallinnan tehokkuuteen
- kyberturvallisuuskäytännöt ja koulutukset
- linjaukset ja toimenpiteet salauksen ja kryptografian käyttöön
- henkilöstöturvallisuus, käyttöoikeuksien hallinta ja omaisuuden hallinta
- monivaiheinen ja jatkuva tunnistautuminen, suojatut viestintä- ja hätäjärjestelmät organisaation sisällä (Direktiivi (EU) 2022/2555, 2022)

Direktiivi edellyttää organisaatioita varmistamaan verkko- ja tietojärjestelmiensä asianmukaisen turvatason, huomioiden niihin kohdistuvat riskit (Eckhardt & Kotovskaia, 2023). Organisaation on varmistettava, että se täyttää vaatimukset ja toteuttaa tarvittavat toimenpiteet saavuttaakseen riittävän operatiivisen riskienhallinnan ja kybersietokyvyn. Tämä on kokonaisuus, joka edellyttää merkittävää muutosjohtamisen osaamista. Vaatimustenmukaisuuden saavuttaminen edellyttää, että sidosryhmillä on riittävä tietoisuus, ymmärrys ja asiantuntemus. (Asikainen, 2024)

Jotta NIS2-direktiivin vaatimukset olisivat täytetty, tulee organisaatioiden lisäksi huomioida alan viimeisimmät kehitykset sekä tarvittaessa asiaankuuluvat eurooppalaiset ja kansainväliset standardit. Direktiivin noudattamisen varmistamiseksi jäsenvaltioiden on määrättävä hallinnollisia sakkoja, mikäli organisaatiot eivät toteuta asetettuja vaatimuksia. Sakot voivat olla enintään 10 miljoonaa euroa tai 2 % yrityksen koko maailmanlaajuisesta vuotuisesta liikevaihdosta. (Direktiivi (EU) 2022/2555, 2022.) NIS2-direktiivi on tutkimusten mukaan sääntelyltään ja ohjeistuksiltaan vielä joustava ja tulkinnanvarainen, minkä takia tarvetta lisätoimeenpanosäädöksille ja tapaustutkimuksille löytyy yhä (Vandezande, 2024).

4.3 NIS2 ja Kyberturvallisuus, Cyber Solidarity Act

NIS2 toimii yleisenä kyberturvallisuuslakina, mutta se ei vaikuta alakohtaisten erityislakien soveltamiseen. Tämä vahvistaa NIS2:n asemaa EU:n kyberturvallisuuden keskeisenä

lainsäädäntönä, mutta jättää samalla tilaa tarkemmin rajatuille säädöksille, kuten digitaalisten tuotteiden tai rahoitusalan turvallisuutta koskeville laeille. (Direktiivi (EU) 2022/2555, 2022)

NIS2-direktiivi määrittelee kyberturvallisuuden Euroopan parlamentin ja neuvoston aiemmin antaman asetuksen mukaan ”toimiksi, jotka ovat tarpeen verkko- ja tietojärjestelmien, niiden käyttäjien sekä muiden kyberuhkien vaikutuksen kohteeksi joutuvien henkilöiden suojaamiseksi” (Asetus (EU) 2019/881, 2019; Direktiivi (EU) 2022/2555, 2022). Kyberturvallisuuden tavoitteena on saavuttaa luottamuksellisuus, eheys ja saatavuus (Bayuk ym., 2012). NIS2-direktiivissä verkko- ja tietojärjestelmien turvallisuuden määritelmässä korostetaan, että näiden järjestelmien kohdalla pitää saavuttaa tietty varmuus siitä, että ne pystyvät säilyttämään häiriön tullen sekä tallennettujen, siirrettyjen tai käsiteltyjen tietojen että näiden järjestelmien tarjoamien tai niiden kautta saatavien palvelujen saatavuuden, aitouden, eheyden ja luottamuksellisuuden (Direktiivi (EU) 2022/2555, 2022).

EU:ssa on rakennettu yhteistä kyberturvallisuutta lisäksi muilla asetuksilla kuten DORA (Digital Operational Resilience Act), kyberkestävyyssäädös (engl. Cyber Resilience Act, CRA) ja kybersolidaarisuussäädös (engl. Cyber Solidarity Act, CSA). DORA-asetus keskittyy finanssialan digitaaliseen häiriönsietokykyyn eli kykyyn sietää tietojärjestelmien vikoja ja häiriöitä (Asetus (EU) 2022/2554, 2022). Kyberkestävyyssäädös määrittää kyberturvallisuuden vähimmäisvaatimukset laitteille ja ohjelmistoille, jotka sisältävät digitaalisia elementtejä ja voivat olla suoraan tai epäsuorasti yhteydessä toisiin laitteisiin tai verkkoon (Asetus (EU) 2024/2847, 2024).

Kybersolidaarisuussäädös poikkeaa tarkoituksellaan kolmesta muusta EU:n kyberturvallisuussäädöksestä, sillä se keskittyy parantamaan kyberturvallisuuteen liittyvää valmiutta, havainnointia ja reagointia häiriöihin (Euroopan komissio, 2025c). Se pyrkii paikkaamaan aukon reaaliaikaisessa tapahtumavasteessa, rajat ylittävässä solidaarisuudessa ja koordinoidussa kyberpuolustuksessa. Asetuksen keskiössä on kriisitilanteiden hallinta ja operatiivinen yhteistyö, mitä toteutetaan mekanismeilla, joilla pyritään lieventämään ja reagoimaan suuriin kyberturvallisuuskriiseihin. Asetuksen avulla halutaan saavuttaa kybertoimintaympäristön kollektiivinen puolustus, jossa kyberhyökkäyksiä katsotaan koko EU:n haasteena eikä kansallisena ongelmana. Yhteinen valmius, nopea reagointi ja koko Euroopan laajuiset kyberpuolustuskyvykkyydet rakentavat EU:n kybersietokykyä. (Asetus (EU) 2025/38, 2024; Nis-2-directive.com, haettu 31.3.2025.)

NIS2-direktiivi luo perustan EU:n kyberturvallisuuden hallintaan ja häiriöiden raportointiin. Kybersolidaarisuussäädös määrittää suunnan yhteistyölle ja ohjaa reagointikyvyn parantamiseen.

NIS2-direktiivi ja kybersolidaarisuussäädös ovat toisiaan tukevia, vaikka niissä painotetaan eri asioita. NIS2-direktiivi määrää kyberturvallisuuteen liittyvät vähittäisvaatimukset erittäin kriittisten ja kriittisten sektorien toimijoille ja kybersolidaarisuussäädös puolestaan keskittyy muodostamaan EU:n laajuiset kyberhätätilanteiden torjunta- ja valmiusmekanismit. NIS2-direktiivin keskiössä on varmistaa organisaatioiden säädösten mukainen toiminta ja se kannustaa yhteistyöhön, kun taas kybersolidaarisuussäädöksen on tarkoitus vahvistaa rajojen ylittävää tukea EU:n jäsenvaltioissa, jotta mittavissa kyberhäiriöissä voidaan saada tukea yhteistyöstä. Kybersolidaarisuussäädös sisältää erityisiä hätätilanteiden hallintamekanismeja, joita NIS2-direktiivi ei sisällä, minkä vuoksi suurten kyberhäiriöiden hallinnassa säädös menee soveltamisessa direktiivin edelle. (Asetus (EU) 2025/38, 2024; Nis-2-directive.com, haettu 31.3.2025)

4.4 NIS2 ja Häiriöiden hallinta

Euroopan komissio vaatii jäsenvaltioltaan lainsäädännön täydellistä täytäntöönpanoa, sillä se on avainasemassa julkisten ja yksityisten toimijoiden sietokyvyn ja häiriötilanteiden hallintakyvyn parantamisessa direktiivissä luokitelluilla kriittisillä sektoreilla ja koko EU:ssa (Euroopan komissio, 2024). NIS2-direktiivi asettaa organisaatioille vaatimuksia siitä, miten niiden tulee hallita tietoturvaan ja verkkojen toimivuuteen liittyviä häiriöitä (Ferguson, 2023). Direktiivissä häiriöiden hallinta on määritelty kattavan kaikki toiminnot, joilla pyritään ehkäisemään, havaitsemaan, analysoimaan ja rajoittamaan tai käsittelemään häiriötä niin, että siitä voidaan palautua (Direktiivi (EU) 2022/2555, 2022). NIS2-direktiivin määritelmä häiriölle on käsitelty aikaisemmin tutkielmassa alaluvussa 3.3.

Jäsenvaltioiden tulee perustaa CSIRT-tiimi (Computer Security Incident Response Team), jotka vastaavat merkittävien häiriöiden ilmoituksien käsittelystä ja tarvittaessa jatkotoimista. CSIRT-tiimien tarkoituksena on muodostaa kokonaiskuva mahdollisista kyberuhkista ja pystyä tehokkaasti aloittamaan tarvittavat toimenpiteet häiriön sattuessa. Ajatuksena on, että CSIRT-tiimit ylläpitävät Euroopan unionin jäsenvaltioiden välistä yhteistyötä kyberturvallisuuden takaamiseksi. Jäsenvaltioiden on huolehdittava CSIRT-tiimien salassapitovelvollisuudesta ja luotettavuudesta, sillä tiimit käsittelevät suuria määriä dataa, joka voi usein sisältää arkaluontoista tietoa. (Direktiivi (EU) 2022/2555, 2022)

Erittäin kriittisten sektorien ja kriittisten sektorien toimijoiden tulee ilmoittaa alustavasti tunnistamistaan merkittävistä häiriöistä oman valtionsa CSIRT-tiimille tai vastaavan tasoiselle viranomaiselle 24 tunnin sisällä. 72 tuntia häiriön huomaamisen jälkeen pitää pystyä lähettämään varsinainen häiriöilmoitus, mutta ilmoitus tulisi tehdä niin nopeasti kuin mahdollista. Myöhemmällä

ilmoituksella päivitetään ensimmäisessä ilmoituksessa annettuja tietoja ja tehdään jo arvio häiriön vakavuudesta, mahdollisista vaikutuksista ja vaarantumisindikaattoreista (engl. Indicators of Compromise, IOC). Lopullinen raportti tulee toimittaa viimeistään kuukauden kuluttua varsinaisesta häiriöilmoituksesta. Ilmoitusten aikarajan taustalla vaikuttaa se, että tieto häiriöstä saadaan mahdollisimman nopeasti ja voidaan aloittaa tarvittavien toimenpiteiden suorittaminen. Direktiivissä nostetaan kuitenkin esille, että raportointivelvoitteiden ei pitäisi viedä liikaa resursseja itse häiriön ratkaisemiselta. (Direktiivi (EU) 2022/2555, 2022)

NIS2-direktiivissä painotetaan muiden vaatimusten ohella organisaatioiden kybersietoisuutta. Kybersietoisuus on kokonaisuus erilaisia kyvykkyyksiä. Näiden kyvykkyysien avulla organisaatio on valmiimpi tunnistamaan uhkia, haavoittuvuuksia ja riskejä, jotka siihen kohdistuvat ja voisivat mahdollisesti aiheuttaa negatiivisia vaikutuksia sen toimintaan. Kyvykkyyksien avulla myös suojaudutaan kyberhyökkäyksiltä, havaitaan realisoituneet hyökkäykset, reagoidaan niihin sekä palaudutaan hyökkäyksien jälkeen. Tämän ohella tärkeää on, että organisaatio ylläpitää tilannekuvaa kyberturvallisuudestaan. (Asikainen, 2024)

NIS2-direktiivin rinnalla toinen Euroopan parlamentin ja neuvoston samana päivänä 14. joulukuuta 2022 julkaisema direktiivi on kriittisten toimijoiden fyysiseen ja operatiiviseen sietokykyyn keskittyvä CER-direktiivi (engl. Critical Entities Resilience). Direktiivin avulla halutaan varmistaa kriittisten toimijoiden ja infrastruktuurien kyky selviytyä häiriöistä ja kriiseistä. CER-direktiivissä kriittisiä toimijoita ovat: energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveysala, juoma- ja jätevesi, digitaalinen infrastruktuuri, julkishallinto ja avaruus. Direktiivi asettaa vaatimuksena soveltamisalaansa kuuluville toimijoille riskien ja uhkien arvioimisen, toimijoiden keskinäisten riippuvuuksien tunnistamisen sekä varautumis- ja suojelutoimenpiteiden käyttöönoton. Näiden rinnalla NIS2-direktiivin tavoin CER-direktiivissä vaaditaan mahdollisimman aikaista ilmoitusta häiriöistä ja kybersolidaarisuussäädöksen kaltaisesti jäsenvaltioiden välistä yhteistyötä. (Direktiivi (EU) 2022/2557, 2022)

5 Teoreettinen viitekehys

Tässä luvussa esitellään tutkielman teoreettinen viitekehys ja määritellään teoreettinen pohja tutkimukselle. Nämä konseptit käydään läpi häiriöiden hallinnan näkökulmasta. Tämä luku yhdistää kirjallisuuskatsauksessa esitetyt teoriat EU:n NIS2-direktiivistä sekä kokonaisarkkitehtuurista osana häiriöiden hallintaa. Tavoitteena on hahmottaa kirjallisuuskatsauksessa tarkastelluista teemoista johdettu häiriöiden hallintaan keskittyvä kokonaisarkkitehtuuriviitekehys, jonka taustalla vaikuttaa NIS2-direktiivin kyberturvallisuusvaatimukset.

Kirjallisuuskatsauksen perusteella voidaan todeta, että EU:n NIS2-direktiivi sekä digitalisaation myötä yleistyneet häiriöt asettavat yrityksille merkittäviä vaatimuksia ja tarpeita häiriöiden hallinnan osalta. Vaatimuksiin vastaaminen vaatii yrityksiltä kokonaisvaltaista lähestymistapaa kyberturvallisuuden hallintaan. Kokonaisarkkitehtuurin avulla voidaan muodostaa yhtenäinen rakenne organisaatiosta, sen IT-infrastruktuurista ja näiden keskinäisistä riippuvuuksista, mikä helpottaa muutosvaikutusten arviointia.

Aluksi tarkastellaan viitekehykseen liittyviä taustatietoja. Tämän jälkeen esitellään viitekehyksen kaksi pääelementtiä eli Kotusevin (2017) kahdeksan kokonaisarkkitehtuurin artefaktia ja NIST kyberturvallisuusviitekehys 2.0 (2024). Näistä muodostuva tutkielman viitekehys käydään tämän jälkeen tarkemmin läpi ja keskitytään siihen, miten luotu viitekehys soveltuu vastaamaan tutkimuskysymyksiin.

5.1 Taustaa

Tämän tutkimuksen tavoitteena on mallintaa viitekehys, jolla voidaan arvioida kokonaisarkkitehtuurin osuutta häiriöiden hallinnassa. Häiriöitä tutkitaan normaalioloissa eli tutkimuksessa ei tulla huomioimaan poikkeusoloissa syntyviä häiriöitä. Tutkielman ja sen viitekehyksen taustalla vaikuttaa EU:n NIS2-direktiiviin asettamat vaatimukset kriittisten sektorien toimijoille. Viitekehys muodostaa pohjan tutkimuskysymyksiin vastaamiselle yhdistämällä kokonaisarkkitehtuurin, häiriöiden hallinnan ja kyberturvallisuusnäkökulman. Empiirinen data tullaan keräämään toimeksiantajaorganisaation kokonaisarkkitehtuurin mallintamiseen tarkoitetusta ohjelmasta ja häiriöiden raportointijärjestelmästä. Tutkielman viitekehystä käytetään toimeksiantajaorganisaatiolta saadun datan analysointiin ja tämän prosessin myötä saaduilla tuloksilla vastataan tutkielman tutkimuskysymyksiin.

Al-Turkistani ym. (2021) tutkimus osoittaa, ettei tällä hetkellä ole olemassa kokonaisarkkitehtuuriviitekehystä, joka kattavasti täyttäisi kaikkien sidosryhmien liiketoiminta- ja turvallisuusvaatimukset. Nykyiset viitekehykset ovat puutteellisia erityisesti turvallisuuden näkökulmasta, mikä voi heikentää niitä hyödyntävien organisaatioiden toimintaedellytyksiä. Organisaatioiden tulisikin kehittää viitekehyksiään siten, että kaikki turvallisuuden osa-alueet otetaan huomioon liiketoiminnan suojaamiseksi. Tehokkaassa viitekehyksessä turvallisuusvaatimukset huomioidaan järjestelmällisesti koko kehitysprosessin ajan. Lisäksi viitekehyksen turvallisuusominaisuuksien tulee olla mitattavissa, jotta liiketoiminnan edustajat voivat arvioida vaatimusten toteutumista määrällisesti. Kyseisessä tutkimuksessa ehdotetaan, että tarpeeksi kattava viitekehys voitaisiin muodostaa yhdistämällä useamman eri viitekehyksen vahvuudet yhtenäiseksi kokonaisuudeksi. Organisaatioiden tulisi käyttää sellaisia kokonaisarkkitehtuuriviitekehyksiä, joita pystytään tarpeen vaatiessa muuttamaan liiketoiminnan, turvallisuuden ja kybersietokyvyn tulevaisuuden tarpeiden mukaan. Näiden rinnalla viitekehyksen tulisi mahdollistaa sijoitetun pääoman tuoton maksimointi sekä riskien ja resurssien käytön optimointi.

Tämän takia tutkielman viitekehyksessä on haluttu yhdistää kaksi eri viitekehystä, jotta voitaisiin saada kokonaisuus, joka huomioisi sekä kokonaisarkkitehtuurin että kyberturvallisuuden ja häiriöiden hallinnan pääelementit. Tutkielman viitekehykseen on otettu vaikutteita Kotusevin kahdeksan artefaktin listauksesta sekä NIST kyberturvallisuusviitekehyksestä 2.0.

5.2 Kotusevin kahdeksan artefaktia

Kotusev (2017) on määritellyt kahdeksan keskeistä kokonaisarkkitehtuuri artefaktia, jotka ovat keskeisimpiä toimivan ja menestyksekkään kokonaisarkkitehtuurikäytäntöjen tukemisessa organisaatiossa. Kotusev on halunnut muodostaa tiiviimmän listauksen artefakteista vastapainona monille tunnetuille kokonaisarkkitehtuuriviitekehyksille, joiden artefaktiluettelot ovat käytännöntarkoituksissa liian pitkiä toteutettavaksi. Nämä kahdeksan Kotusevin tutkimaa artefaktia ovat käytössä kaikista menestyneimmissä kokonaisarkkitehtuureissa: periaatteet, liiketoimintakyvykkyysmallit, tiekartat, ratkaisukuvaukset, teknologian viitemallit, ohjeistukset, arkkitehtuurin maisemakaaviot ja ratkaisusuunnitelmat.

Perinteisten kokonaisarkkitehtuuriviitekehysten suosittelemat artefaktit ovat usein teoreettisia, liian laajoja tai käytännössä toteuttamiskelvottomia. Kotusev haluaa korostaa empiiristä ja käytäntöön perustuvaa näkökulmaa, jossa luodaan ratkaisuja organisaatioiden oikeaan käyttöön. Kotusev perustaakin mallinsa tutkimukseen ja havaintoihin oikeista ja toimivista organisaatioista.

Näiden kahdeksan konkreettisen ja käytännössä hyödyllisen artefaktin tarkoituksena on aidosti tukea IT:n ja liiketoiminnan yhteensovittamista. Kotusev painottaa, että kokonaisarkkitehtuurin käytäntöjen tulisi perustua käytännössä hyödyllisiin ja toimiviksi todettuihin artefakteihin, ei viitekehysten teoreettisiin ja usein epärealistisiin ohjeisiin. Valittujen kahdeksan artefaktin ymmärtämisen ja käyttämisen avulla organisaatioiden pitäisi pystyä muodostamaan kokonaisarkkitehtuuristaan todellista arvoa tuottavan työkalun.

Kotusev sijoittaa esittelemänsä artefaktit CSVLOD-taksonomiaan (engl. Considerations, Standards, Visions, Landscapes, Outlines ja Designs), joka määrittelee kuusi yleistä kokonaisarkkitehtuurin artefaktityyppiä, joita esiintyy käytännön toiminnassa. Nämä kuusi artefaktityyppiä ovat harkinnat, standardit, visiot, kokonaiskuvat, hahmotelmat ja suunnitelmat. Taksonomiaan sisältyvät kahdeksan valittua artefaktia edustavat johdonmukaisia kokonaisarkkitehtuurin artefaktiryhmiä, joilla on hyvin samankaltainen merkitys eri organisaatioissa riippumatta niiden organisaatiokohtaisista nimityksistä. Kotusevin nimitykset ovat artefaktien yleisimpiä nimiä, mutta samoja artefakteja voidaan käyttää eri nimillä eri organisaatioissa.

Periaatteet (engl. Principles) määrittävät korkeantason linjauksia organisaatiossa. Nämä vaikuttavat organisaation liiketoimintaan ja IT-toimintoihin. Periaatteet laaditaan yleensä arkkitehtien ja liiketoimintajohdon toimesta, ja niitä syntyy tyypillisesti noin 10–20. Tavoitteena on luoda yhteinen ymmärrys keskeisistä perussäännöistä, arvoista, suuntaviivoista ja tavoitteista organisaatiossa. Periaatteita voidaan hyödyntää monissa organisaation toimissa, sillä ne tarjoavat kokonaisvaltaisen kuvan organisaation suuntaviivoista ja tavasta toimia. Periaatteita voidaan hyödyntää osana päätöksentekoa sekä tukemassa IT-projektien arkkitehtuurien suunnittelua. Kotusevin CSVLOD-taksonomiassa periaatteet-artefakti sijoittuu harkinnat-luokkaan (engl. Considerations). Harkintoja hyödynnetään ylätason näkökulmina tietojärjestelmien suunnittelussa ja kehittämisessä.

Teknologian viitemallit (engl. Technology Reference Models) ovat vakiomuotoisia teknologialuetteloita, joita kaikkien IT-projektien tulee noudattaa. Teknologiat on jäsennelty aihealueittain, ja niihin on merkitty kunkin teknologian elinkaarivaihe. Viitemallit laaditaan arkkitehtien ja eri teknologia-alueiden asiantuntijoiden yhteistyönä, ja niitä päivitetään säännöllisesti. IT-projektien arkkitehtuurit tarkistetaan järjestelmällisesti, jotta varmistetaan viitemallin mukaisuus. Tavoitteena on teknologioiden yhdenmukaistaminen ja IT-ympäristön johdonmukaisuus koko organisaatiossa. CSVLOD-taksonomiassa teknologian viitemallit on luokiteltu standardeihin. Standardit ovat IT-keskeisiä sääntöjä, jotka edustavat hyväksi havaittuja ja uudelleen käytettäviä keinoja IT-projektien toteuttamisessa.

Standardeihin on myös Kotusevin taksonomiassa luokiteltu ohjeistukset-artefakti (engl. Guidelines). Ohjeistukset ovat IT-keskeisiä, teknologialuokittain jäsenneltyjä ja yksityiskohtaisia suosituksia ja määräyksiä. Ne on luotu arkkitehtien ja kyseisten teknologia-alueiden asiantuntijoiden yhteistyön tuloksena ja niitä tulee noudattaa organisaation IT-projekteissa. Ohjeistuksia päivitetään säännöllisesti, jotta ne ovat mahdollisimman yhteensopivia organisaation sen hetkiseen tilanteeseen. Ohjeistuksilla pyritään varmistamaan IT-ratkaisujen yhdenmukaisuus, sääntelyvaatimusten noudattaminen ja edistetään teknistä yhteen toimivuutta. Ohjeistukset ja teknologian viitemallit liittyvät vahvasti toisiinsa, mutta erona niissä on käyttötarkoitus ja niiden tyyppi. Teknologian viitemalleista löytyy tieto siitä, mitä teknologioita organisaatiossa käytetään ja ohjeistukset määrittävät, miten kyseisiä teknologioita tulisi käyttää.

Liiketoimintakyvykkyysmalleiksi (engl. Business Capability Models) kutsutaan jäsenneltyjä esityksiä, joissa esitetään organisaation kaikki liiketoimintakyvykkyydet tiiviisti yhdellä sivulla. Malleja voidaan käyttää myös keskeisten investointikohteiden tunnistamiseen, IT-investointien priorisointiin ja sen varmistamiseen, että IT-investoinnit ovat linjassa liiketoimintatavoitteiden kanssa. Esimerkiksi sisällyttämällä tietoja liiketoimintastrategiasta, tavoitteista, kumppaneista ja keskeisistä asiakasryhmistä. Liiketoimintakyvykkyysmallit laaditaan tyypillisesti arkkitehtien ja liiketoimintajohdon yhteistyönä ja näitä pidetään usein liiketoimintajohdon ensisijaisena väylänä tai lähtökohtana IT-toimintojen tarkasteluun.

Tiekartat-artefakti (engl. Roadmaps) sisältää tietoa organisaation tulevaisuuden IT-investoinneista ja kehityshankkeista. Ne sisältävät alustavat aikataulut ja kohdistuvat tiettyihin liiketoimintakyvykkyyksiin tai liiketoiminta-alueisiin. Tiekarttoihin sisältyy usein myös korkean tason kuvaukset tavoitetiloista useamman vuoden aikajänteellä. Tyypillisesti tiekartat kuvaavat, miten ja milloin lämpökartoituksessa tunnistetut keskeiset kyvykkyydet on tarkoitus kehittää seuraavalle tasolle. Tiekarttojen laadinta kuuluu tyypillisesti arkkitehtien ja ylimmän liiketoimintajohdon vastuulle ja niitä hyödynnetään IT:n hankkeiden ja investointien suunnittelussa ja priorisoinnissa. Sekä tiekartat että liiketoimintakyvykkyysmallit ovat artefakteja, jotka tarjoavat tietoa organisaation tulevaisuudesta liiketoiminnan näkökulmasta. Molemmat artefaktit tarjoavat erilaisen näkökulman täydentäen toisiaan. Liiketoimintakyvykkyysmallien avulla tarkastellaan, mihin investointeja tulisi tehdä ja tiekarttojen avulla suunnitellaan investointien aikatauluja. Liiketoimintakyvykkyysmallit ja tiekartat ovat keskeisiä kokonaisarkkitehtuurin artefakteja, ja ne luokitellaan CSVLOD-taksonomiassa visioihin, eli liiketoimintalähtöisiin rakenteisiin. Ne ilmentävät organisaation pitkän aikavälin tavoitteita, jotka on yhteisesti sovittu liiketoiminnan ja IT:n välillä.

Arkkitehtuurin maisemakaaviot (engl. Landscape Diagrams) esittävät korkeantason yhteyksiä eri sovellusten, tietokantojen, alustojen, järjestelmien ja lisäksi liiketoimintaprosessien välillä. Maisemakaavion tarjoamien yhteyksien avulla saadaan ajankohtainen kokonaiskuva organisaation IT-ympäristöstä. Arkkitehtuurin maisemakaavioita päivittävät arkkitehdit, jotka huolehtivat maisemakaavioihin vaikuttavien muutosten mallintamisesta. Tämä on tärkeää, jotta arkkitehtuurin maisemakaavioiden tiedot pysyvät ajankohtaisina, jotta niitä voidaan hyödyntää osana teknistä suunnittelua. Kotusevin taksonomiassa arkkitehtuurin maisemakaaviot-artefakti kuuluu osaksi kokonaiskuvat-luokkaa (engl. Landscapes), jotka ovat pääasiassa tietojärjestelmien kuvauksia ja rakenteita.

Ratkaisukuvaukset-artefakti (engl. Solution Overviews) sisältää ylätason arkkitehtuurikuvauksen, odotetut hyödyt liiketoiminnalle, kustannusarvion, merkittävimmät riskit ja alustavan aikataulun, joiden avulla muodostetaan selvitys uusia IT-hankkeita varten. Arkkitehdit yhdessä liiketoiminnan asiantuntijoiden kanssa luovat ratkaisukuvaukset ennen hankkeiden suunnittelua, jotta niiden sisältämää tietoa voidaan hyödyntää. Ratkaisukuvaukset tukevat ylimmän johdon päätöksentekoa hankkeen osalta tarjoamalla tietoa vaikutuksista ja odotetusta arvontuotannosta. Kotusevin taksonomiassa ratkaisukuvaukset-artefakti on osana hahmotelmat-luokkaa, jossa käyttötarkoitus liittyy suunnittelua edeltävään IT-hankkeiden hyötyjen, aikataulujen ja kustannusten selvittämiseen.

Ratkaisusuunnitelmat (engl. Solution Designs) ovat teknisesti yksityiskohtaisia kuvauksia yksittäisistä IT-hankkeista, ja ne sisältävät kaikki olennaiset tiedot hankkeiden toteuttamisen tueksi. Suunnitelmat laaditaan kaikille hyväksytyille IT-hankkeille arkkitehtien, projektitiimien ja liiketoiminnan edustajien yhteistyönä, jotta ne huomioivat sekä liiketoiminnalliset että arkkitehtoniset vaatimukset. Ratkaisusuunnitelmiin voidaan tukeutua hankkeen aikana, jotta saadaan tarvittavaa tietoa hankkeen tavoitteista ja vaatimuksista. Kotusevin taksonomiassa ratkaisusuunnitelmat-artefakti on osa suunnitelmat-luokkaa, jossa artefaktit sisältävät tietoa IT:hen liittyvistä muutoksista ja jakavat oleellista tietoa arkkitehtuurin ja projektin välillä.

Taulukko 1 Kotusevin kahdeksan artefaktia tiivistetysti

Artefakti	**Taksonomia**	**Kuvaus**
Periaatteet	Harkinnat	Korkeantason linjaukset liiketoiminnalle ja IT-toimintoihin

Teknologian viitemallit	Standardit	Teknologialuettelo: teknologiat aihealueittain ja elinkaaren vaiheet
Ohjeistukset	Standardit	Yksityiskohtaisia ja IT-keskeisiä suosituksia tai määräyksiä
Liiketoimintakyvykkyysmallit	Visiot	Jäsenneltyjä esityksiä organisaation kaikista liiketoimintakyvykkyyksistä
Tiekartat	Visiot	Jäsenneltyjä esityksiä organisaation tulevista IT-investoinneista ja kehityshankkeista (sis. alustavat aikataulut)
Arkkitehtuurin maisemakaaviot	Kokonaiskuvat	Kokonaiskuva organisaation IT-ympäristöstä: korkeantason yhteyksiä eri sovellusten, tietokantojen, alustojen, järjestelmien ja liiketoimintaprosessien välillä
Ratkaisukuvaukset	Hahmotelmat	Tiiviitä ja liiketoimintalähtöisiä esityksiä yksittäisistä IT-hankkeista: arkkitehtuurikuvaus, arvio odotetuista liiketoimintahyödyistä, alustava kustannusarvio, keskeiset riskit ja suunniteltu aikataulu
Ratkaisusuunnitelmat	Suunnitelmat	Teknisesti yksityiskohtaisia kuvauksia yksittäisistä IT-hankkeista, joissa kaikki olennaiset tiedot hankkeiden

		toteuttamisen tueksi (Hyväksytyille IT-hankkeille)

(Kotusev, 2017)

5.3 The NIST Cybersecurity Framework (CFS) 2.0

National Institute of Standards and Technology:n (2024) NIST kyberturvallisuusviitekehys (Cybersecurity Framework, CFS) 2.0 tarjoaa systemaattisen viitekehyksen, jonka tarkoituksena on tukea teollisuuden, julkishallinnon ja muiden organisaatioiden kyberturvallisuusriskien hallintaa. Kehys esittää korkean tason kyberturvallisuustavoitteiden jäsennyksen, jota voidaan soveltaa organisaatiotyypistä, koosta, toimialasta tai kypsyystasosta riippumatta. Viitekehyksen tarkoituksena on auttaa organisaatioita systemaattisesti ymmärtämään, arvioimaan, priorisoimaan ja viestimään omista kyberturvallisuustoimista. NIST kyberturvallisuusviitekehys ei tarjoa yksiselitteistä ohjeistusta tavoiteasetelman operatiiviseksi toimeenpanoksi, vaan ohjaa käyttäjän hyödyntämään ulkoisia lähteitä, joissa käsitellään vaihtoehtoisia menetelmiä ja hallintakäytäntöjä tavoitteiden toteuttamiseksi.

Viitekehys on suunniteltu niin, että sitä voidaan hyödyntää riippumatta siitä, kuinka kehittyneellä tasolla organisaation kyberturvallisuusohjelmat ovat teknisesti tai organisatorisesti. Viitekehyksessä tunnistetaan se, ettei ole yhtä tiettyä lähestymistapaa, jonka tulisi sopia kaikille, joten viitekehyksen soveltaminen organisaatiossa sopivalla tavalla nähdään väistämättömänä osana prosessia. Kyberturvallisuuskehyksen integrointi organisaation riskienhallintaprosessiin on tehokkain tapa hyödyntää sitä. Tämä tunnistaa ja priorisoi kyberturvallisuusriskit suhteessa organisaation muihin riskeihin, kuten taloudellisiin, tietosuojaan ja yksityisyyteen liittyviin, toimitusketjuun liittyviin, maineeseen liittyviin, teknologisiin ja fyysisiin turvallisuusriskeihin.

Kyberturvallisuusviitekehystä ei ole tarkoitus käyttää täysin erillään muista organisaation viitekehyksistä, standardeista tai käytännöistä. Eri resursseista saatu hyödyllinen tieto voidaan yhdistää niin, että kyberturvallisuuteen sekä tieto- ja viestintäteknologiaan liittyvien riskien hallintaa voidaan entisestään tukea ja tehostaa. On huomioitava, että organisaatioiden riskienhallintaan vaikuttavat yksilölliset tekijät, kuten erilaiset uhkat, haavoittuvuudet, riskinsietokyvyt sekä toiminnalliset tavoitteet ja vaatimukset. Näin ollen kyberturvallisuusviitekehyksen käyttöönotto ja soveltaminen muotoutuvat kunkin organisaation erityispiirteiden mukaisesti.

Kyberturvallisuusviitekehyksen tavoitteena on tarjota selkeä kuva kyberturvallisuuden hallinnasta erityisesti niille organisaation toimijoille, jotka eivät pääasiallisesti keskity kyberturvallisuuteen organisaatiossa, kuten ylin johto, esihenkilöt ja muiden liiketoiminnan osa-alueiden asiantuntijat. Koska lopputulokset ovat neutraaleja toimialan, kansallisen kontekstin ja teknologian suhteen, ne tarjoavat organisaatioille tarvittavaa joustavuutta omien riskien, teknologisten ratkaisujen ja strategisten tavoitteiden huomioon ottamiseen. Nämä lopputulokset on yhdistetty suoraan mahdollisiin suojaustoimenpiteisiin, joita voidaan hyödyntää kyberturvallisuusuhkien hallitsemiseksi.

5.3.1 Osa-alueet

Kyberturvallisuusviitekehys koostuu kolmesta pääelementistä: ydin, organisaatioprofiilit ja tasot. Tässä tutkielmassa keskitymme ytimen muodostamaan NIST kyberturvallisuusviitekehykseen. Ydin muodostaa kyberturvallisuuskehyksen keskeisimmän osan. Se sisältää korkean tason kyberturvallisuustavoitteiden jäsennyksen, joka tukee organisaatioita kyberturvallisuusriskien hallinnassa riippumatta organisaation koosta, toimialasta tai kypsyystasosta. Ydin muodostuu kolmesta tasosta, jotka ovat toiminnot, luokat ja alaluokat. Tasot on tarkoitettu kyberturvallisuuden hallinnan tavoitteiden määrittelyyn. Määritelmät pyritään muotoilemaan mahdollisimman ymmärrettäviksi, jotta niitä pystyvät tulkitsemaan useat eri toimijat riippumatta heidän kyberturvallisuustietämyksestään.

Organisaatioprofiilit toimivat välineenä, jonka avulla voidaan kuvata organisaation tämänhetkinen ja tavoiteltu kyberturvallisuuden tila suhteessa kyberturvallisuusviitekehyksen ytimen tuottamiin tuloksiin. Viitekehyksen tasot voidaan puolestaan liittää organisaatioprofiileihin organisaation kyberturvallisuusriskien hallinnan ja ohjauksen järjestelmällisyyden kuvaamiseksi. Tästä muodostetaan organisaation kyberturvallisuutta uhkaavat riskit ja mietitään toimenpiteet riskien hallitsemiseksi.

5.3.2 Kyberturvallisuusviitekehyksen toiminnot

Kyberturvallisuusviitekehyksen ytimen toiminnot on jaettu kuuteen eri vaiheeseen: ohjaa, tunnista, suojaa, havaitse, reagoi ja palauta. Jokainen toiminto jakautuu kategorioihin, jotka sisältävät kyberturvallisuustuloksia. Nämä kategoriat jatkuvat alakategorioihin, joissa kuvataan tarkemmin teknisiä ja hallinnollisia toimenpiteitä sekä niiden tavoitteita. Tässä tutkielmassa ei syvennytä toiminnoissa kategoriatasolle vaan keskitytään yhdistämään kokonaisarkkitehtuuriin ja häiriöiden hallinnan elementit kyberturvallisuuden näkökulma huomioiden.

Ohjaa-toiminto keskittyy kyberturvallisuuden hallintaan ja ohjaukseen. Se sisältää organisaation kyberturvallisuuden riskienhallintastrategian, odotukset ja käytännöt. Ohjaa-toiminto auttaa organisaatiota kohdentamaan ja asettamaan etusijalle muiden viiden toiminnon tavoitteet omien strategisten päämääriensä ja sidosryhmien odotusten mukaisesti. Tavoitteena on yhdistää kyberturvallisuus osaksi organisaation muita riskienhallintatoimia, jotta ei muodostu toisistaan irrallisia menetelmiä. Ohjaa-toimintoon liittyvät esimerkiksi kyberturvallisuusstrategian muodostaminen, toimitusketjuihin liittyvien riskien hallinta, vastuualueiden jakaminen ja käytäntöjen määrittely.

Tunnista-toiminnossa pyritään siihen, että aikaisessa vaiheessa saadaan selville organisaation toimintaan kohdistuvat riskit ja pystytään arvioimaan olemassa olevat resurssit. Riskit voivat kohdistua laajasti eri osa-alueisiin organisaation sisällä tai sen ulkopuolella. Tyypillisiä sisäisiä riskialttiita osa-alueita ovat laitteisto, ohjelmistot, järjestelmät ja tieto, kun taas ulkoisesti riskit liittyvät usein toimittajiin. Näiden osa-alueiden tuntemuksella organisaatio pystyy priorisoimaan toimintaansa riskienhallintastrategiansa ja Ohjaa-toiminnossa määriteltyjen toimintojen perusteella. Tunnista-toimintoon sisältyy lisäksi organisaation kyberturvallisuusriskien hallintaa tukevien käytäntöjen, suunnitelmien, prosessien ja menettelyjen kehitystarpeiden tunnistaminen. Tämä tukee toimia kaikissa kuudessa toiminnossa.

Suojaa-toiminto tarkoittaa organisaation kyberturvallisuusriskien hallintaa tarkoituksenmukaisilla suojatoimenpiteillä. Kriittisten omaisuuserien ja niihin liittyvien riskien tunnistamisen ja priorisoinnin jälkeen vahvistetaan organisaation kykyä suojata nämä resurssit. Tavoitteena on ehkäistä kyberuhkien toteutuminen, vähentää niiden vaikutuksia sekä samalla kasvattaa kykyä ottaa hyöty tarjoutuvista mahdollisuuksista. Suojaavia toimenpiteitä ovat esimerkiksi identiteetin hallinta, käyttöoikeuksien valvonta, koulutukset, todennusmenetelmät ja digitaalisten infrastruktuurien palautumiskyvyn ja sietokyvyn vahvistaminen.

Havaitse-toiminnossa tunnistetut kyberturvallisuuden ja tietoturvan uhat sekä häiriöt käsitellään tarkemmin ja analysoidaan. Tämän toiminnon avulla pyritään häiriöiden ja muiden mahdollisesti haitallisten tapahtumien oikea-aikaiseen havaitsemiseen ja analysointiin, mikä tukee tehokasta häiriöiden hallintaa ja palautumista. Havaitse-toiminnossa pyritään keräämään muiden toimintojen kannalta oleellista tietoa.

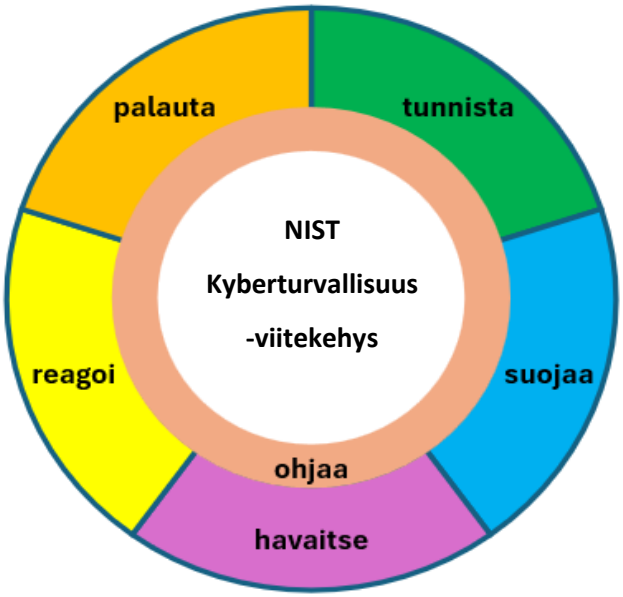
Reagoi-toiminnon tarkoituksena on vastata havaittuihin poikkeamiin tehokkaasti ja hallitusti. Tämän avulla organisaatio pystyy paremmin rajoittamaan kyberpoikkeamien vaikutuksia.

Toiminnossa oleellisena osana on poikkeamien hallinta, analysointi, lieventäminen, raportointi ja viestintä.

Palauta-toiminnossa keskitytään toiminnan palauttamiseen häiriötilanteiden jälkeen. Tässä tärkeitä osa-aleuita ovat kärsineet omaisuuserät sekä toiminnot, joiden palauttaminen normaaliin toimintaan on erityisen tärkeää. Toiminnon keskiössä on tukea normaalin toiminnan oikea-aikaista palautumista, vähentää poikkeaman haittavaikutuksia ja mahdollistaa asianmukainen viestintä palautumisprosessin aikana.

5.3.3 Kyberturvallisuusviitekehyksen toimintojen mallinnus

Kyberturvallisuusviitekehyksen toiminnot esitetään pyörämallina, koska ne ovat toisiinsa kytkeytyviä ja muodostavat eheän, toisiaan täydentävän ja toistettavan kokonaisuuden. Tämä malli toimii tämän tutkielman viitekehyksen perustana. Toimintojen yhteinen tarkastelu ja niiden integroitu hyödyntäminen mahdollistavat suunnitelmallisemman kyberturvallisuuden hallinnan, tehokkaamman reagoinnin sekä poikkeamien oikea-aikaisen havaitsemisen. Kyberturvallisuusviitekehys pystyy myös mukautumaan vaadittaessa muuttuvien teknologioiden ja toimintaympäristöjen tarpeisiin. Tämä on oleellista siinä, että viitekehys on hyödynnettävissä myös tulevaisuudessa.



Kuvio 1 NIST Kyberturvallisuusviitekehys

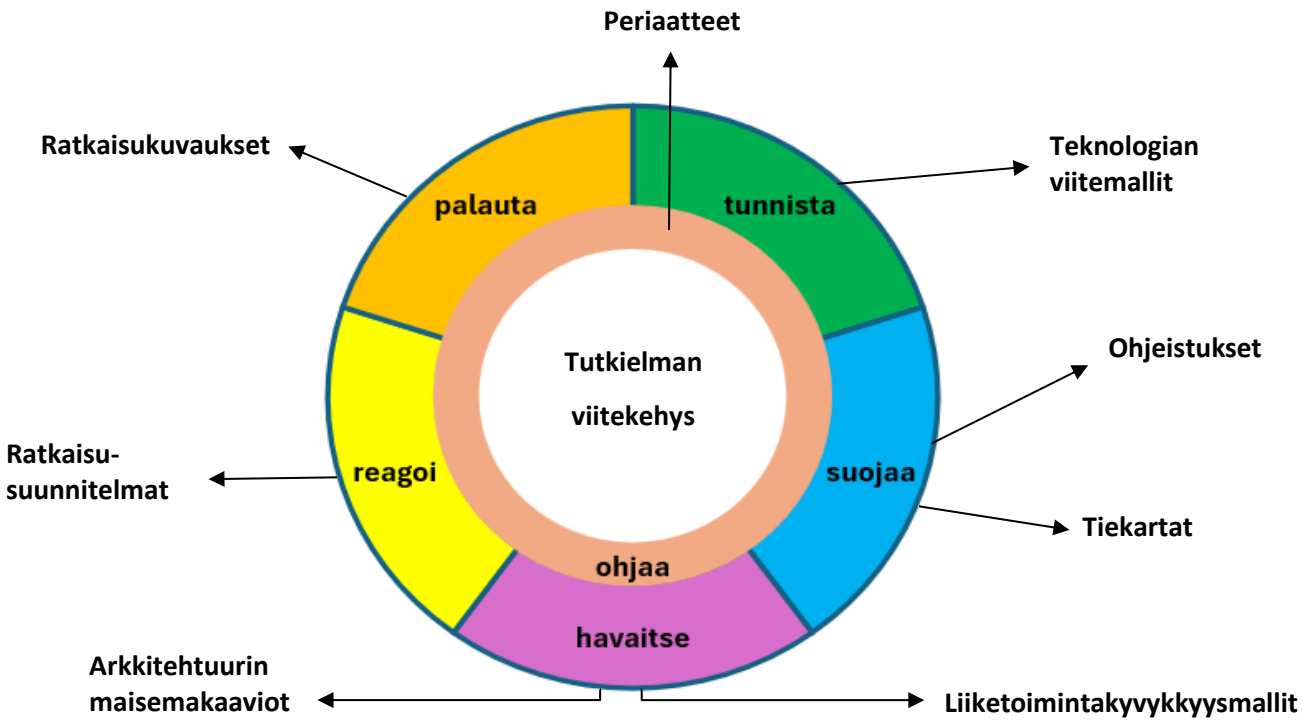
Kaikilla viitekehyksen toiminnoilla on keskeinen rooli kyberturvallisuuden häiriöiden hallinnassa. Pyörän keskiössä sijaitseva ohjaa-toiminto suuntaa ja jäsentää organisaation tapaa toteuttaa muita

viittä toimintoa. Ohjaa-toiminto sekä tunnista- ja suojaa-toiminnot tukevat häiriöiden ehkäisyä ja ennakointia. Havaitse-, reagoi- ja palauta-toiminnot yhdessä ohjaa-toiminnon kanssa tukevat häiriöiden tunnistamista ja hallintaa.

(National Institute of Standards and Technology, 2024)

5.4 Tutkielman viitekehys

Kotusevin kahdeksan artefaktin ja NIST Kyberturvallisuusviitekehyksen pohjalta on tässä tutkielmassa mallinnettu viitekehys, jossa yhdistyy kirjallisuuskatsauksessa läpikäydyt pääteemat: kokonaisarkkitehtuuri, häiriöiden hallinta ja NIS2-direktiivin asettamat vaatimukset. Tutkielman viitekehyksen tavoitteena on auttaa hahmottamaan kokonaisarkkitehtuurin ja häiriöiden hallinnan yhteyttä kyberturvallisuuteen sekä tutkimaan, miten tämä olisi toteutettavissa organisaatioissa.



Kuvio 2 Tutkielman viitekehys

5.4.1 Kotusev artefaktit yhdistettynä NIST Kyberturvallisuusviitekehykseen

NIST Kyberturvallisuusviitekehyksen ohjaa-toiminto muodostaa perustan muille toiminnoille ja määrittää, miten niitä tulisi toteuttaa. Ohjaa-toimintoon kuuluu oleellisena osana strategisten lähtökohtien suunnittelu ja päättäminen, minkä avulla muiden toimintojen suunta määräytyy. Kotusevin nimeämistä kahdeksasta kokonaisarkkitehtuurin artefaktista tähän toimintoon

kytkeytyvät periaatteet. Sekä ohjaa-toiminnon että periaatteiden tarkoituksena on luoda yhteisymmärrys organisaation toiminnasta ja tavoitteista, joiden pohjalta muut viitekehyksen toiminnot toteutetaan.

Teknologian viitemallit on liitetty tutkielman viitekehyksessä tunnista-toimintoon, sillä niissä olevalla tiedolla voidaan analysoida ja ennakoida riskejä systemaattisesti. Viitemallien data sisältää muun muassa organisaation käytössä olevat teknologiat, niiden elinkaarivaiheet ja mahdolliset haavoittuvuudet sekä toimittajista. Tunnista-toiminnossa on oleellista selvittää, mihin osa-alueeseen organisaatiossa ja/tai sen ulkopuolella häiriö liittyy. Tähän saadaan apua teknologian viitemalleista.

Suojaa-toimintoon on tutkielman viitekehyksessä liitetty kaksi kokonaisarkkitehtuurin artefaktia: ohjeistukset ja tiekartat. Ohjeistuksissa käydään läpi organisaation teknologioiden turvallinen käyttö ja annetaan suosituksia sopivista toimista. Tätä voidaan hyödyntää suojaa-toiminnossa, jotta tunnistettuja riskejä pystytään hallitsemaan paremmin ja selkein suojatoimin. Tunnista- ja suojaa-toiminnot liittyvät vahvasti toisiinsa, minkä myötä myös teknologian viitemallien ja ohjeistusten välinen yhteys vahvistaa artefaktien hyötyä osana kyseisiä toimintoja. Tunnista-toiminnossa riskien tunnistaminen on oleellista myöhemmin toteutettaville suojatoimille. Teknologian viitemallit puolestaan määrittelevät organisaatiossa olevat teknologiat ja ohjeistukset sääntelevät, miten niitä tulisi hyödyntää.

Tiekartat-artefakti on toinen kokonaisarkkitehtuurin artefakteista, joka on liitetty tutkielman viitekehyksessä suojaa-toimintoon. Tiekartat sisältävät tietoa tulevista IT-investoinneista ja -projekteista sekä niiden aikatauluista. Näiden tietojen avulla suojaa-toiminnossa voidaan ennakoivasti tehdä ratkaisuja, joiden avulla kehitetään kyberturvallisuutta ja poistetaan mahdollisia riskitekijöitä. Tiekarttojen avulla saadaan tarvittavat kokonaiskuva, jota hyödyntämällä suojaa-toiminnossa pystytään suunnittelemaan, aikatauluttamaan ja sovittamaan toimenpiteet organisaatiossa riskien varalta. Tällaisia toimenpiteitä ovat esimerkiksi ohjelmistojen päivitykset, pian vanhentuvien järjestelmien korvaaminen tai henkilöstön asianmukainen kouluttaminen. Suojaa-toiminnossa oleellista on kehittää organisaation sietokykyä ja häiriöiden ennakointia, missä tiekartat auttavat tarjoamalla tärkeää tietoa aikatauluista ja kyvykkyyksistä sekä yhdistämällä suojatoimet osaksi muita kehityshankkeita.

Havaitse-toimintoon on liitetty tutkielman viitekehyksessä myös kaksi eri kokonaisarkkitehtuurin artefaktia: liiketoimintakyvykkyysmallit ja arkkitehtuurin maisemakaaviot. Näiden artefaktien tarkoituksena on tuoda esille organisaation toiminnasta ja IT-ympäristöstä strategiset ja rakenteelliset osa-alueet, joita voidaan hyödyntää häiriöiden havaitsemiseen ja niiden vaikutusten

arviointiin. Liiketoimintakyvykkyysmallien avulla pystytään havaitsemaan, mitkä organisaation tärkeimmistä kyvykkyyksistä voivat altistua häiriölle ja siten aiheuttaa merkittävintä haittaa organisaation toiminnalle, tavoitteille ja liiketoiminnalle. Tämän tiedon avulla voidaan määrittää, mitä osa-alueita tulisi seurata erityisen tarkasti häiriöiden varalta tai mitkä osa-alueet vaativat ylimääräisiä varotoimia ja resursseja. Liiketoimintamallit tarjoavat lisäksi tärkeää tietoa keskeisistä henkilöistä ja toimijoista, mitä voidaan havaitse-toiminnossa hyödyntää häiriötilanteen sattuessa. Arkkitehtuurin maisemakaavioihin on mallinnettu ajankohtainen kokonaiskuva organisaation IT-ympäristöstä, johon kuuluvat muun muassa sovellukset, alustat ja näiden väliset yhteydet. Havaitse-toiminnossa arkkitehtuurin maisemakaaviota voidaan hyödyntää rakenneosien välisten suhteiden, riippuvuuksien ja vaikutusalueiden kartoittamiseen, jotta voidaan selvittää havaitun häiriön vaikutusalue.

Tutkielman viitekehyksessä reagoi-toimintoon on liitetty kokonaisarkkitehtuurin artefakteista ratkaisusuunnitelmat, jota voidaan häiriötilanteissa hyödyntää vaikutusten nopeaan ja järjestelmälliseen korjaamiseen. Valmiiden ratkaisusuunnitelmien avulla saadaan selkeitä suuntaviivoja ja toimenpiteitä, joita voidaan muokata sopivaksi sen hetkisen häiriön ratkaisemiseen. Korjaavien toimenpiteiden pitää hallita ja rajoittaa häiriön vaikutuksia organisaatiossa ja sen ulkopuolella mahdollisimman tehokkaasti, jolloin jo olemassa olevien ratkaisusuunnitelmien hyödyntäminen on merkittävää nopean, koordinoidun ja suunnitelmallisen toiminnan mahdollistamiseksi. Ratkaisusuunnitelmien tarkoituksena on vähentää improvisointia ja varmistaa, ettei jokaisen häiriön kohdalla mietitä uudelleen, miten tulisi toimia. Kun häiriön sattuessa on tarjolla selkeät ja aiemmin suunnitellut toimintaohjeet, voidaan reagointiaikaa nopeuttaa ja vähentää riskejä.

Palauta-toimintoon on tutkielman viitekehyksessä liitetty kokonaisarkkitehtuurin artefakteista ratkaisukuvaukset, jotka tarjoavat tärkeää tietoa palautumisen suunnittelussa. Ratkaisukuvauksien avulla voidaan häiriötilanteesta palautuessa määrittää aikataulu, arvioida riskejä ja keskeisiä riippuvuuksia ja selvittää oleelliset vaikutukset liiketoimintaan. Tämä auttaa siinä, että palauta-toiminto tapahtuu oikea-aikaisesti ja tärkeimpien toimintojen sekä järjestelmien palautumiseen keskitytään ensimmäisenä. Näin normaaliin toimintaan paluu tapahtuu mahdollisimman nopeasti, mutta myös varmistetaan, että häiriön vaikutukset eivät uusiudu. Palauta-toiminnossa on tärkeää huolehtia lisäksi viestinnästä, jotta tieto häiriöstä ja sen päättymisestä tavoittaa tarvittavat henkilöt. Ratkaisukuvauksien avulla saadaan hyödyllistä tietoa tehokkaasti, jotta häiriöstä ja sen päättymisestä voidaan viestiä organisaation sisällä.

Tutkielman viitekehys tarjoaa selkeän ja jäsennellyn kokonaisuuden NIST kyberturvallisuusviitekehyksestä yhdessä Kotusevin kahdeksan artefaktin kanssa. Jokaiseen kyberturvallisuusviitekehyksen toimintoon on kytketty artefakti, joiden tarkoituksena on tuottaa kriittistä tietoa häiriöiden hallinnan tueksi. Kyberturvallisuusviitekehyksen ja artefaktien yhdistämisen tavoitteena on osoittaa, miten arkkitehtuuriperusteinen lähestymistapa voi tukea sekä kyberturvallisuuden että häiriöiden hallinnan suunnittelua, toteutusta ja jatkuvuutta kokonaisvaltaisesti. Näin viitekehys toimii pohjana paitsi organisaatioiden käytännön kehittämistyössä, myös kokonaisarkkitehtuurin ja häiriöiden hallinnan tutkimuksessa.

6 Menetelmät ja tutkimusprosessi

Tässä tutkimuksessa pyritään tutkimaan kokonaisarkkitehtuurin vaikutuksia häiriöiden hallintaan ja selvittämään, miten kokonaisarkkitehtuuri voisi auttaa organisaatioita täyttämään NIS2-direktiivin vaatimukset. Seuraavaksi luvussa esitellään tutkimusprosessi sekä valitut tutkimus- ja analyysimenetelmät, ja perustellaan niiden valinta.

6.1 Tutkimusote ja -strategia

Tässä tutkielmassa hyödynnettiin kvalitatiivista eli laadullista suunnittelutieteellistä tutkimusotetta (engl. Design Science Research), joka keskittyy uuden ratkaisun eli artefaktin kehittämiseen ja arviointiin käytännön ongelmaan vastaten (Gregor, 2006). Suunnittelutieteellisiä menetelmiä on hyödynnetty laajasti tietojärjestelmätieteen tutkimuksissa (Gregor & Hevner, 2013; Peffers ym., 2007). Suunnittelutieteellinen tutkimusote soveltuu tutkimuksiin, jossa tavoitteena on yhdistää teoreettinen tieto ja käytännön sovellettavuus. Se mahdollistaa aktiivisen kehittämisen, kun keskitytään siihen, miten asioita voitaisiin parantaa eikä vain, miten ne ovat. Usein suunnittelutieteellisen tutkimusotteen tavoitteena on ratkaista vaikeasti hahmotettavia, monitulkintaisia organisaatioiden ongelmia, jotka edellyttävät innovatiivisia ja käytäntöön sovellettavia ratkaisumalleja. Suunnittelutieteellisen tutkimuksen tavoitteena on laajentaa olemassa olevaa tieteellistä tietopohjaa ja tuottaa samalla käytännön arvoa sekä tutkijayhteisölle että alan ammattilaisille. (Hevner & Chatterjee, 2010.) Laadullinen tutkimusote on tarkoituksenmukainen, kun tavoitteena on saavuttaa syvällinen ja kokonaisvaltainen ymmärrys tutkittavista ilmiöistä (Eriksson & Kovalainen, 2008).

Suunnittelutieteelliselle tutkimusotteelle on ominaista käytännön ratkaisun systemaattinen kehittäminen ja sen arviointi. Näiden lisäksi tutkimusprosessiin sisältyy useita muita vaiheita, jotka ohjaavat tutkimuksen etenemistä. Laajasti käytetty ja tunnettu viitekehys on Peffersin ym. (2007) esittämä kuusivaiheinen Design Science -prosessi, joka tarjoaa jäsennellyn lähestymistavan tutkimuksen toteuttamiseen. Vaiheet ovat seuraavat:

1. Tunnista ongelma ja perustele merkitys
2. Määrittele ratkaisun tavoitteet
3. Suunnittelu ja kehittäminen
4. Demonstrointi
5. Arviointi

6. Viestintä

Ensimmäinen vaihe sisältää tutkimusongelman tunnistamisen ja määrittelyn sekä perustelun sen tieteelliselle ja käytännön merkitykselle. Toisessa vaiheessa määritellään tavoitetila, eli mitä ratkaisulla pyritään saavuttamaan ja millaiset toteutusmahdollisuudet ovat olemassa. Kolmannessa vaiheessa kehitetään ratkaisu eli artefakti. Kehitetty artefakti voi olla menetelmä, malli tai teknologinen sovellus. Neljäs vaihe on tarkoitettu artefaktin toimivuuden havainnollistamiselle käytännön esimerkkien tai sovellusten avulla. Viidennessä vaiheessa arvioidaan artefaktin tehokkuus suhteessa alkuperäiseen ongelmaan ja tarkastellaan mahdollisia kehityskohteita. Kuudennessa vaiheessa tutkimuksen tuotokset ja niiden merkitys tuodaan esiin tutkimusyhteisölle ja muille sidosryhmille. (Peffers ym., 2007)

Tässä tutkielmassa Peffersin ym. (2007) esittämän suunnittelutieteellisen tutkimusprosessin vaiheet on sovellettu seuraavasti. Ensimmäinen ja toinen vaihe toteutuvat johdannossa ja tutkimuskysymysten määrittelyssä, jossa on esitelty ongelma ja sen merkitys sekä asetettu tavoitteet tutkimukselle. Kolmannessa vaiheessa kehitetään itse artefakti, joka on tämän tutkielman viitekehys. Tutkielman viitekehys on rakennettu niin, että sen avulla voidaan vastata, miten kokonaisarkkitehtuuri tukee häiriöiden hallintaa ja tarkastella näiden hyödyntämistä tutkittavassa organisaatiossa. Neljäs vaihe eli demonstrointi tarkoittaa tämän tutkielman tutkimusvaihetta, jonka tulokset on kirjattu osaksi tutkielmaa. Tutkimuksessa artefaktia eli tutkielman viitekehystä testataan toimeksiantajaorganisaation kokonaisarkkitehtuurin ja häiriöiden raportointijärjestelmän avulla. Arviointi eli viides vaihe sisältyy tutkimuksen tulosten esittelyyn, mutta toteutuu niiden syvällisemmässä analysoinnissa. Tämän lisäksi tutkielman artefaktia arvioidaan NIS2-direktiivin vaatimusten avulla. Kuudes vaihe eli viestintä toteutetaan tutkielman johtopäätöksissä, jossa käydään läpi tärkeimmät tulokset ja tutkielman keskeisimmät elementit.

Suunnittelutieteellisen tutkimusotteen rinnalla tutkimusstrategiaksi valikoitui laadullinen tapaustutkimus (engl. case study). Tapaustutkimukset sopivat tietojärjestelmätieteen tutkimuksiin (Williamson & Johanson, 2018), sillä mielenkiinto tutkittavissa ongelmissa on siirtynyt yhä enemmän teknisistä organisaatiokeskeisiin näkökulmiin (Benbasat ym., 1987). Lisäksi tapaustutkimuksia on hyödynnetty monipuolisten yritystoimintaan liittyvien ilmiöiden tarkastelussa.

Tapaustutkimus mahdollistaa usein monimutkaisten asiakokonaisuuksien esittämisen selkeällä ja ymmärrettävällä tavalla (Eriksson & Kovalainen, 2008). Tapaustutkimuksessa erityistä on se, ettei kaikkia tarkkoja teoreettisia konstruktioita tarvitse välttämättä tietää etukäteen, sillä ne voivat nousta esille tutkimuksen edetessä. Lisäksi on mahdollista muokata alkuperäistä tutkimuskysymystä

prosessin aikana ja tapaustutkimus voi auttaa saavuttamaan rikastetun, kontekstuaalisen ja aidon tulkinnan ilmiöstä. (Bhattacherjee, 2012.) Tapaustutkimus keskittyy yksilöön, ihmisryhmään tai yksikköön, mutta tavoittelee tutkimuksen havaintojen yleistystä useampaan yksikköön (Gustafsson, 2017). Tämä sopii tutkielman tavoitteisiin, sillä tulosten avulla halutaan toimeksiantajan lisäksi löytää ratkaisuja, jotka voisivat olla hyödyllisiä myös muiden organisaatioiden kokonaisarkkitehtuurityössä. Tapaustutkimuksen käyttö mahdollistaa monimutkaisten ja vaikeasti hahmotettavien liiketoimintaongelmien tarkastelun helposti lähestyttävässä ja käytännönläheisessä muodossa. Keskeisessä osassa onkin tutkimuskysymysten muotoileminen tapauksen ymmärtämisen ja ratkaisemisen tukemiseksi. Tapaustutkimuksen käyttö soveltuu tutkimuksiin, joissa halutaan saada tarkempi kuva jo olemassa olevasta teoriasta sekä tutkimuksiin, joissa halutaan luoda täysin uusi teoria. (Eriksson & Kovalainen, 2008.) Nämä tapaustutkimuksen attribuutit ovat sopivia tämän tutkimuksen osalta, sillä tutkittavassa aiheessa yhdistyvät sekä kokonaisarkkitehtuuri, häiriöiden hallinta, että NIS2-direktiivin vaatimukset organisaatiolle. Menetelmän avulla aihetta voidaan lähestyä kokonaisvaltaisesti ja moniulotteisesti, mikä voi edesauttaa uusien näkökulmien esiin nousemista.

Valittu tutkimusote ja -strategia tukevat tutkielman aiheen tarkoituksenmukaista tarkastelua. Suunnittelutieteellinen tutkimusote soveltuu erityisesti käytännönläheisten ja monitulkintaisten organisaatio-ongelmien tutkimiseen, kun taas laadullinen tapaustutkimus mahdollistaa ilmiön syvällisen ja kontekstuaalisen analyysin todellisessa toimintaympäristössä. Tämä lähestymistapojen yhdistelmä tukee tutkielman tavoitetta selvittää, miten kokonaisarkkitehtuuria voitaisiin hyödyntää häiriötilanteiden hallinnassa ja siten vähentää niiden negatiivisia vaikutuksia organisaatioon, sen toimintaan ja toimijoihin. Koska aihetta on tutkittu toistaiseksi vain rajallisesti, laadullinen lähestymistapa on perusteltu keino tarkastella ilmiötä tilanteessa, jossa ennakkotieto on vielä vähäistä (Eriksson & Kovalainen, 2008).

6.1.1 Tapauksen kuvaus

Tapaustutkimuksissa on tärkeää määritellä analyysiyksikkö eli mihin tutkimuksessa keskitytään. Tämän tutkimuksen analyysiyksikkönä ovat häiriöiden hallinta ja kokonaisarkkitehtuuri sekä niiden yhteensovittaminen NIS2-direktiivin vaatimuksiin. Lisäksi tärkeässä osassa on tutkimuskohteen valinta eli määrittely siitä, millaisesta organisaatiosta aineisto kerätään. (Benbasat ym., 1987.) Tässä tutkielmassa tutkimuskohteena on toimeksiantajaorganisaatio, joka on mallintanut ja kuvannut liiketoimintansa eri osa-alueet kokonaisarkkitehtuuriprojektissaan. Organisaatiolla on käytössään erillinen häiriöiden raportointijärjestelmä, johon on dokumentoitu tapahtuneet häiriöt, niiden

käsittelyn vaiheet sekä olennainen tieto. NIS2-direktiivin mukaan toimeksiantaja kuuluu kriittisen sektorin toimijoihin. Toimeksiantajaorganisaatio soveltuu erinomaisesti tutkimuskohteeksi, koska se on jo mallintanut kokonaisarkkitehtuuriaan, häiriöitä on seurattu systemaattisesti ja siihen kohdistuvat NIS2-direktiivin asettamat vaatimukset. Lisäksi se on riittävän suuri toimija ja häiriöistä löytyy paljon raportointeja. Tämä mahdollistaa sen, että analysoitavaa dataa on tarpeeksi.

Toimeksiantajaorganisaatiossa kokonaisarkkitehtuurin mallintamiseen käytetty järjestelmä on käytössä pääasiallisesti visuaalisten mallinnusten tekemiseen, järjestelmä listauksien dokumentointiin ja integraatioiden hahmotteluun. Kokonaisarkkitehtuuri on jaoteltu siellä viiteen osa-alueiseen: strategia ja liiketoiminnan ohjaustekijät, liiketoiminta-arkkitehtuuri, sovellusarkkitehtuuri, tietoarkkitehtuuri ja integraatioarkkitehtuuri. Toimeksiantajaorganisaation häiriöiden raportointijärjestelmässä on yksittäisiin häiriöihin liittyvien raporttien lisäksi koko organisaatiossa esiintyvien häiriöiden osalta tilastoja ja niihin liittyviä raportointinäkymiä (engl. dashboard). Tämän lisäksi myös häiriöiden raportointijärjestelmään on kerätty kokonaisarkkitehtuuriin liittyvää dataa kuten sovelluslistauksia ja integraatioita. Kokonaisarkkitehtuuriin liittyvää dataa löytyy siis molemmista järjestelmistä, mutta kummassakin järjestelmässä kokonaisarkkitehtuurin mallintaminen on vielä osittain keskeneräistä.

6.2 Aineiston keruu

Tutkielman aineisto kerättiin tarkastelemalla toimeksiantajan kokonaisarkkitehtuurin mallinnuksia ja häiriöiden raportointijärjestelmää. Menetelmänä käytettiin dokumenttianalyysiä, sillä tutkimus perustuu dokumenttiaineistoon, joka sisältää tekstisisältöjen lisäksi numeerista tietoa ja visuaalisia elementtejä. Dokumenttianalyysia on systemaattinen menettelytapa dokumenttien tarkasteluun ja arviointiin. Oleellista dokumenttianalyysissä on tuoda aineiston tutkimisen ja tulkinnan kautta esiin merkitystä, syventää ymmärrystä ja kehittää empiiristä tietoa. (Corbin & Strauss, 2014.) Dokumenttianalyysi käsittää prosessin, jossa aineistoa haetaan, valikoidaan, tulkitaan ja yhdistellään kokonaisuuksiksi (Labuschagne, 2003). Dokumenttianalyysissä tyypillisesti tarkastellaan aiempaa kirjallisuutta osana tutkimusta ja hyödynnetään sitä osana analyysiprosessia (Bowen, 2009). Aiemman kirjallisuuden tutkiminen on toteutettu tämän tutkielman kirjallisuuskatsauksessa.

Dokumenttianalyysin vahvuutena tapaustutkimuksissa on mahdollisuus käydä läpi dataa niin usein kun on tarpeen. Dokumentit eivät ole ainoastaan tutkimusta varten luotua dataa, mikä lisää aineiston autenttisuutta heijastamalla organisaation todellista toimintaa ja sen omaa tiedontuotantoa. Usein miten dokumentaatio on tarkkaa ja siinä voi olla laajasti kuvattuna eri tapahtumat ja aiheet.

Yleisenä haasteena dokumenttianalyysissä voi olla dokumenttien saaminen. Tämän lisäksi dokumentaatio on voitu suorittaa puutteellisesti tai data on vääristynyt esimerkiksi tekijän toimesta. (Yin, 2009). Tässä tutkielmassa haasteena ei ollut dokumentaatioon käsiksi pääsy, sillä toimeksiantaja tarjosi kattavat dokumentaatiot eri lähteistä. Tutkimukseen ja sen tuloksiin negatiivisesti vaikuttavat tekijät olivat paikoitellen dokumentaation puutteellisuus ja mahdolliset vääristymät datassa.

Dokumenttianalyysin rinnalla tutkimuksen aineistonkeruu pohjautuu suunnittelutieteellisen tutkimusotteen prosessin neljänteen vaiheeseen, jossa kehitettyä ratkaisua eli artefaktia demonstroidaan käytännön esimerkkien avulla. Tavoitteena on tunnistaa tapauksia, joiden kautta artefaktin toimivuutta voidaan empiirisesti tarkastella. Tässä tutkimuksessa kehitetty ratkaisu on tutkielman viitekehys ja sen toimivuutta tutkitaan toimeksiantajaorganisaation häiriöiden raportointiohjelmaan ja kokonaisarkkitehtuurimallinnuksiin peilaten.

Tutkimusta varten valittiin 2 sopivaksi katsottua häiriötä raportointijärjestelmästä, joita tarkasteltiin tutkielmassa aiemmin esitellyn viitekehyksen avulla. Toimeksiantajaorganisaation raportointijärjestelmään kirjataan yli 2000 häiriötä kuukaudessa, joista noin 95% on luokiteltu prioriteetiltaan matalaksi. Kohtalaisen prioriteetin häiriöitä on keskimäärin 100 kuukaudessa, korkean prioriteetin häiriöitä esiintyy muutamia kymmeniä ja kriittisen prioriteetin häiriöitä on alle 10 kuukaudessa. Häiriötapauksista nostetiin tutkimukseen sellaiset, joiden avulla pystyttiin mahdollisimman laajasti tutkimaan, miten viitekehyksessä tunnistetut elementit toteutuvat. Tästä syystä tutkimukseen valitut häiriöt ovat sellaisia, joiden käsittely on saatu päätökseen. Tutkimuksessa toimeksiantajan kokonaisarkkitehtuuria tutkittiin suhteessa häiriöraportteihin. Tämän avulla haluttiin selvittää kokonaisarkkitehtuurin mahdollinen rooli häiriöiden hallinnassa. Kokonaisarkkitehtuurin dataa ja mallinnuksia tutkimalla haluttiin selvittää, millä tasolla kokonaisarkkitehtuuri on ja miten se voisi tuke häiriöiden hallintaprosessia. Kokonaisarkkitehtuuridatasta poimittiin häiriötilanteet mielessä pitäen oleellinen tieto ja tutkittiin sitä viitekehyksen avulla.

Tutkimus aloitettiin syventymällä valittuihin häiriöihin raportointijärjestelmässä tehtyjen kirjausten avulla. Molemmista häiriöistä oli tehty omat raportit järjestelmään, jossa näkyivät perustietojen lisäksi kirjaukset häiriön selvittämisprosessin etenemisestä, häiriöön liittyvien osapuolten välisestä kommunikaatiosta ja mahdolliset lisätiedot toisista häiriöistä, jotka liittyivät kyseisiin häiriöihin. Häiriöiden alustavan läpikäynnin jälkeen tutkittiin häiriöitä tarkemmin tutkielman viitekehyksen avulla. Ensin katsottiin, miten NIST kyberturvallisuusviitekehyksestä johdetut toiminnot toteutuivat

valittujen häiriöiden osalta. Tämän jälkeen häiriöitä ja niiden raportointia tutkittiin kokonaisarkkitehtuurin näkökulmasta keskittymällä Kotusevin nimeämiin kahdeksaan artefaktiin. Tätä varten tutkimuksessa käytiin tarkasti läpi, millaisia mallinnuksia toimeksiantajaorganisaatio on tehnyt ja miten ne vastasivat Kotusevin kahdeksaa artefaktia. Tutkimuksessa etsittiin yhtymäkohtia häiriöiden raportoinnissa ja kokonaisarkkitehtuurissa eli etsittiin sellaisia kokonaisarkkitehtuurin mallinnuksia, joita oli hyödynnetty tai voisi hyödyntää osana häiriöiden hallintaa. Tämän lisäksi tutkimuksessa arviointiin, kuinka laajasti kokonaisarkkitehtuuria oli mallinnettu toimeksiantajaorganisaatiossa ja miten sitä oli ylläpidetty. Tätä varten käytettiin tutkimuksen toteuttamisessa huomattavasti aikaa toimeksiantajaorganisaation kokonaisarkkitehtuurin läpikäyntiin. Kokonaisarkkitehtuuria on mallinnettu kerroksittain eli kokonaisarkkitehtuurista löytyy eri tasoja, jotka mallintavat dataa yksityiskohtaisemmin. Jotta tutkimuksessa voitiin tehdä päätelmiä toimeksiantajan kokonaisarkkitehtuurin osalta, oli kokonaisarkkitehtuurin mallinnuksiin perehdyttävä huolella. Kokonaisarkkitehtuurin mallinnukset olivat pääasiassa tähän tarkoitetussa järjestelmässä, mutta osa kokonaisarkkitehtuuriin liittyvästä datasta oli tallennettuna häiriöiden raportointijärjestelmään. Aikaa kului myös siihen, että selvitettiin, mihin etsitty data oli tallennettu vai puuttuiko se kokonaan.

Alla olevassa taulukossa on esitelty kaksi tutkimukseen valittua häiriötä. Häiriö A koski puhelinyhteyksissä olevaa ongelmaa. Organisaation toimipisteessä oli huomattu aamulla klo 4, ettei toimipisteen sisällä pystytty saada yhteyttä puhelimitse toisiin organisaation puhelimiin, mutta asiasta tehtiin häiriöilmoitus vasta klo 7 aamulla. Häiriö oli arvioitu kiireellisyydeltään ja vaikutukseltaan korkeaksi sekä prioriteetiltaan kriittiseksi. Häiriössä ensisijainen vaikutus kohdistui mobiililaitteisiin. Ilmoituksesta kesti 8 tuntia ja 11 minuuttia, että häiriö saatiin ratkaistua. Raportointijärjestelmään häiriö merkattiin suljetuksi 5 vuorokautta 8 tuntia ja 56 minuuttia ilmoittamisen jälkeen. Häiriö B:ssä toiminnanohjausjärjestelmässä varastosaldojen siirto eri varastojen välillä ei onnistunut. Häiriö oli luokiteltu vaikutukseltaan ja kiireellisyydeltään korkeaksi sekä prioriteetiltaan kriittiseksi. Ensisijaisesti häiriö vaikutti organisaation toiminnanohjausjärjestelmään. Häiriön ratkaisemiseen meni 6 tuntia ja 11 minuuttia ja häiriö merkittiin suljetuksi 2 vuorokautta 4 tuntia 50 minuuttia ilmoituksen jälkeen.

Taulukko 2 Tutkimuksessa analysoidut häiriöt

Häiriö	Aihe	Kiireellisyys	Vaikutus	Prioriteetti	Vaikutuksen alainen rakenneosa	Kesto Ratkaistu/ Suljettu
Häiriö A	Puhelin yhteydet alhaalla	Korkea	Korkea	Kriittinen	Mobiililaitteet	8h 11min/ 5vrk 8h 56min
Häiriö B	Varastosaldojen päivitys tuotannonohjaus-järjestelmässä	Korkea	Korkea	Kriittinen	Toiminnanohjaus-järjestelmä	6h 11min/ 2vrk 4h 50min

Aineistonkeruussa on huomioitava, että tarkasteluun valitut kaksi häiriötä eivät edusta kattavasti kaikkia organisaatiossa esiintyviä häiriöitä, joita on kirjattu raportointijärjestelmään keskimäärin yli 2000 kuukaudessa. Tämä rajoittaa tutkimustulosten yleistettävyyttä. Valittujen häiriöiden avulla pyritään kuitenkin ennen kaikkea arvioimaan tutkimuksen viitekehyksen sovellettavuutta ja sitä kautta selvittämään, miten kokonaisarkkitehtuuria voidaan hyödyntää häiriöiden hallinnassa mahdollisimman laaja-alaisesti. Lisäksi on tärkeää huomioida, että organisaation kokonaisarkkitehtuurityö on vielä osin keskeneräistä, mikä vaikuttaa siihen, kuinka yksityiskohtaisesti tietyt osa-alueet ja toiminnot on mallinnettu. Yleinen haaste dokumenteissa aineistomuotona on niissä mahdollisesti esiintyvät vinoumat, mikäli raportointi on ollut puutteellista tai ne sisältävät tekijän subjektiivisia näkemyksiä. Näistä rajoituksista huolimatta tutkimuksessa on pyritty rakentamaan mahdollisimman monipuolinen näkökulma tutkielman kannalta keskeisiin kysymyksiin.

6.3 Aineiston analyysi

Tutkimuksen analyysivaiheeseen sisältyi kaksi eri osaa. Ensin analysoitiin kerättyä aineistoa tutkielman viitekehyksen avulla ja sen jälkeen suunnittelutieteellisen tutkimusotteen mukaisesti arvioitiin artefaktia eli itse viitekehystä. Näiden kahden vaiheen tavoitteena oli selvittää:

1. Tapaustutkimuksen mukaisesti, miten häiriöiden hallinta ja kokonaisarkkitehtuuri yhdistyvät toimeksiantajaorganisaatiossa ja mitä tästä voidaan havaita yleisesti liittyen kokonaisarkkitehtuurin ja häiriöiden hallinnan välisestä yhteydestä.

2. Onko tutkielmassa hahmoteltu viitekehys mahdollinen työkalu kokonaisarkkitehtuurin ja häiriöiden hallinnan yhdistämiseen ja sen myötä tapa vastata NIS2-direktiivin vaatimuksiin?

Analyysin ensimmäisessä vaiheessa on hyödynnetty Yin (2009) esittelemää analyysistrategiaa, jossa kerättyä aineistoa analysoidaan viitekehyksen ja teoreettisen taustan kautta. Teoreettisena taustana toimii tutkielman kirjallisuuskatsaus, joka on määrittänyt koko tutkimuksen suuntaa. Tämän analyysistrategian vahvuutena on teorian ja empiirisen aineiston yhdistäminen, mikä luo johdonmukaisuutta läpi koko tutkielman. Tässä tutkimuksessa kerätty data on analysoitu tutkielman yhteydessä luodulla viitekehyksellä, joka on rakennettu NIST kyberturvallisuusviitekehykseen ja Kotusevin kahdeksaan artefaktiin pohjautuen. Viitekehystä käytetään arvioimaan toimeksiantajan kokonaisarkkitehtuurista ja häiriöiden raportointijärjestelmästä kerättyä dataa ja tutkitaan, kuinka hyvin se vastaa NIS2-direktiivin vaatimuksia sekä kokonaisarkkitehtuurin häiriötilanteiden hallinnan elementtejä.

Toinen vaihe analyysiprosessissa on suunnittelutieteellisen tutkimusotteen mukaisesti artefaktin eli viitekehyksen demonstrointi ja arviointi. Demonstrointi ja arviointi ovat olennaisia vaiheita suunnittelutieteellisessä prosessissa, ja ne toteutuvat osana tutkimuksen analyysia. Suunnittelutieteellistä tutkimusotetta on esitelty tarkemmin alaluvussa 6.1 Tutkimusote ja -menetelmä. Suunnittelutieteellinen tutkimusote edellyttää, että kehitettävää artefaktia ei ainoastaan suunnitella, vaan myös demonstroidaan käytännön kontekstissa ja arvioidaan sen toimivuutta suhteessa asetettuihin tavoitteisiin. Näillä toimenpiteillä varmistetaan artefaktin ajankohtaisuus, käytettävyys ja mahdolliset vaikutukset kohdeympäristöön. Demonstrointi- ja arviointivaiheet muodostavat keskeisen osan suunnittelutieteellisen tutkimuksen prosessia ja tukevat tutkimuksen tieteellistä luotettavuutta.

Artefaktin eli tutkielman viitekehyksen arviointi toteutui analysoimalla, miten kyseisen viitekehyksen avulla voidaan vastata NIS2-direktiivin asettamiin vaatimuksiin. NIS2-direktiivi toimii tässä arviointipohjana tutkielman viitekehykselle, koska kriittisten sektorien toimijoiden on toteutettava häiriöiden hallintansa NIS2-direktiivin vaatimusten mukaisesti. Tutkielman viitekehys puolestaan edustaa kokonaisarkkitehtuurille ja häiriöiden hallintaprosessille tunnistettua vaatimustasoa. Tämän vuoksi on perusteltua, että NIS2-direktiivin vaatimusten toteutumista kokonaisarkkitehtuurin avulla on tässä tutkimuksessa tutkittu vertaamalla viitekehyksen ominaisuuksia direktiivin asettamiin vaatimuksiin. Tutkimuksessa keskityttiin kuuteen pääosa-alueeseen, joita NIS2-direktiivissä vaaditaan kriittisten sektorien toimijoilta. Nämä olivat:

1. Vastuu toimitusketjuista

2. Häiriöiden hallinnan vahvistaminen
3. Häiriöiden raportoinnin aikarajan tiukentaminen
4. Riskienhallinta
5. Jatkuvuudenhallinta
6. ”Kyberhygienia” ja kouluttaminen

Näillä osa-alueilla tarkasteltiin viitekehyksen sovellettavuutta ja sitä, miten hyvin sen avulla voidaan toteuttaa yleisesti kyberturvallisuutta organisaatioissa sekä tarkemmin häiriöiden hallintaa. Kyberturvallisuus ja häiriöiden hallinta ovat monimutkaisia kokonaisuuksia, joiden onnistunut toteutus edellyttää organisaatioilta systemaattista ja laaja-alaista toimintaa. Näin ollen myös tässä hyödynnettävän viitekehyksen on pystyttävä käsittämään useita eri osa-alueita.

6.4 Tutkimuksen luotettavuus ja etiikka

Tutkimusetiikka muodostaa keskeisen perustan tieteelliselle tutkimukselle, ja tutkijan on tehtävä eettisesti kestäviä ratkaisuja tutkimuksen eri vaiheissa (Tuomi & Sarajärvi, 2018). Eettisesti toteutettu tutkimus lisää tutkimusprosessin läpinäkyvyyttä, mahdollistaa tutkimuksen vahvuuksien ja rajoitteiden tunnistamisen sekä tukee sen luotettavuuden ja laadun arviointia (Eriksson & Kovalainen, 2008). Tässä tutkimuksessa tehdyillä eettisillä valinnoilla on pyritty nimenomaan edistämään näitä periaatteita.

Tutkimukseen osallistuva toimeksiantajaorganisaatio on pidetty nimettömänä tutkimusetiikan ja luotettavuuden varmistamiseksi. Kaikki organisaatiolta saatu tieto ja aineisto on käsitelty, tallennettu ja raportoitu siten, ettei siitä voida tunnistaa organisaatiota tai paljastaa sen kannalta kriittistä tai arkaluontoista sisältöä. Toimeksiantajaorganisaatio on määritellyt, mihin aineistoihin tutkimuksella on käyttöoikeus. Heille on myös esitelty tutkielman eri vaiheissa, millaista dataa tutkimuksessa on tarkoitus käsitellä ja mihin tarkoituksiin sitä käytetään.

Tutkimuksessa oleellisessa osassa on aineiston hallinta ja sen toteuttaminen eettisesti. Tutkielman aineistonhallintasuunnitelma tehtiin ennen aineiston keräämistä ja sitä ylläpidettiin osana tutkimusprosessia. Siinä on esitelty muun muassa, mistä tutkimusaineisto koostuu ja miten sitä on tutkimuksen aikana säilytetty. Viimeistelty aineistonhallintasuunnitelma on lisätty tutkielman liitteeksi (liite 1).

Tutkielmassa on huolehdittu eettisyydestä myös tekoälyn vastuullisella käytöllä. Työssä on käytetty ChatGPT:n versioita 3.5 ja 4.0, ja niiden käyttö on rajoittunut eettisesti hyväksyttäviin tarkoituksiin, kuten ideoinnin tukemiseen, vieraskielisten tekstien kääntämiseen ja oman tekstin tarkistamiseen. Tekoälyä on hyödynnetty esimerkiksi englanninkielisten termien käännöksissä sekä kirjoitusvirheiden tarkistuksessa. Tekoäly ei ole kirjoittanut tutkielman varsinaisia sisältöjä, mutta sen avulla on haettu parempia sanavalintoja ja ilmaisutapoja. Tekoälysovelluksilla ei ole käsitelty mitään toimeksiantajaorganisaatiolta saatua dataa, eikä mitään muuta arkaluontoista sisältöä. Tekoälyn avulla on perehdytty tutkielmaan liittyviin aiheisiin, mutta sen tarkoituksena on ollut oman ymmärryksen syventäminen, eikä tekoälyn tuottamia selityksiä ole käytetty osana tutkielmaa. Tekoälyä on käytetty yksinomaan Turun yliopiston ohjeistuksia noudattaen. Selvitys generatiivisen tekoälyn käytöstä (Declaration on the Use of Generative Artifical Intelligence) löytyy tutkielman lopusta liitteenä 2 ja käytöstä on yleisesti ilmoitettu tutkielman johdannossa.

7 Tulokset

Aineiston analyysin kautta tunnistettiin kokonaisarkkitehtuurilla olevan huomattavia vaikutuksia häiriöiden hallintaan. Tutkimuksen avulla löydettiin seitsemän tapaa, joilla kokonaisarkkitehtuuri tukee häiriöiden hallintaa. Tämän lisäksi analyysin avulla on tutkittu, miten kokonaisarkkitehtuuri pystyy tukemaan NIS2-direktiivin vaatimuksiin vastaamisessa. Tutkimuksessa tunnistettiin kolme osa-aluetta, joissa kokonaisarkkitehtuuri vastasi NIS2-direktiivin vaatimuksiin. Tämän luvun ensimmäisessä alaluvussa on esitelty kokonaisarkkitehtuurin ja häiriöiden hallinnan välisestä yhteydestä tunnistetut attribuutit ja keskitytty tutkimustuloksiin, joilla haettiin vastausta ensimmäiseen tutkimuskysymykseen. Toisessa alaluvussa on keskitytty NIS2-direktiivin vaatimusten toteutumisen tarkasteluun ja tarkasteltu tutkimuksessa toisen tutkimuskysymyksen kannalta oleellisiin tutkimustuloksiin.

7.1 Kokonaisarkkitehtuurin vaikutus häiriöiden hallintaan

Häiriöiden hallintaprosessin yhtenäistäminen

Toimeksiantajaorganisaation häiriöiden raportoinnista pystyttiin löytämään molempien häiriöiden osalta tutkielman viitekehyksen mukaisesti kaikki muut toiminnot paitsi ohjaa-toiminto. Ohjaa-toiminto luo strategisen pohjan turvallisuuskäytänteille sekä yhteisen linjan organisaation toiminnalle ja tavoitteille, mikä toimii perustana muille toiminnoille. Vaikka häiriöiden raportointijärjestelmä luo itsessään tietynlaisen kaavan, jolla raportointi toteutetaan, ei tämä riitä vielä täysin toteuttamaan viitekehyksessä tunnistetun ohjaa-toiminnon tarkoitusta. Ohjaa-toimintoon liittyy tutkielman viitekehyksen mukaisesti artefakti periaatteet. Periaatteet muodostavat organisaatiolle perussäännöt, arvot, suuntaviivat ja tavoitteet. Kuten ohjaa-toiminto oli myös periaatteiden tunnistaminen toimeksiantajaorganisaatiossa haasteellista. Selkeän yhteisen linjan muodostaminen olisi oleellista sekä häiriöiden hallinnan että kokonaisarkkitehtuurityön kannalta. Ne määrittävät muiden toimintojen ja artefaktien käytön organisaatiossa sekä varmistavat sen, että toimintoja ja artefakteja käytetään samalla tavalla eri häiriöissä. Tässä tunnistettiin tapa, jolla kokonaisarkkitehtuuri voisi tukea häiriöiden hallintaa. Toimeksiantajaorganisaatiossa tämä tarkoittaisi kuitenkin artefaktin lisäksi mahdollisesti uusien toimintamallien kehittämistä.

Häiriöiden laajuuden selvittäminen organisaation rakenneosissa

Tunnista-toiminnon avulla voidaan organisaatiossa tunnistaa riskit ja resurssit, joiden avulla pystytään ennakoimaan häiriön vaikutuksia sekä missä häiriö voisi realisoitua.

Toimeksiantajaorganisaatiossa tunnista-toiminto toteutuu osittain häiriöiden raportointijärjestelmässä luokittelemalla häiriö sen vaikutuksen, kiireellisyyden ja prioriteetin mukaan. Häiriöstä listataan lisäksi muita perustietoja kuten sijainti, ilmoittaja ja mihin rakenneosaan häiriö vaikuttaa. Nämä voidaan laskea osaksi tunnista-toimintoa, mutta kokonaisavaltaisesti riskien ja resurssien havainnointi ei toteudu järjestelmässä. Tunnista-toiminnon osalta oleellinen kokonaisarkkitehtuurin artefakti tutkielman viitekehyksen mukaan on teknologian viitemallit. Teknologian viitemallien tunnistaminen toimeksiantajaorganisaation kokonaisarkkitehtuurissa osoittautui epäselväksi. Tämä havainto paljasti samalla puutteen, joka vaikeuttaa tunnista-toiminnon tehokasta toteuttamista. Häiriötilanteen käsittelyssä oli tunnistettu välitön rakenneosa, johon häiriö vaikutti, mutta häiriön vaikutuksen laajuudesta ei voitu nopeasti tehdä päätelmiä. Tässä tunnistettiin merkittävä tapa, jossa kokonaisarkkitehtuurilla voitaisiin tukea häiriöiden hallintaa. Tarpeeksi kattavalla teknologian viitemallilla pystyttäisiin häiriöiden hallintaprosessissa kehittämään tehokasta riskien ja resurssien tunnistamista heti häiriöilmoituksen jälkeen tai jopa ennakoivasti. Lisäksi voitaisiin tunnistaa ne organisaation järjestelmät, jotka ovat suoraan yhteydessä ulkopuolisiin sidosryhmiin. Tällöin voidaan arvioida, missä määrin tunnistetun häiriön vaikutukset voivat levitä organisaation ulkopuolelle.

Häiriöiden hallintaprosessin selkeyttäminen ja systemaattinen toteutus

Suojaa-toimintoon tutkielman viitekehyksessä on yhdistetty kokonaisarkkitehtuurin artefakteista ohjeistukset ja tiekartat. Ohjeistukset eivät olleet toimeksiantajaorganisaatiossa selkeästi esillä. Artefaktina ohjeistusten rooli on olla kertomassa, miten teknologian viitemalleissa määriteltyjä teknologioita tulisi organisaatiossa käyttää. Ohjeistukset kulkevat organisaatiossa enemmän hiljaisena tietona eteenpäin siitä, miten eri järjestelmiä hyödynnetään. Tämä heijastaa aikaisemmin tutkimuksessa huomattua puutetta ohjaa-toiminnon ja periaatteiden osalta. Tämä voi olla yksi syy sille, miksi toimeksiantajaorganisaatiossa kokonaisarkkitehtuurityö jakautuu kokonaisarkkitehtuurin mallintamisjärjestelmään ja häiriöiden raportointijärjestelmään. Kokonaisarkkitehtuurin tarkoituksena on tuoda selkeyttä ja ketteryyttä organisaation toimintaan, mutta tämä vaatii sen, että kokonaisarkkitehtuuria mallinnetaan rakenteellisesti yhdenmukaisesti, systemaattisesti ja yhteisten linjausten mukaisesti. Tällöin ei haittaa, vaikka järjestelmien määrä olisi suuri, koska rakenne tukee kokonaisuuden ylläpitoa. Tämä ei täysin toteudu tutkitussa organisaatiossa, mikä johtaa päällekkäiseen ylläpitoon sekä puutteisiin, jotka saattavat tulla näkyväksi vasta häiriötilanteissa. Ohjeistusten merkitys korostuu suojaa-toiminnossa, kun häiriötilanteessa tavoitellaan nopeaa, systemaattista ja kattavaa toimintaa. Niiden avulla varmistetaan, että huolimatta siitä, kuka häiriön kohtaa, tietää hän, miten toimia, jotta organisaation kannalta tärkeät suojatoimet saadaan tehtyä.

Tästä tunnistettiin, että kokonaisarkkitehtuuri voisi auttaa häiriöiden hallinnassa luomalla yhteiset toimintamallit ja määrittelemällä selkeästi, miten häiriöiden hallintaprosessin tulisi organisaatiossa toimia.

Häiriöiltä suojautuminen ja ennakointi

Toinen suojaa-toimintoon liittyvä kokonaisarkkitehtuurin artefakti tutkielman viitekehyksessä on tiekartat. Tiekarttoja oli mallinnettuna toimeksiantajaorganisaation kokonaisarkkitehtuurissa. Näissä tiedot olivat paikoittain puutteellisia, eivätkä täysin ajan tasalla. Monien tiekarttojen päättymispäiväksi oli lisäksi merkitty 31.12.2025 eli päivittämis- ja suunnittelutyö näiden osalta oli keskeneräistä. Tämä voi mahdollisesti kasvattaa toimeksiantajaorganisaation alttiutta häiriöille, mikäli esimerkiksi eri järjestelmien elinkaaresta ei ole selkeää kuvaa. Tällöin oleelliset päivitykset, uudet investoinnit tai muut suojatoimet voivat jäädä tekemättä. Tiekartat tukisivat häiriöiden hallinnassa ennakointia ja varautumista, mikä edistää suojaa-toiminnon tavoitteita. Tästä tunnistettiin kokonaisarkkitehtuurin merkitys ennakoivien toimenpiteiden edistämisessä osana häiriöiden hallintaa.

Häiriöiden analysointi ja syiden tunnistus

Havaitse-toimintoon kuuluvat tutkielman viitekehyksessä artefakteista liiketoimintakyvykkyysmallit ja arkkitehtuurin maisemakaaviot. Toiminnossa keskitytään uhka- ja poikkeamahavaintojen tekemiseen sekä analysoimiseen. Tämä toiminto on häiriöiden raportointijärjestelmän oleellisin tarkoitus ja toteutuu alusta loppuun saatetuilla häiriöraporteilla. Tutkituissa häiriöissä raportointiosuus toteutuu, mutta analysointiin ei ole käytetty juuri aikaa tai sitä ei ole merkitty järjestelmään. Molemmat artefaktit olivat löydettävissä toimeksiantajaorganisaation kokonaisarkkitehtuurista, mutta liiketoimintakyvykkyysmalleja oli muokattu viimeksi maaliskuussa 2023. Tämä vaikuttaa oleellisesti kyseisen artefaktin paikkansapitävyyteen. Liiketoiminnankyvykkyysmalleilla voitaisiin avustaa analysoinnin tekemistä osana häiriöiden hallintaa, sillä ne muodostavat jäsennellyn ja strategisiin tavoitteisiin kytketyn kokonaisuuden. Tämä tukisi havaittujen poikkeamien tulkintaa liiketoimintanäkökulmasta.

Häiriöiden vaikutusten laajuuden selvitys

Arkkitehtuurin maisemakaaviot ovat yksi niistä kokonaisarkkitehtuurin osista, jotka toimeksiantajaorganisaatiolla on mallinnettuna häiriöiden raportointijärjestelmässä. Häiriöiden raportoinnissa oli käytössä arkkitehtuurin maisemakaavioita vastaavat riippuvuuskaaviot, jotka sisälsivät artefaktin kanssa samanlaisia tietoja kuten rakenneosien väliset suhteet, mahdolliset

riippuvuudet ja vaikutusalueet. Kuitenkin tutkimuksessa huomattiin, että vain toisessa tutkituista häiriöistä kaavio sisälsi paikkansa pitävää dataa. Tämä tieto olisi oleellista, kun häiriö havaitaan ja lähdetään selvittämään, mihin kaikkialle sen vaikutukset ovat levinneet tai voivat levitä. Häiriöiden hallinnassa tämä toisi merkittävää etua prosessin läpiviennissä sekä sen jälkeisessä analysoinnissa. Tästä tunnistettiinkin, miten kokonaisarkkitehtuuri tukee häiriöiden hallintaa mahdollistamalla vaikutusalueen ja riippuvuuksien tehokkaan tunnistuksen sekä poistamalla aukot, joista häiriön vaikutukset pääsevät leviämään organisaatioissa niin, ettei sitä huomata.

Häiriöihin reagointi

Reagoi-toiminnossa tehdään konkreettisia toimia havaitse-toiminnossa tunnistettuihin häiriötilanteen osa-alueisiin. Reagoi-toiminnossa pyritään vastaamaan havaittuun häiriöön tehokkaasti ja hallitusti. Tutkittujen häiriöiden raportoinnissa kävi ilmi, että Häiriö A:ssa reagointi tapahtui johdonmukaisesti virallisen ilmoituksen jälkeen, mutta ilmoitus tehtiin vasta 3 tuntia sen jälkeen, kun ongelma oli ensimmäisen kerran huomattu. Molemmissa häiriöissä reagoi-toimintoon kuului yhteistyö organisaation palveluntoimittajien kanssa. Reagoi-toimintoon on liitetty tutkielman viitekehyksessä artefakteista ratkaisusuunnitelmat. Niiden tarjoamia olemassa olevia suunnitelmia voidaan hyödyntää esimerkiksi korjaavien toimenpiteiden teknisessä toteutuksessa, infrastruktuurin palauttamisessa tai vaihtoehtoisten ratkaisujen käyttöönotossa. Tutkielman viitekehyksessä tunnistettua artefaktia vastaavaa ei löytynyt toimeksiantajaorganisaation kokonaisarkkitehtuurista. On kuitenkin todettava, että käytössä olevassa raportointijärjestelmässä muodostuu tietynlainen kaava, joka vaikuttaa häiriöiden hallintaprosessissa. Tämä ei silti täytä ratkaisusuunnitelman tuomia puolia häiriöiden hallinnassa. Tutkimuksen perusteella ei voitu suoraan todeta, että ratkaisusuunnitelmat olisivat edistäneet häiriöihin reagointia merkittävästi. Ne voisivat osassa tapauksista tukea prosessin etenemistä, mutta häiriöiden määrä ja variaatio toimeksiantajan kaltaisissa organisaatioissa on niin suurta, ettei yleispäteviä tai moniin erilaisiin tarkoituksiin sopivia ratkaisusuunnitelmia ole mahdollista ylläpitää. Lisäksi on huomioitava, että digitaalisen transformaation myötä häiriöiden kehittyminen on entistä nopeampaa, eikä niitä voida aina etukäteen ennustaa.

Häiriöiden jälkeisen palautumisprosessin tukeminen

Viimeisenä tutkittiin palauta-toiminnon toteutumista ja siihen tutkielman viitekehyksessä yhdistettyä artefaktia ratkaisukuvaukset. Palauta-toiminnossa oleellista on keksittyä viestintään, normaalin toiminnan palauttamiseen oikea aikaisesti sekä häiriöstä aiheutuneiden vaikutusten minimoimiseen, jotta häiriön jälkeen saavutetaan normaali toiminnan tila mahdollisimman

sujuvasti. Häiriössä A palauta-toiminto on toteutunut pääasiassa systemaattisesti ja oleelliset toimenpiteet on suoritettu. Häiriön kohdalla ei ole kuitenkaan raportoinnin perusteella selvitetty, mihin muihin toimintoihin häiriö on voinut vaikuttaa ja siten suunniteltu palauta-toimintoa niiden osalta. Häiriö B:n kohdalla palauta-toiminto eteni aluksi sujuvasti, mutta raportin perusteella jää epäselväksi, varmistettiinko tilanteen lopullinen korjaantuminen. Viimeisessä kuittauksessa todetaan vain, että ilmoitetaan, jos ongelma toistuu, mutta ei suoraan vahvisteta, että häiriön syy olisi ratkaistu ja korjaavat toimenpiteet tehty. Kun uusia ilmoituksia ei ole saapunut, häiriö on merkitty suljetuksi myöhemmin järjestelmässä. Ratkaisukuvauksien tarkoituksena on tarjota tietoa, jonka avulla häiriöistä palautuminen voidaan toteuttaa suunnitelmallisesti ja tärkeimpiä osa-alueita priorisoiden sekä tunnistamalla kriittiset rajapinnat. Toimeksiantajaorganisaation kokonaisarkkitehtuurista löydettiin ratkaisukuvauksia vastaava mallinnus. Kuten Häiriön B kohdalla huomattiin häiriön jälkeinen palautuminen ja siihen liittyvien toimien toteuttaminen, ei seurannut järjestelmällistä kaavaa tai toteutunut kattavasti. Tämä mahdollistaa sen, että häiriö ei tule täysin ratkaistuksi ja sen vaikutukset organisaatiossa jatkuvat tai ei olla huomattu, jotain sivullista tahoa, jonka osalta palauttavia toimia olisi pitänyt suorittaa. Tällöin häiriö voi edelleen uhata organisaation toimintaa. Tästä tunnistettiin, että ratkaisukuvauksia hyödyntämällä osana häiriöiden hallintaprosessia, voitaisiin vähentää mahdollisuutta häiriön uusimiselle tai sen vaikutusten huomaamattoman leviämisen muihin organisaation osa-alueisiin.

Tutkielman viitekehystä apuna käyttäen tunnistettiin siis seitsemän tapaa, joilla kokonaisarkkitehtuuri tukee häiriöiden hallintaa organisaatioissa. Ensimmäinen tunnistettu tapa liittyi ohjaa-toimintoon ja periaatteet-artefaktiin. Tässä kokonaisarkkitehtuurin tukisi häiriöiden hallintaa määrittämällä yhtenäisen linjan häiriöiden hallintaprosessille, mikä varmistaisi, että eri häiriöitä ei käsiteltäisi vaihtelevalla tarkkuudella tai toimittaisi prosessin aikana vastoin organisaation suurempia tavoitteita. Toinen tunnistettu tapa liittyi tunnista-toimintoon ja teknologian viitemallit -artefaktiin. Tässä kokonaisarkkitehtuurin avulla voitaisiin tukea häiriön laajuuden selvittämistä, mikä puolestaan tehostaisi siitä seuraavien toimenpiteiden toteutusta sekä häiriön vaikutusten kokonaisvaltaista ratkaisemista. Kolmas tunnistettu tapa liittyi suojaa-toimintoon ja ohjeistukset-artefaktiin. Tässä kokonaisarkkitehtuuri voisi tukea häiriöiden hallintaprosessin systemaattista toteutusta ja selkeyttää prosessiin liittyviä toimenpiteitä. Näin jokaisen häiriön kohdalla ei lähdettäisi alusta asti miettimään, mitä tulisi tehdä vaan voitaisiin seurata ennalta määriteltyjä ohjeistuksia, jolloin mahdollisuus sille, että jotain jäisi tekemättä pienenee. Neljäs tunnistettu tapa liittyi suojaa-toiminnon toiseen artefaktiin tiekarttoihin. Tässä kokonaisarkkitehtuurin merkitys liittyi häiriöiltä suojautumiseen ja niiden ennakointiin. Viides

tunnistettu tapa liittyi havaitse-toimintoon ja liiketoimintakyvykkyysmallit-artefaktiin. Tässä kokonaisarkkitehtuuri tukisi häiriöiden analysointia, mikä on oleellisessa osassa häiriöiden hallintaa, kun halutaan selvittää mahdollisimman tarkasti, miten häiriö organisaatiossa vaikuttaa. Kuudes tunnistettu tapa liittyi havaitse-toiminnon toiseen artefaktiin arkkitehtuurin maisemakaavioihin. Tässä kokonaisarkkitehtuuri tukisi häiriöiden hallinnassa häiriön ja sen vaikutusten laajuuden selvittämistä, mikä edistäisi häiriön kokonaisvaltaista hallitsemista. Seitsemäs tunnistettu tapa liittyi palauta-toimintoon ja ratkaisukuvaukset-artefaktiin. Tässä kokonaisarkkitehtuuri tukisi häiriöiden hallintaprosessia luomalla selkeän kuvan siitä, missä häiriö on vaikuttanut ja miten sen jälkeen toisiinsa liittyviä toimintoja voidaan lähteä palauttamaan.

7.2 NIS2-direktiivin vaatimusten toteutuminen

NIS2-direktiivi asettaa organisaatioille useita vaatimuksia, joiden tarkoituksena on vahvistaa koko EU:n kyberturvallisuutta. Yleisellä tasolla tämä tarkoittaa niille organisaatioille, joita vaatimukset koskevat, että heidän tulee pystyä havaitsemaan omaan toimintaan kohdistuvat kyberuhat ja -riskit. Tämä edellyttää lisäksi oman toiminnan tuntemista ja sen kriittisten osa-alueiden selvittämistä. Tavoitteena on, että organisaatiot pystyvät rakentamaan itselleen kybersietoisuuden, joka parantaa niiden kykyä toimia tämän päivän ja tulevaisuuden uhkien vallitessa.

Tutkimuskysymys, johon haettiin vastausta, oli ”*Voidaanko kokonaisarkkitehtuurin avulla vastata NIS2-direktiivin asettamiin vaatimuksiin?*”. Tätä tutkittiin soveltamalla suunnittelutieteellisen tutkimusotteen arviointivaihetta, jossa arvioitiin tutkielmassa kehitettyä viitekehystä artefaktina. Tutkimuksessa muodostettiin NIS2-direktiivin vaatimuksista kuusi pääosa-aluetta ja analysoitiin, miten nämä osa-alueet toteutuvat viitekehyksen avulla.

Ensimmäinen osa-alue oli vastuu toimitusketjuista. Tähän NIS2-direktiivin vaatimukseen viitekehys ja kokonaisarkkitehtuuri voi vastata riittävällä tavalla. Organisaation kokonaisarkkitehtuuriin mallinnetaan omien sisäisten prosessien rinnalla koko toimintaympäristö, jossa tulisi näkyä tärkeät sidosryhmät. Näihin lukeutuvat esimerkiksi toimittajat, alihankkijat, pilvipalvelut tai logistiikkakumppanit. Viitekehyksen havaitse-toiminnossa keskitytään erityisesti tähän, kun hyödynnetään kokonaisarkkitehtuurin liiketoimintakyvykkyysmallit-artefaktia, jossa tärkeimpien sidosryhmien kuten, keskeisten asiakasryhmien ja yhteistyökumppanien, tulisi näkyä.

Toinen tarkasteltu osa-alue oli häiriöiden hallinnan vahvistaminen. NIS2-direktiivi vaatii organisaatioilta häiriöiden hallinnan osalta systemaattista prosessia, jonka avulla häiriöt voidaan havaita, niihin reagoida, jatkaa ja palauttaa toiminta häiriön jälkeen sekä varautua tuleviin

häiriöihin. Tutkielman viitekehys kattaa nämä kaikki osa-alueet. Kaikkien muiden toimintojen kohdalla paitsi reagoi-toiminnossa todettiin, että kokonaisarkkitehtuurin artefaktin avulla pystyttiin tukea häiriöiden hallintaa. Näin ollen voidaan siis todeta, että kokonaisarkkitehtuurilla voidaan vastata NIS2-direktiivin vaatimuksista myös tähän.

Kolmas osa-alue oli häiriöiden raportoinnin tiukentunut aikaraja. NIS2-direktiivi vaatii, että ensimmäinen alustava ilmoitus häiriöstä tehdään viimeistään 24 tuntia häiriön huomaamisesta ja kattavampi varsinainen häiriöilmoitus 72 tunnin sisällä. Lopullinen raportti häiriöstä tulee toimittaa kuukauden sisällä varsinaisesta häiriöilmoituksesta. Viitekehys ei suoraan määrittele, kuinka nopeasti eri toiminnot tulee suorittaa. Sen kuitenkin muodostaa selkeät toiminnot häiriöiden hallintaan ja määrittää, mihin kokonaisarkkitehtuurin artefaktiin tulisi nojautua toiminnon suorittamisessa. Viitekehyksessä on määritelty, miten häiriön tunnistaminen tulisi toteuttaa ja mikä kokonaisarkkitehtuurin artefakti auttaa siinä. Kun häiriö ja sen vaikutuksen alla olevat osa-alueet pystytään tunnistamaan ajoissa, voidaan todennäköisemmin tehdä ilmoitus mahdollisimman nopeasti. Vaikka suoraa aikamäärettä viitekehyksen toiminnoille ei ole, selkeyttää ja johdonmukaistaa viitekehys häiriötilanteissa toimimista, mikä voi merkittävästi helpottaa aikataulussa pysymistä. Kokonaisarkkitehtuurin yhdistäminen häiriöiden hallintaan voi siis auttaa NIS2-direktiivin aikarajavaatimusten täyttämisessä.

Neljäs osa-alue oli riskienhallinta. NIS2-direktiivissä riskienhallinnan tulisi sisältää kyberturvallisuusriskien varautumisen ja hallitsemisen, säännöllisten viranomaistarkastusten suorittamisen sekä verkko- ja tietojärjestelmien ajantasaisuuden varmistamisen. Tutkielman viitekehyksessä tunnista-toimintoon kytkeytyvät teknologian viitemallit tarjoavat arvokasta tietoa mahdollisista haavoittuvuuksista, mikä voi auttaa riskien järjestelmällisessä analysoinnissa ja kyberuhkien ennakoinnissa. Tätä voitaisiin soveltaa direktiivin mukaiseen riskienhallintaan. Lisäksi tutkielman viitekehyksessä suojaa-toiminto liittyy oleellisesti häiriöihin varautumiseen. Siihen liittyvä tiekartat-artefakti auttaa hahmottamaan häiriöiden osalta niihin liittyviä riskejä ja niiden vaikutuksia organisaatiossa. Tiekarttoja voitaisiin yhtä lailla hyödyntää riskienhallinnassa kyberturvallisuusriskien arvioinnissa, ennakoinnissa ja lievittämisessä. Ohjeistukset-artefakti on toinen suojaa-toimintoon liittyvä kokonaisarkkitehtuurin artefakti, jonka avulla voidaan hallita tunnistettuja riskejä käytännön suojatoimin. NIS2-direktiivin mukaisessa riskienhallinnassa vastaavaa voitaisiin toteuttaa kokonaisarkkitehtuurin ohjeistukset-artefaktilla. Säännöllisillä viranomaistarkastuksilla halutaan varmistaa se, että direktiivin vaatimuksia noudatetaan ja riskienhallinnan taso pysyy tarpeeksi korkealla. Tarkastuksia varten tutkielman viitekehyksessä tunnistetuilla kokonaisarkkitehtuurin artefakteilla pystyttäisiin seuraamaan organisaation ja sen

järjestelmien tilaa paremmin ja siten tunnistamaan mahdollisia riskejä. Tämä voisi merkittävästi auttaa tarkastuksiin varautumisessa ja vaatimusten täyttämisessä. Aiemmin mainituilla tiekartoilla voitaisiin lisäksi seurata verkko- ja tietojärjestelmiä ja varmistaa niiden ajantasaisuus. Kokonaisarkkitehtuurin avulla voitaisiin siis vastata myös NIS2-direktiivin riskienhallintaa koskeviin vaatimuksiin.

Viides osa-alue on jatkuvuudenhallinta. Sen tarkoituksena on tunnistaa mahdolliset organisaatiota kohtaavat uhat ja selvittää kyseisen uhan vaikutukset. Tämän lisäksi jatkuvuudenhallinnan tarkoituksena on vahvistaa organisaation sietokykyä ja parantaa reagointikykyä. (Herbane ym., 2004.) Häiriöiden hallinta lukeutuu jatkuvuudenhallintaan, mutta jatkuvuudenhallinta koostuu lisäksi muista toimista, joilla pyritään varmistamaan organisaation toiminnan jatkuvuus erilaisten uhkien kohdatessa. Aiemmassa kappaleessa nostettiin riskienhallinnan osalta esille, miten tutkielman viitekehyksessä tunnista-toimintoon kytkeytyvät teknologian viitemallit ja suojaa-toimintoon liitetyt tiekartat auttavat riskien analysoinnissa ja kyberuhkien tunnistamisessa. Kuten riskienhallinnassa tätä voitaisiin soveltaa myös jatkuvuudenhallinnassa mahdollisten uhkien ja niiden vaikutusten kartoittamisessa. Tutkielman viitekehyksen tarkoituksena on tukea häiriöiden hallintaa, mikä tarkoittaa myös organisaation sietokyvyn kasvattamista häiriöiden varalle. Mikäli tutkielmassa tunnistettuja kokonaisarkkitehtuurin artefakteja hyödynnettäisiin laajemmin jatkuvuudenhallinnassa, voitaisiin niiden avulla vahvistaa myös tämän osa-alueen vaatimaa sietokykyä. Tutkielman viitekehyksen tarkastelussa todettiin, ettei valitulla kokonaisarkkitehtuurin artefaktilla pystytty toteamaan merkittävää vaikutusta reagoi-toiminnon osalta häiriöiden hallinnassa. Näin ollen kokonaisarkkitehtuuri ei välttämättä parantaisi jatkuvuudenhallintaan liittyvää reagointikykyä. Näiden osa-alueiden tarkastelulla todettiin, että kokonaisarkkitehtuurilla voitaisiin osittain vastata NIS2-direktiivin vaatimuksiin jatkuvuudenhallinnasta.

Kuudes osa-alue on ”kyberhygienia” ja kouluttaminen. NIS2-direktiivin osalta tämä tarkoittaa, että organisaation sisällä otetaan käyttöön selkeät käytännöt, jotka tukevat turvallista kyberkäyttäytymistä sekä koulutetaan henkilökuntaa kyberturvallisuudesta. Tutkielman viitekehyksessä on nostettu esille selkeiden periaatteiden ja ohjeistusten muodostaminen, joilla tavoitellaan yhteistä tapaa toimia häiriötilanteissa sekä selkeää yhteistä linjaa koko häiriöiden hallintaprosessiin. Yhtäläisyyksiä löytyy NIS2-direktiivin tämän osa-alueen vaatimusten ja tutkielman viitekehyksessä laadittujen toimenpiteiden väliltä, mutta ei voida todeta, että kokonaisarkkitehtuuri merkittävästi vaikuttaisi tähän. Huolehtiakseen ”kyberhygieniasta” ja henkilöstön kouluttamisesta organisaation on todennäköisimmin otettava käyttöön erillisiä materiaaleja ja koulutuksia tätä tarkoitusta varten.

Viitekehys pystyi vastaamaan neljään kuudesta NIS2-direktiivin päävaatimuksesta ja osittain viidenteen eli jatkuvuuden hallintaan. Näin ollen voidaan todeta, että tutkielman viitekehyksen ja kokonaisarkkitehtuurin avulla voidaan monilta osin vastata NIS2-direktiivin vaatimuksiin. Vaatimuksista täyttyivät vastuu toimitusketjuista, häiriöiden hallinnan vahvistaminen, häiriöiden raportoinnin tiukentuneet aikarajat ja riskienhallinta. Lisäksi tutkimuksessa havaittiin, että tutkielman viitekehyksessä tunnistetuilla kokonaisarkkitehtuurin artefakteilla pystyttiin vastaamaan osittain jatkuvuudenhallintaan liittyviin vaatimuksiin. Tutkimuksen perusteella voidaan todeta, ettei kokonaisarkkitehtuurin avulla pystytty vastaamaan NIS2-direktiivin vaatimuksiin ”kyberhygieniasta” ja kouluttamisesta.

8 Johtopäätökset

Tässä luvussa käydään läpi tutkielman johtopäätökset ja tarkastellaan tutkimuksen keskeisiä löydöksiä. Luvussa peilataan tutkimuksen tuloksia kirjallisuuteen ja käytetään tutkimuksessa tehtyjä johtopäätöksiä apuna vastaamisessa tutkimuskysymyksiin. Tämän jälkeen on koottu käytännön toimenpidesuosituksia tutkimuksen toimeksiantajalle. Toimenpidesuositusten tarkoituksena on käsitellä toimeksiantajan kokonaisarkkitehtuuria sekä häiriöiden raportointiprosessia ja tarjota näkemyksiä niiden kehittämiseen tutkimustulosten pohjalta. Lisäksi pohditaan NIS2-direktiivin vaatimusten täyttämistä toimeksiantajaorganisaation osalta. Viimeisenä käydään läpi tutkimuksen rajoitukset ja annetaan ehdotuksia jatkotutkimukselle.

8.1 Vastaukset tutkimuskysymyksiin

Tutkimuksen tavoitteena oli selvittää, miten kokonaisarkkitehtuuri voisi tukea häiriöiden hallintaa ja millaisia hyötyjä kokonaisarkkitehtuurin käytöstä voisi organisaatiolle olla. Tutkielmassa keskityttiin selvittämään kokonaisarkkitehtuurin hyödynnettävyyttä häiriötilanteiden hallinnan työkaluna normaalioloissa. Tutkittavan aiheen myötä haluttiin saada vastauksia siihen, voiko kokonaisarkkitehtuuri auttaa häiriötilanteiden hallinnassa ja millaisia konkreettisia hyötyjä sen käytöstä voisi olla. Häiriöiden hallinnan merkitys tiedonhallinnan, järjestelmien hallinnan, tietoturvan ja liiketoimintaprosessien osalta kasvaa organisaatioissa jatkuvasti kehittyvien uhkien ja riskien myötä, minkä vuoksi sen suunnitteluun, toteuttamiseen, arviointiin ja tehostamiseen tarvitaan jatkuvasti kehittyviä ratkaisuja. Kokonaisarkkitehtuuri tarjoaa organisaatioille menetelmän, jonka avulla niiden toiminta voidaan mallintaa siten, että eri osa-alueiden väliset yhteydet hahmottuvat selkeästi ja toiminnan kehittäminen on mahdollista jatkuvasti ylläpidettävänä ja nykytilaa mahdollisimman hyvin kuvaavana kokonaisuutena. Kokonaisarkkitehtuuria kuitenkin kritisoidaan usein sen työläydestä, eikä sen koeta tuottavan tarpeeksi konkreettista hyötyä suhteessa työmäärään. Tutkielmassa halutaan tarkastella kokonaisarkkitehtuurin hyödynnettävyyttä häiriöiden hallinnan näkökulmasta, sillä kasvavat häiriöiden määrät ja merkittävä tarve niiden hallinnalle on tällä hetkellä esillä monissa organisaatioissa. Kokonaisarkkitehtuurin ja häiriöiden hallinnan rinnalla tutkielmassa käsiteltiin NIS2-direktiivin vaatimuksia ja velvoitteita, joiden noudattamista erittäin kriittisten ja kriittisten sektorien toimijoiden on alettava toteuttaa. Tutkielmassa haluttiin selvittää, miten kokonaisarkkitehtuurin yhdistäminen häiriöiden hallintaan voisi tukea myös NIS2-direktiivin vaatimusten täyttämistä organisaatioissa.

Tutkimuskysymykset, joihin haettiin vastaus, olivat:

1. *Miten kokonaisarkkitehtuuri tukee häiriöiden hallintaa organisaatioissa?*
2. *Voidaanko kokonaisarkkitehtuurin avulla vastata NIS2-direktiivin asettamiin vaatimuksiin?*

Aiemman tutkimuskirjallisuuden läpi käynti osoitti selkeän tutkimusaukon kokonaisarkkitehtuurin ja häiriöiden hallinnan välisen yhteyden tarkastelun osalta. Tutkielman aihetta vastaavaa aiempaa tutkimusta on löydettävissä vain vähän. Eniten samankaltaisuuksia tämän tutkielman kanssa oli Al-Turkistani ym. (2021) tutkimuksessa, jossa vertailtiin eri kokonaisarkkitehtuurin viitekehyksiä ja miten ne toteuttavat kyberturvallisuusvaatimuksia. Kokonaisarkkitehtuuria on käsitelty lähinnä riskienhallinnan (Barateiro ym., 2012), kriisinhallinnan (Breithaupt ym., 2021) ja tietoturvan (Diefenbach ym., 2019) yhteydessä, jotka sivuavat häiriöiden hallintaa, mutta eivät keskity siihen suoraan. Euroopan unionin NIS2-direktiivi astui voimaan joulukuussa 2022. Direktiiviä koskevaa tutkimusta on toistaiseksi vähän, mutta aiheeseen liittyvä keskustelu on jatkuvassa kasvussa (Ruohonen, 2024).

Tutkimuksen viitekehys rakennettiin Kotusevin (2017) kahdeksasta kokonaisarkkitehtuurin artefaktista ja NIST Kyberturvallisuusviitekehyksestä (2024). Tavoitteena oli luoda viitekehys, jossa yhdistyisivät kokonaisarkkitehtuuri ja häiriöiden hallintaprosessi. Tutkimus toteutettiin laadullisena tutkimuksena, jossa yhdistettiin suunnittelutieteellinen tutkimusmenetelmä ja tapaustutkimus. Tapaustutkimus toteutettiin toimeksiantajaorganisaation häiriöiden raportointijärjestelmää ja kokonaisarkkitehtuuria tutkimalla. Tämän avulla pyrittiin löytämään vastauksia ensimmäiseen tutkimuskysymykseen. Suunnittelutieteellisen tutkimusmenetelmän toteuttamisessa hyödynnettiin Peffersin ym. (2007) laajasti käytettyä viitekehystä, jossa Design Science -prosessi toteutetaan kuudessa vaiheessa: tunnista ongelma ja perustele merkitys, määrittele ratkaisun tavoitteet, suunnittelu ja kehittäminen, demonstrointi, arviointi sekä viestintä. Suunnittelutieteellisessä tutkimusmenetelmässä kehitetään artefakti, jonka toimivuutta arvioidaan. Tässä tutkielmassa artefakti oli tutkielman viitekehys ja sen arviointiin käytettiin NIS2-direktiivin vaatimuksia. Näin pyrittiin vastaamaan myös toiseen tutkimuskysymykseen.

Tutkimuksen data sisälsi kokonaisarkkitehtuurin mallinnuksia ja häiriöraportteja, jotka saatiin toimeksiantajaorganisaatiolta käyttöön tutkielman kirjoittamisen ajaksi. Toimeksiantajaorganisaatio on mallintanut kokonaisarkkitehtuuriaan pääasiassa tätä tarkoitusta varten hankitulla ohjelmalla. Tämän lisäksi häiriöiden raportointiin käytetyssä järjestelmässä oli häiriöraporttien lisäksi kokonaisarkkitehtuuriin liittyviä järjestelmälistauksia ja integraatioita. Tutkimusta varten häiriöiden

raportointijärjestelmästä valittiin kaksi häiriötä, joita tutkittiin tarkemmin tutkielman viitekehyksen avulla. Tämän rinnalla käytiin systemaattisesti läpi, mitä kokonaisarkkitehtuurin artefakteja toimeksiantajan mallinnuksista löytyi keskittyen tutkielman viitekehyksessä käytettyihin Kotusevin (2017) kahdeksaan artefaktiin.

Ensimmäisen tutkimuskysymyksen osalta tunnistettiin seitsemän tapaa, joilla kokonaisarkkitehtuuri tukee häiriöiden hallintaa. Tunnistettuja tapoja olivat häiriöiden hallintaprosessin yhtenäistäminen, häiriöiden laajuuden selvittäminen organisaation rakenneosissa, häiriöiden hallintaprosessin selkeyttäminen ja systemaattinen toteutus, häiriöiltä suojautuminen ja ennakointi, häiriöiden analysointi ja syiden tunnistaminen, häiriöiden vaikutusten laajuuden selvitys sekä häiriöiden jälkeisen palautumisprosessin tukeminen.

Vastauksena toiseen tutkimuskysymykseen todettiin, että kokonaisarkkitehtuurilla pystytään vastaamaan neljään kuudesta tunnistetusta NIS2-direktiivin vaatimuksesta. Täyttyneet vaatimukset olivat vastuu toimitusketjuista, häiriöiden hallinnan vahvistaminen, häiriöiden raportoinnin aikaraja ja riskienhallinta. Lisäksi vaatimuksista pystyttiin vastaamaan osittain viidenteen eli jatkuvuuden hallintaan. Kokonaisarkkitehtuurin avulla ei pystytty vastaamaan kuudenteen vaatimukseen eli ”kyberhygieniaan” ja kouluttamiseen. Seuraavassa alaluvussa tutkimuskysymyksiin saadut vastaukset tarkastellaan tarkemmin vertaamalla tuloksia aiempaan tutkimukseen.

8.2 Tuloksien tarkastelu suhteessa aikaisempaan tutkimukseen

Tässä luvussa keskitytään tarkastelemaan tämän tutkielman tuloksia suhteessa aikaisempaan tutkimukseen. Erityisesti nostetaan esille tulokset, jotka tukivat aikaisempaa tutkimusta, tulokset, jotka poikkesivat odotuksista, sekä täysin uudet löydökset. Tutkimuksen tulokset on esitelty tarkemmin luvussa seitsemän.

Häiriön hallinnan tukeminen

Kokonaisarkkitehtuurin tarkoituksena on muodostaa yhtenäinen kokonaisuus, joka tukee organisaation eri toimintojen ja rakenneosien välisen yhteyden tunnistamista. Häiriöiden hallinnassa kokonaisarkkitehtuurin avulla häiriöitä pystytään käsittelemään suhteessa muuhun toimintaan organisaatiossa eikä vain irrallisena osana sitä. Barateiro ym. (2012) totesivat saman tutkimuksessaan kokonaisarkkitehtuurin ja riskienhallinnan välisestä yhteydestä. Kokonaisarkkitehtuurin avulla riskienhallinnassa pystyttäisiin paremmin tunnistamaan, miten riskit leviävät ja vaikuttavat organisaatiossa. Tämän tutkielman tuloksissa tunnistettiin vastaavanlainen yhteys kokonaisarkkitehtuurin ja häiriöiden hallinnan välillä. Kokonaisarkkitehtuuri pystyy

tukemaan häiriöiden hallintaprosessissa häiriön ja sen vaikutusten laajuuden hahmottamista, mikä puolestaan helpottaa ja tehostaa korjaavien toimenpiteiden määrittelyä. Organisaation sisäinen häiriöiden hallinta on tärkeää myös asiakkaiden ja muiden sidosryhmien kannalta, sillä omassa organisaatiossa tapahtuvat häiriöt voivat heijastua muihin sidosryhmiin. Kokonaisarkkitehtuuri tukee häiriöiden hallintaa myös tästä näkökulmasta, koska sen avulla voidaan seurata ja tunnistaa, miten häiriöiden vaikutukset leviävät organisaation rajojen ulkopuolelle.

Diefenbach ym.(2019) kävivät läpi tutkimuksessaan 46 julkaisua, jossa tutkittiin, miten kokonaisarkkitehtuurin hallinta voisi tukea riskienhallintaa ja tietoturvanhallintaa. Selkeä linja julkaisuissa oli se, että kokonaisarkkitehtuurin tuoma lisäarvo liittyi sen tarjoamaan tietoon organisaation rakenteen ja IT-järjestelmien yhteydestä. Tämä tunnistettiin myös tässä tutkimuksessa kokonaisarkkitehtuurin ja häiriöiden hallinnan osalta. Kokonaisarkkitehtuurin avulla pystytään paremmin analysoimaan häiriöitä ja niiden liiketoimintavaikutuksia organisaatiossa, kun tunnistetaan, miten eri osa-alueet, kuten järjestelmät, prosessit ja palvelut sitoutuvat toisiinsa.

Tuloksissa tunnistettiin, että kokonaisarkkitehtuurilla oli positiivinen vaikutus häiriöiden tunnistamisessa, suojautumisessa ja ennakoinnissa. Bemthuis ym. (2020) nostivat esille tutkimuksessaan, miten tärkeää organisaation häiriönsietokyvyn kannalta olisi, että kokonaisarkkitehtuuri suunniteltaisiin parantamaan häiriöiden varhaista tunnistamista ja tehokkaampaa hallintaa. Nämä ovat tärkeässä osassa häiriöiden hallintaprosessissa ja vaikuttavat merkittävästi siihen, miten vahvasti häiriö tulee vaikuttamaan organisaatiossa ja sen keskeisissä sidosryhmissä. Kokonaisarkkitehtuuri pystyy lisäksi tukemaan häiriöistä palautumista. Tämä tunnistettiin myös Al-Turkistani ym. (2021) tutkimuksessa, missä palautumis- ja sietokyvyn tärkeys osana organisaation toimintaa nostettiin esille ja toteutuksen ratkaisuksi ehdotettiin turvallista ja sietokykyistä kokonaisarkkitehtuuriviitekehystä. Tämä oli tavoitteena tutkielman viitekehyksessä, jossa yhdistyivät häiriöiden hallinnan tärkeät osa-alueet sekä kokonaisarkkitehtuurin oleelliset artefaktit. Häiriöiden ja uhkien määrä tulee todennäköisesti lisääntymään tulevaisuudessa, mutta niiden vaikutuksia organisaatioon voidaan vähentää ja palautumista nopeuttaa selkeillä ja tarkoituksen mukaisilla kokonaisarkkitehtuurimallinnuksilla.

Tutkimuksessa havaittiin, että kokonaisarkkitehtuuri voi tukea häiriöiden hallintaprosessin yhtenäistämistä organisaation sisällä, mikä parantaisi prosessin tehokkuutta ja johdonmukaisuutta. Tätä näkökulmaa ei ole aiemmassa tutkimuksessa käsitelty. Kokonaisarkkitehtuurin artefakteista erityisesti periaatteet ja ohjeistukset voivat edistää prosessin yhdenmukaistamista ja luoda selkeät

linjaukset sen kaikille vaiheille. Tämä vähentäisi riskiä, että yksittäisiä häiriöitä käsiteltäisiin organisaatiossa toisistaan poikkeavin tavoin.

Tutkimuksessa tunnistettiin lisäksi, että kokonaisarkkitehtuurin avulla pystyttiin selkeyttämään häiriöiden hallintaprosessia ja tukemaan prosessin systemaattista toteutusta. Tämä ei noussut esille aikaisemmassa tutkimuksessa. Kokonaisarkkitehtuurin ylläpitäminen vaatii organisaatioilta resursseja ja voi olla ajoittain työlästä. Vaikka kokonaisarkkitehtuurin kuvaukset, taulukoinnit, yhteyskaaviot ja muut dokumentoinnit eivät olisi täydellisiä, on niistä silti hyötyä häiriöiden hallinnassa. Ne ohjaavat häiriöiden hallintaprosessia kokonaisvaltaisempaan tarkasteluun kuin mitä se olisi ilman kokonaisarkkitehtuurin mallinnuksia.

Tutkimuksessa ei tunnistettu tapoja, joilla kokonaisarkkitehtuuri selkeästi tukisi reagoi-toimintoa, jossa pyritään korjaamaan häiriö käytännön toimenpiteillä. Kokonaisarkkitehtuurin artefakteista ei löydetty sellaisia hyötyjä, jolla olisi merkittävästi tehostettu tai selkeytetty reagoi-toimintoon kuuluvia toimenpiteitä. Tulos ei vastannut odotuksia, sillä kokonaisarkkitehtuurin hyötyjä oli tunnistettu muissa toiminnoissa.

NIS2-direktiivin vaatimuksien mukaisuus

NIS2-direktiivin asettamat vaatimukset vaativat organisaatioilta systemaattista tapaa hallita kyberturvallisuuteen liittyviä riskejä. Kokonaisarkkitehtuurilla pystyttiin vastaamaan useaan vaatimukseen ja tukemaan direktiivin vaatimia toimenpiteitä organisaatiossa. Diefenbach ym. (2019) nostivat esille tutkimuksessaan tarpeen tutkia uusien tietoturvavaatimusten tuomia haasteita suhteessa kokonaisarkkitehtuuriin. Tähän perehdyttiin myös tässä tutkimuksessa tarkastelemalla, miten kokonaisarkkitehtuurin hyödyntäminen osana häiriöiden hallintaa voisi toimia samalla ratkaisuna NIS2-direktiivin vaatimusten täyttämisessä.

NIS2-direktiivin vaatimusten ja velvoitteiden täyttäminen on herättänyt paljon keskustelua organisaatioissa. Tutkimuksen viitekehys tarjoaa yhden ratkaisun organisaatioille, jolla vaatimuksien toteuttamista omassa toiminnassa voisi lähteä toteuttamaan. Tässä tutkimuksessa todettiin, että kokonaisarkkitehtuuri pystyi vastaamaan direktiivin vaatimuksista osa-alueisiin vastuu toimitusketjuista, häiriöiden hallinnan vahvistaminen, häiriöiden raportoinnin aikaraja ja riskienhallinta sekä osittain jatkuvuuden hallintaan. Kriisienhallinnan suhteen oli todettu, että kokonaisarkkitehtuurin hyödyt kiteytyvätkin siihen, miten siinä on entuudestaan huomioitu riskienhallinta, jatkuvuudenhallinta, IT-turvallisuus, liiketoimintaprosessien hallinta ja IT-strategia

(Breithaupt ym., 2021). Tämä tukee tässä tutkimuksessa tunnistettuja elementtejä, joilla kokonaisarkkitehtuuri tuki NIS2-direktiivin vaatimuksiin vastaamista.

On tärkeä korostaa, ettei kokonaisarkkitehtuuria ole tarkoitettu ainoastaan häiriöiden hallinnan tukemiseen tai NIS2-direktiivin vaatimusten täyttämiseen, vaan sen hyödyntämiseen liittyy lisäksi muita merkittäviä etuja, kuten päätöksenteon tukeminen, resurssien käytön tehostaminen ja muutoksenhallinnan edistäminen. Kehittämällä kokonaisarkkitehtuuria siten, että se tukee häiriöiden hallintaa ja vastaa kyberturvallisuusvaatimuksia, organisaatio voi luoda systemaattisen ja yhtenäisen toimintatavan koko organisaation tasolle. Näin vältetään useiden päällekkäisten ratkaisujen ylläpito ja tehostetaan toimintaa. NIS2-direktiivin vaatimukset eivät myöskään ole ainoat, joita organisaatioiden tulee miettiä toimintansa kehittämisessä vaan samanaikaisesti tulisi toteuttaa monia eri velvoitteita, kuten tässäkin tutkielmassa aikaisemmin esiteltyjen kybersolidaarisuussäädöksen ja CER-direktiivin osalta. Mikäli organisaatiolla on tarve toteuttaa tämä yhtälö, on kokonaisarkkitehtuurin käyttöönotto perusteltua.

8.3 Teoreettiset kontribuutiot

Tämän tutkimuksen myötä saadaan uusia teoreettisia kontribuutioita kokonaisarkkitehtuurin, häiriöiden hallinnan ja NIS2-direktiivin osalta. Kokonaisarkkitehtuurin ja häiriöiden hallinnan välisen yhteyden tarkastelu tuo lisää näkökulmia siihen, miten kokonaisarkkitehtuuria voidaan hyödyntää organisaatioissa sekä mitä keinoja organisaatioilla on häiriöiden hallintaan. Lisäksi NIS2-direktiivin vaatimusten tutkiminen suhteessa kokonaisarkkitehtuuriin ja häiriöiden hallintaan syventää ymmärrystä siitä, miten vaatimusten täyttämistä voitaisiin lähestyä organisaatioissa. Tutkimus lisää tietoa siitä, millä tavoilla ja mitä kokonaisarkkitehtuurin osa-alueita hyödyntämällä organisaatiot voivat tehostaa omaa häiriöiden hallintaprosessiaan.

Tutkimuksen viitekehys muodostettiin yhdistämällä Kotusevin (2017) kahdeksan kokonaisarkkitehtuurin artefaktia ja NIST kyberturvallisuusviitekehys (2024), jotta sen avulla voitiin tarkastella tutkielman tutkimuskysymyksiä. Tutkielman viitekehyksessä häiriöiden hallintaa tukeviin toimintoihin on yhdistetty kokonaisarkkitehtuurin artefaktit. Samalla syntyi tutkielman artefakti eli viitekehys, jonka tarkoituksena on auttaa häiriöiden hallinnan tehostamista kokonaisarkkitehtuurin avulla sekä vastata NIS2-direktiivin vaatimuksiin. Tutkimuksen avulla saatiin seitsemän tapaa, joilla kokonaisarkkitehtuuri tukee häiriöiden hallintaa ja pystyttiin vastaamaan neljään kuudesta NIS2-direktiivin vaatimuksista sekä osittain viidenteen. Tutkielman viitekehys tarjoaa uuden lähestymistavan häiriöiden hallinnan tukemiseen sekä välineen, jonka avulla organisaatiot voivat integroida NIS2-direktiivin vaatimuksia osaksi omaa toimintaansa.

Häiriöiden hallinnan voidaan katsoa olevan osa riskienhallintaa, kriisinhallintaa ja organisaation sietokykyä. Näistä osa-alueista on tehty enemmän tutkimusta kokonaisarkkitehtuurin kanssa (Al-Turkistani ym., 2021; Bemthuis ym., 2020; Diefenbach ym., 2019). Tämän tutkimuksen tulokset monelta osalta vahvistavat aiemmissa tutkimuksissa tunnistettuja kokonaisarkkitehtuurin hyötyjä ja tämän tutkimuksen tuloksia voidaan hyödyntää myös näiden osa-alueiden jatkotarkastelussa. Tutkimus täyttää osaltaan tutkielmassa tunnistettua tutkimusaukkoa tuomalla vastauksia kokonaisarkkitehtuurin ja häiriöiden hallinnan välisen yhteyden tarkasteluun.

8.4 Käytännön toimenpidesuositukset

Tutkimuksen perusteella organisaatiossa on tarve luoda yhteiset periaatteet ja ohjeistukset häiriöiden hallinnalle. Tämä auttaa organisaation häiriöiden hallintaprosessin yhdenmukaistamisessa ja ohjaa henkilöstöä toimimaan sovittujen linjausten mukaisesti. Häiriöiden taustalla on usein inhimillinen virhe, minkä takia on tärkeää kouluttaa organisaation henkilöstöä ja keskeisiä sidosryhmiä häiriöiden hallinnasta, yleisistä riskeistä ja turvallisista tavoista toimia. Kouluttamisen tulisi olla jatkuvaa ja sisältää päivittäisen toiminnan tueksi tarkoitettuja ohjeistuksia. Lisäksi häiriöiden hallintaan liittyvistä aiheista tulisi viestiä organisaation sisällä ja ulkopuolisille tahoille mahdollisimman aktiivisesti, jotta organisaation toimintaan vaikuttavien henkilöiden tietotaito pysyy ajantasaisena. Mitä useampi organisaation jäsen ymmärtää häiriöiden hallintaprosessin pääelementit, sitä paremmin pystytään häiriöitä ennakoimaan ja tunnistamaan. Oman roolin, vastuualueen ja yhdessä sovittujen toimenpiteiden tuntemus parantavat ja nopeuttavat kykyä reagoida häiriöihin, minkä seurauksena häiriön kestoa voidaan lyhentää ja vaikutuksia vähentää. Tällä on merkittävät vaikutukset koko organisaation häiriöiden hallintaan.

Häiriöiden hallintaan liittyvien periaatteiden suunnittelussa ja kehittämisessä on varmistettava, että ne ovat linjassa organisaation muiden periaatteiden, linjausten ja toimintapolitiikkojen kanssa. Useamman eri periaatteen ylläpito on aikaa vievää ja eri periaatteiden ristiriitaisuus voi johtaa epäjohdonmukaisuuteen muissa toiminnoissa, jolloin systemaattinen ja tehokas häiriöiden hallinta vaikeutuu. Organisaation tulisi siksi luoda mekanismi, jolla häiriöiden hallinnan ja tietoturvan periaatteet tarkistetaan suhteessa muihin ylätason linjauksiin ennen niiden käyttöönottoa, jotta vältetään päällekkäisyydet ja ristiriidat.

Kokonaisarkkitehtuuri ja usein myös häiriöiden hallinta mielletään yhä ensisijaisesti tietohallinnon ja järjestelmävastaavien vastuulle kuuluviksi tehtäviksi. Häiriötilanteissa tämä rajautuminen voi kuitenkin muodostua haasteeksi: aikaa kuluu helposti siihen, että eri organisaation osapuolet eivät käytä samoja käsitteitä tai tunne ICT-alan termejä. Tämä saattaa hidastaa viestintää, päätöksentekoa

ja toimenpiteiden käynnistämistä kriittisissä tilanteissa. Erityisen tärkeää olisi, että organisaation johto ymmärtäisi kokonaisarkkitehtuurin hyödyt häiriöiden hallinnan ja muiden toimintojen osalta. Johdon parempi ymmärrys mahdollistaisi tehokkaamman päätöksenteon, riskienhallinnan ja toiminnan ohjaamisen silloin, kun häiriötilanteet vaativat korkeampaa päätöksentekotason panosta. Tämän saavuttamiseksi voidaan harkita, pitäisikö kokonaisarkkitehtuuria ja sen dokumentointia yksinkertaistaa ja kehittää siten, että entistä helpommin eri toimintojen vastuuhenkilöt pystyisivät sitä hyödyntämään.

Tutkimuksessa havaittiin, että toisen tarkastellun häiriön dokumentaation perusteella häiriön selvittäminen ja perusteellinen ratkaiseminen olivat jääneet vaiheeseen. Häiriöiden hallintaprosessia voitaisiin kehittää erityisesti perusteellisen juurisyiden analyysin ja ratkaisujen osalta. Vaikka tämä vaatii ajoittain lisäresursseja yksittäisten häiriöiden käsittelyyn, se on pitkällä aikavälillä organisaation toiminnan kannalta merkittävää: huolellinen analyysi ja ratkaisu vähentävät samanlaisten häiriöiden toistumisen riskiä ja tukevat toiminnan jatkuvaa parantamista.

Vaikka tutkimukseen liittyvän tarkastelun myötä löytyi kehitettävää kokonaisarkkitehtuurissa, niin saadaan siitä silti hyötyä häiriöiden hallintaan. Jopa ulkopuolinen henkilö tutkimustilanteessa pystyy järjestelmiin tehtyjen mallinnusten ja ylläpidetyn tiedon avulla hahmottamaan organisaation kokonaisuutta ja järjestelmien välisiä yhteyksiä, vaikka aikaisempaa tuntemusta organisaation toiminnasta ei olisi. Laajasti mallinnettu kokonaisarkkitehtuuri avaa organisaation toimintaa ja helpottaa eri toimintojen välisten yhteyksien ja vastuiden hahmottamista sekä helpottaa tilanteen määrittelyä häiriötilanteessa. Toimeksiantajaorganisaation kannattaa siis tulevaisuudessakin jatkaa kokonaisarkkitehtuurityötään ja jatkokehittää sitä sopivaksi myös uusiin tarpeisiin, kuten häiriön hallinnalle ja NIS2-direktiivin vaatimuksiin.

8.5 Rajoitukset

Tutkimuksen rajoitteet edellyttävät monipuolista tarkastelua. Tutkimuksessa tutkittiin vain kahta häiriötä yhdessä organisaatiossa, mikä vaikuttaa tulosten yleistettävyyteen. Jotta häiriöiden hallinnan ja kokonaisarkkitehtuurin yhteydestä olisi saatu tuloksia laajemmassa kontekstissa, olisi tutkimuksessa pitänyt olla mukana useampi ja mahdollisimman erilaisia häiriöitä. Näin olisi tutkimustuloksista saatu monipuolisempia. Lisäksi useamman organisaation häiriöiden tutkiminen voisi tuoda esille organisaatioiden tai toimialojen välisiä eroja häiriöiden hallinnassa. Rajoitukset siis tutkittujen häiriöiden määrässä ja organisaatiossa tarkoittavat sitä, että tuloksissa voi heijastua niihin liittyviä ominaispiirteitä.

Kokonaisarkkitehtuuri rakennetaan organisaation prosessien ja tarpeiden mukaisesti, mikä voi rajoittaa tämän tutkimuksen tulosten yleistettävyyttä kokonaisarkkitehtuurin osalta. Tutkielmassa on keskitytty Kotusevin (2017) kahdeksaan kokonaisarkkitehtuurin artefaktiin, jotka ovat yleisesti kokonaisarkkitehtuureissa käytössä. Organisaatioissa samankaltaiset artefaktit voivat kuitenkin sisältää erilaista tietoa, jolloin niiden hyödynnettävyys häiriöiden hallinnassa ei välttämättä vastaa tässä tutkielmassa tunnistettuja tapoja.

On tärkeää huomioida, että NIS2-direktiivin vaatimukset koskevat ainoastaan kriittisiksi sektoreiksi luokiteltuja toimialoja. Tässä tutkimuksessa kokonaisarkkitehtuurin hyötyjä häiriöiden hallinnassa sekä tutkielman viitekehyksen toimivuutta on arvioitu sen perusteella, kuinka hyvin niiden avulla voidaan samalla vastata direktiivin asettamiin vaatimuksiin. Mikäli direktiivin vaatimukset eivät koske organisaatiota, arviointi ei välttämättä tunnu yhtä relevantilta. On kuitenkin syytä korostaa, että vaikka NIS2-direktiivi ei ole kaikille toimijoille velvoittava, se tarjoaa hyödyllisen viitekehyksen organisaation oman toiminnan ja turvallisuuden kehittämiseen.

Yksi vaikuttava tekijä johtopäätösten pysyvyydelle on NIS2-direktiivin osalta sen ajankohtaisuus ja EU:n direktiivien jatkuva kehitys. Häiriöiden hallinnassa johtopäätösten pysyvyyteen voivat vaikuttaa nopeasti kehittyvät ja muuttuvat uhat ja riskit. Tulevaisuudessa vaikuttavia häiriöitä ei pystytä vielä tunnistamaan ja niiden vaatimat toimintatavat voivat erota tämänhetkisistä merkittävästi. Nämä ulkoiset tekijät voivat vaikuttaa tämän tutkimuksen tulosten sovellettavuuteen tulevaisuudessa.

8.6 Jatkotutkimusehdotukset

Tulevaisuudessa kokonaisarkkitehtuurin ja häiriöiden hallintaa tutkittaessa olisi hyödyllistä toteuttaa laajempia tutkimuksia, jossa voitaisiin vertailla tuloksia useamman häiriön ja erilaisten organisaatioiden välillä. Näin saataisiin monipuolisempi käsitys häiriöiden hallinnan ja kokonaisarkkitehtuurin välisestä yhteydestä ja voitaisiin löytää uusia tapoja hyödyntää kokonaisarkkitehtuuria erilaisilla toimialoilla. Jatkotutkimuksessa voitaisiin lisäksi syventyä tutkimaan vain tietyn tyyppisiä häiriöitä, kuten liiketoimintaa vakavammin haitanneet häiriöt tai häiriöt, joiden korjaaminen on ollut erityisen vaikeaa.

Tässä tutkimuksessa keskityttiin selvittämään, voiko kokonaisarkkitehtuurilla ylipäätään tukea häiriöiden hallintaa ja miten. Jatkotutkimuksessa olisi hyödyllistä tutkia tarkemmin tapoja, joilla organisaatiot voisivat toteuttaa kokonaisarkkitehtuurin ja häiriöiden hallintaprosessin yhdistämistä mahdollisimman tehokkaasti ja järjestelmällisesti. Lisäksi tutkimus voisi keskittyä siihen, miten

häiriöiden hallinnan tarpeet voitaisiin huomioida mahdollisimman aikaisessa vaiheessa osana kokonaisarkkitehtuurin kehittämistä.

Tässä tutkielmassa luotiin uusi viitekehys, jossa yhdistettiin Kotusevin (2017) kahdeksan kokonaisarkkitehtuurin artefaktia ja NIST-kyberturvallisuusviitekehys (2024). Tarkoituksena oli luoda tutkimuksen tarpeisiin sopiva viitekehys, jolla voitaisiin selvittää kokonaisarkkitehtuurin ja häiriöiden hallinnan välistä yhteyttä. Tulevaisuudessa voitaisiin tutkia, miten tutkielman viitekehystä voitaisiin jatkokehittää, syventää ja soveltaa laajempaan käyttöön. Tätä voitaisiin tutkia selvittämällä, miten tutkielman viitekehystä tai vastaavaan tarkoitukseen luotua viitekehystä voitaisiin hyödyntää ulkoisissa auditoinneissa, jotka keskittyvät häiriöiden hallinnan arviointiin.

Jatkotutkimuksessa voitaisiin tutkia aihetta ottaen huomioon vielä laajemmin muita häiriöiden hallintaan kohdistuvia vaatimuksia. NIS2-direktiivi ei ole ainoa direktiivi, jonka vaatimuksia monien organisaatioiden pitää tulevaisuudessa toteuttaa, minkä takia muiden direktiivien tai ohjeistusten huomioiminen osana tutkimusta voisi olla hyödyllistä. Mikäli tulevaisuudessa häiriöiden hallintaan kohdistuu uudenlaisia vaatimuksia tai organisaatioiden kohtaamissa häiriötyypeissä tapahtuu merkittävä muutos, on syytä tehdä jatkotutkimusta, joka huomioi nämä muutokset.

NIS2-direktiiviä ei ole tutkittu tällä hetkellä vielä kovin laajasti, minkä vuoksi siihen kohdistuva jatkotutkimus on varmasti tarpeellista. Siihen keskittyvä jatkotutkimus voisi perehtyä direktiivin vaatimusten toteuttamiseen eri toimialoilla tai eri kokoisissa organisaatioissa. Vaatimusten toteuttamiseen kaivataan vastauksia ja uusien ratkaisujen tutkiminen voisi olla hyödyllistä monille organisaatioille.

Lähteet

Abraham, R. (2013). Enterprise Architecture Artifacts As Boundary Objects—A Framework Of Properties. *ECIS 2013 Completed Research*. https://aisel.aisnet.org/ecis2013_cr/120

Ahlemann, F., Stettiner, E., Messerschmidt, M., & Legner, C. (2012). *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments*. Springer Science & Business Media.

Aldea, A., Vaicekauskaitė, E., Daneva, M., & Sebastian Piest, J. P. (2020). Assessing Resilience in Enterprise Architecture: A Systematic Review. *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)*, 1–10. https://doi.org/10.1109/EDOC49727.2020.00011

Alonso, I. A., Verdún, J. C., & Caro, E. T. (2010). Review and Analysis of Enterprise Architecture Models and Focus IT Architecture. *Revista de Procesos y Métricas de Las Tecnologías de La Información*, *7*(3), 15–27.

Alshammari, B. M. (2017). Enterprise architecture frameworks: A critique review from a security perspective. *International Journal of Computer Applications*, *174*(4).

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021). Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. *2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA)*, 79–84. https://doi.org/10.1109/CAIDA51941.2021.9425343

Anthopoulos, L. (2009). *APPLYING ENTERPRISE ARCHITECTURE FOR CRISIS MANAGEMENT–A CASE OF HELLENIC MINISTRY OF FOREIGN AFFAIRS*. Coherency Management: Architecting the Enterprise for Alignment, Agility and Assurance. AuthorHouse Publishing.

Armour, F. J., Kaisler, S. H., & Liu, S. Y. (1999). A big-picture look at enterprise architectures. *IT Professional*, *1*(1), 35–42. https://doi.org/10.1109/6294.774792

Arter Oy. (ei pvm.). *Kokonaisarkkitehtuuri-kategoria—Materiaalipankki*. Arter. Noudettu 21. helmikuuta 2025, osoitteesta https://www.arter.fi/resource/kokonaisarkkitehtuuri/

Asetus (EU) 2019/881. (2019, huhtikuuta 17). *Asetus—2019/881—FI - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2019/881/oj/fin

Asetus (EU) 2022/2554 (2022). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

Asetus (EU) 2024/2847 (2024). https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

Asetus (EU) 2025/38. (2024, joulukuuta 19). *Regulation—EU - 2025/38—EN - EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

Asikainen, M. (2024, tammikuuta 9). NIS2-direktiivi ja laki kyberturvallisuuden riskienhallinnasta – mistä on kyse? *Gofore*. https://gofore.com/nis2-direktiivi-ja-laki-kyberturvallisuuden-riskienhallinnasta-mista-onkaan-kyse/

Barateiro, J., Antunes, G., & Borbinha, J. (2012). Manage Risks through the Enterprise Architecture. *2012 45th Hawaii International Conference on System Sciences*, 3297–3306. https://doi.org/10.1109/HICSS.2012.419

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber Security Policy Guidebook*. John Wiley & Sons.

Bemthuis, R., Iacob, M.-E., & Havinga, P. (2020). A Design of the Resilient Enterprise: A Reference Architecture for Emergent Behaviors Control. *Sensors*, *20*(22), 6672. https://doi.org/10.3390/s20226672

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Bernard, S. A. (2012). *An Introduction to Enterprise Architecture: Third Edition*. AuthorHouse.

Bernard, S. A. (2020). *An Introduction to Holistic Enterprise Architecture: Fourth Edition*. AuthorHouse.

Betz, C. (2024, kesäkuuta 24). Enterprise Architecture: From Design-Driven To Data-Driven. *Forrester*. https://www.forrester.com/blogs/enterprise-architecture-from-design-driven-to-data-driven/

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices.* USF Tampa Bay Open Access Textbooks, Tampa, FL.

Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: New challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, *3*(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

Bizzdesign. (2024). *The State of Enterprise Architecture in 2024 Report*. https://content.bizzdesign.com/lp-state-of-enterprise-architecture-2024

Bossert, O. (2016). A Two-Speed Architecture for the Digital Enterprise. Teoksessa E. El-Sheikh, A. Zimmermann, & L. C. Jain (Toim.), *Emerging Trends in the Evolution of Service-Oriented and Enterprise Architectures* (ss. 139–150). Springer International Publishing. https://doi.org/10.1007/978-3-319-40564-3_8

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Breithaupt, C., Vieracker, J., Chircu, A., Cox, S., & Sultanow, E. (2021). *The Enterprise Architect as a Crisis Manager*. 133–148. https://dl.gi.de/handle/20.500.12116/34720

Buchanan, S., & Gibb, F. (1998). The information audit: An integrated strategic approach. *International Journal of Information Management*, *18*(1), 29–47. https://doi.org/10.1016/S0268-4012(97)00038-8

Buckl, S., Ernst, A. M., Matthes, F., Ramacher, R., & Schweda, C. M. (2009). Using Enterprise Architecture Management Patterns to Complement TOGAF. *2009 IEEE International Enterprise Distributed Object Computing Conference*, 34–41. https://doi.org/10.1109/EDOC.2009.30

Bui, Q. N. (2017). Evaluating Enterprise Architecture Frameworks Using Essential Elements. *Communications of the Association for Information Systems*, *41*(1). https://doi.org/10.17705/1CAIS.04106

Bulletproof. (2022). *Download the Bulletproof 2022 Cyber Security Report*. Bulletproof.Co.Uk. https://www.bulletproof.co.uk/industry-reports/bulletproof-annual-cyber-security-report-2022

Bundy, J., Pfarrer, M. D., Short, C. E., & Coombs, W. T. (2017). Crises and Crisis Management: Integration, Interpretation, and Research Development. *Journal of Management*, *43*(6), 1661–1692. https://doi.org/10.1177/0149206316680030

Cameron, B. H., & McMillan, E. (2013). Analyzing the current trends in enterprise architecture frameworks. *Journal of Enterprise Architecture*, *9(1)*, 60–71.

Chiara, P. G. (2022). The IoT and the new EU cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, *36*(2), 118–137. https://doi.org/10.1080/13600869.2022.2060468

Corbin, J., & Strauss, A. (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications.

Daugulis, A. (2023). Critical Infrastructure Perspective on Digital Transformation. *2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 1–6. https://doi.org/10.1109/ITMS59786.2023.10317788

Diefenbach, T., Lucke, C., & Lechner, U. (2019). Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – A Literature Review. *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 326–333. https://doi.org/10.1109/CloudCom.2019.00057

Direktiivi (EU) 2016/1148 - EN - EUR-Lex (2016). https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

Direktiivi (EU) 2022/2555. (2022). *Direktiivi (EU) 2022/2555—EN - EUR-Lex*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Direktiivi (EU) 2022/2557, EP, CONSIL, 333 OJ L (2022). http://data.europa.eu/eli/dir/2022/2557/oj/eng

Dokuchaev, V. A., Maklachkova, V. V., Makarova, D. V., & Volkova, L. V. (2020). Analysis of Data Risk Management Methods for Personal Data Information Systems. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, 1–5. https://doi.org/10.1109/IEEECONF48371.2020.9078547

Dragstra, P. (2005). *Enterprise architecture*. Research Portal Eindhoven University of Technology. https://research.tue.nl/en/studentTheses/enterprise-architecture

Eckhardt, P., & Kotovskaia, A. (2023). The EU's cybersecurity framework: The interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*, *4*(2), 147–164. https://doi.org/10.1365/s43439-023-00084-z

Eriksson, P., & Kovalainen, A. (2008). *Qualitative Methods in Business Research*. SAGE Publications Ltd. https://doi.org/10.4135/9780857028044

Euroopan komissio. (2020). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0345

Euroopan komissio. (2023). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)—FAQs | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

Euroopan komissio. (2024, marraskuuta 28). *The Commission calls on 23 Member States to fully transpose the NIS2 Directive | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive

Euroopan komissio. (2025a, tammikuuta 15). *NIS2 Directive: New rules on cybersecurity of network and information systems | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Euroopan komissio. (2025b, maaliskuuta 4). *Implementation of the NIS2 Directive in Finland | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-finland

Euroopan komissio. (2025c, maaliskuuta 4). *The EU Cyber Solidarity Act | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

Ferguson, D. D. S. (2023). The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. *International Cybersecurity Law Review*, *4*(4), 371–386. https://doi.org/10.1365/s43439-023-00097-8

Finlex. (2011). *Valmiuslaki | 1552/2011 | Lainsäädäntö | Finlex*. https://www.finlex.fi/fi/lainsaadanto/2011/1552#part_1__chp_1__sec_3

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gartner. (2021). *The Role of Head of Enterprise Architecture in Driving Digital Transformation*. Gartner. https://www.gartner.com/en/information-technology/role/enterprise-architecture-technology-leaders

Ghaznavi-Zadeh, R. (2017). Enterprise Security Architecture-A Top down Approach. *ISACA*, *Volume 4*. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecturea-top-down-approach

Goerzig, D., & Bauernhansl, T. (2018). Enterprise Architectures for the Digital Transformation in Small and Medium-sized Enterprises. *Procedia CIRP*, *67*, 540–545. https://doi.org/10.1016/j.procir.2017.12.257

Goethals, F. (2005). *An overview of enterprise architecture framework deliverables—KU Leuven*. https://kuleuven.limo.libis.be/discovery/fulldisplay/lirias1834426/32KUL_KUL:Lirias

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642. https://doi.org/10.2307/25148742

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*, *37*(2), 337–355.

Gustafsson, J. (2017, tammikuuta 12). *Single case studies vs. Multiple case studies: A comparative study (Thesis)*. Academy of Business, Engineering and Science Halmstad University Halmstad, Sweden.

Hafsi, M., & Assar, S. (2020). Does Enterprise Architecture Support Customer Experience Improvement? Towards a Conceptualization in Digital Transformation Context. Teoksessa S. Nurcan, I. Reinhartz-Berger, P. Soffer, & J. Zdravkovic (Toim.), *Enterprise, Business-Process and Information Systems Modeling* (ss. 411–427). Springer International Publishing. https://doi.org/10.1007/978-3-030-49418-6_28

Havaluddin, P. A. (2012). Exploring COBIT Framework for Information Technology Governance (ITG) at Mulawarman University Samarinda East Kalimantan Indonesia: A Descriptive

Study. *2012 - BIMP- EAGA CONFERENCE: Enhancing Sustainability Competitiveness & Innovation*.

Helsingin Sanomat. (2024, lokakuuta 15). *Pankit | Nordea: Verkkohyökkäysten voima ja kesto täysin ennennäkemätön, tarkoitus horjuttaa yhteiskuntaa*. Helsingin Sanomat. https://www.hs.fi/talous/art-2000010761540.html

Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business Continuity Management: Time for a strategic role? *Long Range Planning*, *37*(5), 435–457. https://doi.org/10.1016/j.lrp.2004.07.011

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice*. Springer Science & Business Media.

Hiekkanen, K., Korhonen, J. J., Collin, J., Patricio, E., Helenius, M., & Mykkänen, J. (2013). Architects' Perceptions on EA Use – An Empirical Study. *2013 IEEE 15th Conference on Business Informatics*, 292–297. https://doi.org/10.1109/CBI.2013.48

IBM. (2022). *2022 IBM Security Cost of a Data Breach Report*. IBM Security Community. https://community.ibm.com/community/user/security/events/community.ibm.com/community/user/security/events/event-description?calendareventkey=7097fd42-4875-4abe-9ff6-d556af01688b&communitykey=96f617c5-4f90-4eb0-baec-2d0c4c22ab50&home=/community/user/home

IBM Corporation. (1975). *Business Systems Planning: Information Systems Planning Guide (1st Edition)*. White Plains, NY.

Jacuch, A. (2021). COMPARATIVE ANALYSIS OF CYBERSECURITY STRATEGIES. EUROPEAN UNION STRATEGY AND POLICIES. POLISH AND SELECTED COUNTRIES STRATEGIES. *Online Journal Modelling the New Europe*, *37*, 102–120.

Jonkers, H., Lankhorst, M. M., Ter Doest, H. W. L., Arbab, F., Bosma, H., & Wieringa, R. J. (2006). Enterprise architecture: Management tool and blueprint for the organisation. *Information Systems Frontiers*, *8*(2), 63–66. https://doi.org/10.1007/s10796-006-7970-2

Jugel, D., & Schweda, C. M. (2014). Interactive Functions of a Cockpit for Enterprise Architecture Planning. *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*, 33–40. https://doi.org/10.1109/EDOCW.2014.14

Kleehaus, M., & Matthes, F. (2021). Automated Enterprise Architecture Model Maintenance via Runtime IT Discovery. Teoksessa A. Zimmermann, R. Schmidt, & L. C. Jain (Toim.), *Architecting the Digital Transformation: Digital Business, Technology, Decision Support,*

Management (ss. 247–263). Springer International Publishing. https://doi.org/10.1007/978-3-030-49640-1_13

Kolehmainen, A. (2024, joulukuuta 18). *Nis2-direktiivin määräaika umpeutui, Suomi myöhästyi*. Tivi. https://www.tivi.fi/uutiset/nis2-direktiivin-maaraaika-umpeutui-suomi-myohastyi/7fab3ae4-de76-457f-9522-19045436e658

Kotusev, S. (2016). *The History of Enterprise Architecture: An Evidence-Based Review*. Journal of Enterprise Architecture.

Kotusev, S. (2017). *Eight essential enterprise architecture artifacts | BCS*. https://www.bcs.org/articles-opinion-and-research/eight-essential-enterprise-architecture-artifacts/

Krzykowski, M. (2021). Legal Aspects of Cybersecurity in the Energy Sector—Current State and Latest Proposals of Legislative Changes by the EU. *Energies*, *14*(23), Article 23. https://doi.org/10.3390/en14237836

Kuehn, W. (2023). *Getting Started with Enterprise Architecture: A Practical and Pragmatic Approach to Learning the Basics of Enterprise Architecture, Foreword*. Apress. https://doi.org/10.1007/978-1-4842-9858-9

Kurnia, S., Kotusev, S., Taylor, P., & Dilnutt, R. (2020). Artifacts, Activities, Benefits and Blockers: Exploring Enterprise Architecture Practice in Depth. *Hawaii International Conference on System Sciences 2020 (HICSS-53)*. https://aisel.aisnet.org/hicss-53/os/it_governance/4

Labuschagne, A. (2003). Qualitative Research—Airy Fairy or Fundamental? *The Qualitative Report*, *8(1)*, 100–103.

Lange, M., & Mendling, J. (2011). An Experts' Perspective on Enterprise Architecture Goals, Framework Adoption and Benefit Assessment. *2011 IEEE 15th International Enterprise Distributed Object Computing Conference Workshops*, 304–313. https://doi.org/10.1109/EDOCW.2011.41

Lange, M., Mendling, J., & Recker, J. (2016). An empirical analysis of the factors and measures of Enterprise Architecture Management success. *European Journal of Information Systems*, *25*(5), 411–431. https://doi.org/10.1057/ejis.2014.39

Lankhorst, M. (2009). *Enterprise Architecture at Work: Modelling, Communication and Analysis* (Vol. 352). Berlin: Springer.

Lankhorst, M. (2017). *Enterprise Architecture at Work*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-53933-0

Laudon, K. C., & Laudon, J. P. (2004). *Management Information Systems: Managing the Digital Firm*. Pearson Educación.

Liebetrau, T. (2024). Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice. *JCMS: Journal of Common Market Studies*, *62*(3), 705–724. https://doi.org/10.1111/jcms.13523

Löhe, J., & Legner, C. (2014). Overcoming implementation challenges in enterprise architecture management: A design theory for architecture-driven IT Management (ADRIMA). *Information Systems and E-Business Management*, *12*(1), 101–137. https://doi.org/10.1007/s10257-012-0211-y

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29; s. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Nis-2-directive.com. (2025, maaliskuuta 31). *The NIS 2 Directive | Updates, Compliance, Training*. https://www.nis-2-directive.com/

Närman, P., Holm, H., Ekstedt, M., & Honeth, N. (2013). Using enterprise architecture analysis and interview data to estimate service response time. *The Journal of Strategic Information Systems*, *22*(1), 70–85. https://doi.org/10.1016/j.jsis.2012.10.002

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Phelps, N. L. (1986). SETTING UP A CRISIS RECOVERY PLAN. *Journal of Business Strategy*, *6*(4), 5–10. https://doi.org/10.1108/eb039125

Radake, F. (2011). Toward understanding enterprise architecture management's role in strategic change: Antecedents, processes, outcomes. *10th International Conference on Wirtschaftsinformatik*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1056&context=wi2011

Rehbohm, T., & Moses, F. (2023). *Federal Cybersecurity Architecture and Information Security Management—Adoption and Diffusion of the NIS-2 Requirements*. 14–28. https://dl.gi.de/handle/20.500.12116/42622

Rehring, K., Greulich, M., Bredenfeld, L., & Ahlemann, F. (2019). *Let's Get in Touch—Decision Making about Enterprise Architecture Using 3D Visualization in Augmented Reality*. http://hdl.handle.net/10125/59617

Ross, J. W., Beath, C. M., & Mocker, M. (2019). *Designed for Digital: How to Architect Your Business for Sustained Success*. MIT Press.

Ross, J. W., Weill, P., & Robertson, D. (2006). *Enterprise Architecture As Strategy: Creating a Foundation for Business Execution*. Harvard Business Press.

Ruohonen, J. (2024). *A Systematic Literature Review on the NIS2 Directive* (arXiv:2412.08084). arXiv. https://doi.org/10.48550/arXiv.2412.08084

Saint-Louis, P., & Lapalme, J. (2016). Investigation of the Lack of Common Understanding in the Discipline of Enterprise Architecture: A Systematic Mapping Study. *2016 IEEE 20th International Enterprise Distributed Object Computing Workshop (EDOCW)*, 1–9. https://doi.org/10.1109/EDOCW.2016.7584364

Scheelen, Y., Machilsen, K., & Deprez, A. (2023, toukokuuta 16). *How to prepare for the NIS2 Directive?* https://www.ey.com/en_be/insights/cybersecurity/how-to-prepare-for-the-nis2-directive

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*, *9*(1), tyad009. https://doi.org/10.1093/cybsec/tyad009

Security Staff. (2022). *Email cyberattacks increased 48% in first half of 2022 | Security Magazine*. https://www.securitymagazine.com/articles/98145-email-cyberattacks-increased-48-in-first-half-of-2022

Simon, D., Fischbach, K., & Schoder, D. (2014). Enterprise architecture management and its role in corporate strategic management. *Information Systems and E-Business Management*, *12*(1), 5–42. https://doi.org/10.1007/s10257-013-0213-4

Sousa, P., Caetano, A., Vasconcelos, A., Pereira, C., & Tribolet, J. (2007). Enterprise Architecture Modeling with the Unified Modeling Language. Teoksessa *Enterprise Modeling and Computing with UML* (ss. 67–94). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-59904-174-2.ch004

Tamm, T., Seddon, P. B., Shanks, G., & Reynolds, P. (2011). How does enterprise architecture add value to organisations? *Communications of the Association for Information Systems*, *12*(10), 141–168.

Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE)*, *4*(1), Article 1. https://doi.org/10.54060/a2zjournals.jase.42

The SABSA Institute. (ei pvm.). *SABSA Executive Summary*. The SABSA Institute. Noudettu 29. huhtikuuta 2025, osoitteesta https://sabsa.org/sabsa-executive-summary/

Tietoevry.com. (2024, syyskuuta 30). *Nordic Cyber Resilience Report 2024*. https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2024/09/nordic-cyber-resilience-report-2024/

TOGAF. (2002, joulukuuta). *TOGAF 8 "Enterprise Edition"*. http://www6.opengroup.org/togaf/index811.htm

TOGAF. (2009). *TOGAF® Version 9*. https://www.opengroup.org/architecture/togaf8/

TOGAF. (2011). *TOGAF® 9.1*. https://pubs.opengroup.org/architecture/togaf91-doc/arch/

TOGAF. (2022). *The TOGAF® Standard, 10th Edition | www.opengroup.org*. https://www.opengroup.org/togaf/10thedition

Truyen, F. (2018). Modelinga SABSA based Enterprise Security Architecture using Enterprise Architect. *Cephas Consulting Corp*.

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Kustannusosakeyhtiö Tammi. https://www.ellibslibrary.com/book/9789520400118/laadullinen-tutkimus-ja-sisallonanalyysi

Urbach, N., & Ahlemann, F. (2019). *IT Management in the Digital Age: A Roadmap for the IT Department of the Future*. Springer International Publishing. https://doi.org/10.1007/978-3-319-96187-3

Valtioneuvosto. (2023, lokakuuta 3). *Hallituksen esitys kyberturvallisuusdirektiivin täytäntöönpanemiseksi lausunnoille*. Valtioneuvosto. https://valtioneuvosto.fi/-/1410829/hallituksen-esitys-kyberturvallisuusdirektiivin-taytantoonpanemiseksi-lausunnoille

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890. https://doi.org/10.1016/j.clsr.2023.105890

Veigurs, M., Lasmanis, T., & Romanovs, A. (2024). IT Governance in Critical Sectors: Towards the NIS2 Implementation. *2024 IEEE 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, 1–7. https://doi.org/10.1109/ITMS64072.2024.10741938

Williamson, K., & Johanson, G. (2018). *Research Methods: Information, Systems, and Contexts*. Chandos Publishing.

Winter, R. (2016). Establishing 'Architectural Thinking' in Organizations. Teoksessa J. Horkoff, M. A. Jeusfeld, & A. Persson (Toim.), *The Practice of Enterprise Modeling* (ss. 3–8). Springer International Publishing. https://doi.org/10.1007/978-3-319-48393-1_1

Winter, R., & Fischer, R. (2006). Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)*, 30–30. https://doi.org/10.1109/EDOCW.2006.33

Yin, R. K. (2009). *Case Study Research: Design and Methods*. SAGE.

Yle. (2024a, toukokuuta 14). *”En ole valtavan yllättynyt” – tietoturva-asiantuntija kertoo, miten Helsingin tietomurto oli mahdollinen*. Yle Uutiset. https://yle.fi/a/74-20088567

Yle. (2024b, lokakuuta 25). *Aleksanteri Kivimäki ei saa uusia syytteitä törkeistä tietomurroista – uhreina tusinan verran suomalaisia kohteita*. Yle Uutiset. https://yle.fi/a/74-20119800

Yle. (2024c, marraskuuta 1). *Melkein joka kolmannen pohjoismaalaisen yhtiön järjestelmiin on murtauduttu vuoden aikana*. Yle Uutiset. https://yle.fi/a/74-20120894

Zachman, J. A. (1987). A framework for information systems architecture. *IBM Systems Journal*, *26*(3), 276–292. IBM Systems Journal. https://doi.org/10.1147/sj.263.0276

Liitteet

Liite 1. Aineistonhallintasuunnitelma

Opiskelijan aineistonhallintasuunnitelma

1. Tutkimusaineisto

Tutkimusaineistolla tarkoitetaan kaikkea sitä aineistoa, millä tutkimuksen analyysi ja tulokset voidaan todentaa ja toisintaa. Se voi olla esim. erilaisia mittaustuloksia, kyselyistä ja haastatteluista syntyvää dataa, äänitteitä ja videoita, muistiinpanoja, ohjelmistoja, lähdekoodeja, biologisia näytteitä, tekstinäytteitä ja keruuaineistoja.

Alla listattuna kaikki tutkimuksessa käytetty tutkimusaineisto.

Aineistotyyppi	**Sisältää henkilötietoja***	**Tuotan aineiston itse**	**Joku muu on tuottanut aineiston**	**Muuta huomioitavaa**
Aineistotyyppi 1: Kokonaisarkkitehtuurin mallinnukset			x	Aineistoa on käsitelty vain toimeksiantajan laitteilla ja pääsy aineistoon päättyy tutkielman valmistumisen jälkeen.
Aineistotyyppi 2: Teams kokonaisarkkitehtuuri aineistot			x	Aineistoa on käsitelty vain toimeksiantajan laitteilla ja pääsy aineistoon päättyy tutkielman valmistumisen jälkeen.

Aineistotyyppi	**Sisältää henkilötietoja***	**Tuotan aineiston itse**	**Joku muu on tuottanut aineiston**	**Muuta huomioitavaa**
Aineistotyyppi 3: Häiriöiden raportointijärjestelmä			x	Aineistoa on käsitelty vain toimeksiantajan laitteilla ja pääsy aineistoon päättyy tutkielman valmistumisen jälkeen.
Aineistotyyppi 4: Muistiinpanot ja analyysi		x		Aineisto on tehty tutkijan omalle koneelle, mutta se ei sisällä mitään arkaluontoista sisältöä.

* Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Esimerkkejä henkilötiedoksi katsotuista tiedoista löydät Tietosuojavaltuutetun toimiston sivuilta

2. Henkilötietojen käsittely tutkimuksessa

Mikäli aineistosi sisältää henkilötietoja, olet velvoitettu noudattamaan EU:n tietosuoja-asetusta (GDPR) sekä Suomen tietosuojalakia. Henkilötietoja sisältävän aineiston osalta sinun tulee laatia tutkittavillesi tietosuojailmoitus sekä selvittää, kuka toimii aineiston osalta rekisterinpitäjänä.

Laadin tutkittavilleni tietosuojailmoituksen** ja toimitan sen heille ennen aineiston keruuta ☐

Henkilötietojen osalta rekisterinpitäjänä** toimii opiskelija ☐ yliopisto ☐

Aineistoni ei sisällä henkilötietoja ☒

**Lisätietoja yliopiston intranetin Tietosuojaohjeita opinnäytetyöhön -sivulta

3. Aineiston käyttöön liittyvät luvat ja oikeudet

3.1 Itse tuotettu aineisto

Tutkielman aineistoon kuuluu tutkijan tekemät muistiinpanot ja analyysi muusta tutkitusta datasta.

Aineistotyyppi 4: Ei erillistä lupaa pyydetty, mutta sisältää vain tietoja, jotka myös osana tutkielman tuloksia.

3.2 Jonkun muun tuottama aineisto

Tutkielman aineisto on saatu toimeksiantajaorganisaatiolta käyttöön tutkielmaa varten.

Aineistoon liittyvät oikeudet ja lisenssit

Aineistotyyppi 1: Lupa saatu toimeksiantajaorganisaatiolta.

Aineistotyyppi 2: Lupa saatu toimeksiantajaorganisaatiolta.

Aineistotyyppi 3: Lupa saatu toimeksiantajaorganisaatiolta.

4. Aineiston säilyttäminen tutkimuksen aikana

Yliopiston verkkokansiossa ☐

Yliopiston tarjoamassa Seafile-pilvipalvelussa ☐

Jossakin muualla, missä? ☒

Aineisto säilytetään toimeksiantajaorganisaation tietokoneella, joka on saatu tutkimuksen ajaksi opiskelijan käyttöön. Omat muistiinpanot ovat tutkija omalla koneella. Tarvittavista päivityksistä ja suojatoimista on pidetty huolta tutkimuksen aikana.

5. Aineiston dokumentointi ja metadata

Aineisto koostuu kokonaisarkkitehtuurin mallinnuksista, häiriöraporteista ja näistä tehdyistä muistiinpanoista sekä analyyseistä.

5.1 Aineiston dokumentointi

Käytän aineiston dokumentointiin

tutkimuspäiväkirjaa ☐

erillistä dokumenttia, johon kirjaan aineiston pääasiat, kuten tehdyt muutokset, analyysin vaiheet sekä esim. muuttujien merkitykset ☒

aineiston mukana kulkevaa readme-tiedostoa, jossa kuvataan aineiston pääasiat ☐

jotain muuta, mitä? ☐

5.2 Aineiston järjestys ja eheys

Säilytän alkuperäisen aineiston erillään tutkimuksenteon aikana käyttämästäni aineistosta, jotta voin palata alkuperäiseen, jos tarvetta ilmenee. ☒

Versionhallinta: mietin jo ennen tutkimuksenteon alkua, miten tulen nimeämään eri aineistoversiot ja noudan sitä systemaattisesti ☒

Tiedostan jo tutkimuksen alussa aineistoni elinkaaren, ja varaudun tilanteisiin, joissa data saattaa huomaamatta muuttua, kuten esim. nauhoitus, litterointi, konversio toiseen tiedostomuotoon, tallentaminen jne. ☒

5.3 Metadata

Tallennan aineistoni arkistoon tai tietopankkiin, joka huolehtii metadatasta puolestani. ☐

Minun pitää luoda metadata, koska arkisto, johon tallennan aineiston edellyttää sitä. ☐

En tallenna aineistoani julkiseen arkistoon, enkä tarvitse metadataa. ☒

6. Aineisto tutkimuksen valmistuttua

Tutkielman aineisto jää toimeksiantajaorganisaation koneelle, eikä sitä ole tallennettuna muihin paikkoihin. Tutkielman valmistumisen jälkeen tietokone palautetaan toimeksiantajan haltuun ja tutkijan tekemät muistiinpanot poistetaan.

Liite 2. Generatiivisen tekoälyn käyttö

Selvitys generatiivisen tekoälyn käytöstä (engl. Declaration on the Use of Generative Artifical Intelligence)

Tämän tutkielman luomisessa käytin generatiivista tekoälyä erilaisiin tukeviin tehtäviin. Työkalut, niiden käyttötarkoitus ja tarkistustoimenpiteet on selitetty yksityiskohtaisesti alla. Vahvistan, että olen käyttänyt kaikkia tekoäly työkaluja tarvittavalla huolellisuudella ja varovaisuudella, olen täysin tuonut esille niiden käytön yliopiston linjausten mukaisesti ja otan täyden vastuun kaikesta tässä tutkielmassa esitellystä materiaalista.

1. **Työkalu: OpenAI ChatGPT (GPT-4 & 3.5 Version)**
    - **Käyttövaihe**: Ideointi ja aiheeseen perehtyminen
    - **Käyttötarkoitus**: Käytin ChatGPT:tä antamaan lisäehdotuksia omille ideoilleni ja erilaisia vaihtoehtoja, miten yhdistää ideani. Lisäksi käytin kyseistä tekoälyä yhtenä tapana perehtyä tutkielmaani liittyviin aiheisiin tehostaakseni oman ymmärryksen kartuttamista aiheesta.
        - Esimerkki Kehote (Helmikuu 2025): "What is the difference between EA artifact and deliverable?" (suom. ”Mikä ero on kokonaisarkkitehtuurin artefaktilla ja tuotoksella?”)
    - **Tarkistustoimenpiteet**: Tekoälyn antama vastaus nosti merkittävimmiksi eroiksi termien välillä niiden laajuuden, tarkoituksen ja miten ne ovat osana koko kokonaisarkkitehtuuriprosessia ja antoi näistä tarkemmat selvitykset. Tämä oli minulle tarvittava tieto jatkaakseni tieteellisten artikkelien läpikäymistä aiheesta ja ymmärtääkseni paremmin kokonaisarkkitehtuuriin liittyvää termistöä.
2. **Työkalu: OpenAI ChatGPT (GPT-4 & 3.5 Version)**
    - **Käyttövaihe**: Editointi
    - **Käyttötarkoitus**: Käytin ChatGPT:tä kirjoittamisen tukena kääntämällä vieraskielistä tekstiä suomeksi, hakemalla ehdotuksia sanavalintoihin, tarkistamalla oman tekstini kirjoitusasua ja pyytämällä kirjoitustyyliin liittyviä parannusehdotuksia tekoälyltä
    - **Tarkoitustoimenpiteet**: Kävin aina huolellisesti läpi tekoälyn tuottamat käännökset, parannukset jne. ja varmistin, ettei alkuperäinen merkitys muuttunut, ja että teksti säilyi akateemisesti oikeana. Kontrolli tekstistä säilyi itselläni.