Tietotarpeet tietoturvallisuuden hallintajärjestelmän toimivuudesta Väylävirastossa

Pirita Tuikka

2024 Laurea

Laurea-ammattikorkeakoulu

Tietotarpeet tietoturvallisuuden hallintajärjestelmän toimivuudesta Väylävirastossa

Pirita Tuikka

Turvallisuus ja riskienhallinta

Opinnäytetyö

Kesäkuu, 2024

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuuden ja riskienhallinnan koulutus

Tradenomi (AMK)

Pirita Tuikka

Tietotarpeet tietoturvallisuuden hallintajärjestelmän toimivuudesta Väylävirastossa

Vuosi 2024 Sivumäärä 43

Opinnäytetyön tarkoituksena oli selvittää, mitä tietoa Väyläviraston päätöksentekijät tarvitsevat kokonaiskuvan muodostamiseksi viraston tietoturvallisuuden hallintajärjestelmän toimivuudesta. Tavoitteena oli laatia ehdotus tietotarpeista, joiden avulla tietoturvallisuuden hallintajärjestelmän suorituskykyä ja vaikuttavuutta voidaan seurata ja mitata sekä raportoida. Taustalla oli tarve luoda ISO/IEC 27001 -standardin mukaisia tietoturvamittareita osana organisaation tietoturvallisuuden hallintajärjestelmän kehitysprojektia.

Tietoperustana käytettiin ISO/IEC 27001 ja 27004 -standardien soveltuvia osia. Lisäksi tietoperustassa hyödynnettiin kokonaiskuvan muodostamisesta sekä tietoturvallisuuden mittaamisesta ja raportoinnista kertovaa kirjallisuutta. Opinnäytetyön menetelmänä oli teemahaastattelu. Haastatteluihin osallistui 2–5 henkilöä kolmesta ryhmästä, jotka olivat asiantuntijat, keskijohto ja ylin johto. Aineisto koostui haastateltujen vastauksista kysymyksiin, jotka käsittelivät seuraavia aihealueita: tunnistaminen, suojaaminen, havainnointikyky ja reagointi. Mainitut teemat oli muodostettu Väyläviraston digitaalisen turvallisuuden periaatteiden mukaan. Lisäksi aineistossa oli haastateltujen näkemyksiä strategisesta ja taktisesta tietoturvaraportoinnista.

Työn keskeisin tuotos oli ehdotus tietotarpeista, jotka kattoivat Väyläviraston digitaalisen turvallisuuden periaatteet. Tietotarpeita olivat muun muassa tietoturvariskeille altistuminen, palveluntuottajanäkökulma eli tietoturvallisuus toimittajasuhteissa, tietojärjestelmien operatiivinen tilannekuva ja tietoturvatapahtumien kehityssuunta. Tietotarpeet saatiin määriteltyä onnistuneesti, ja mittarikehityskin käynnistyi jo menestyksekkäästi tulosten pohjalta. Jatkossa tietotarpeet ja niihin vastaavat mittarit tulisi sovittaa oikeaan kontekstiinsa strategisen tai taktisen tason tietoturvaraportointiin. Tietotarpeiden ja mittareiden käyttö kohentaa päätöksenteon tietoperustaisuutta, mikä edistää tietoturvallisuuden jatkuvaa parantamista virastossa.

Asiasanat: ISO/IEC 27001, tietotarve, tietoturvallisuuden hallintajärjestelmä, tietoturvallisuus

Laurea University of Applied Sciences **Abstract**

Degree Programme in Safety, Security and Risk Management

Bachelor of Business Administration

Pirita Tuikka

Performance and Effectiveness of Väylävirasto's Information Security Management System from an Information Needs Viewpoint

Year 2024 Pages 43

The purpose of the thesis was to determine the information needed by Väylävirasto's decision-makers to form a comprehensive understanding of the performance and effectiveness of the organization's Information Security Management System (ISMS). The objective was to develop a proposal for information needs that would enable the monitoring, measurement, and reporting of the performance and effectiveness of the ISMS. This initiative stemmed from the demand to create information security metrics in accordance with the ISO/IEC 27001 standard as a part of the organization's ongoing ISMS development project.

The theoretical framework was based on the relevant sections of the ISO/IEC 27001 and 27004 standards. Additionally, literature on forming a comprehensive understanding, as well as measuring and reporting information security, was utilized. The methodology of the thesis involved thematic interviews. These interviews included 2-5 participants from three groups: experts, middle management, and top management. The data consisted of the interviewees' answers to questions covering the areas of identification, protection, detection and response. These themes were aligned with Väylävirasto's digital security principles. Moreover, the data included the interviewees' perspectives on strategic and tactical information security reporting.

The primary outcome of this work was a proposal for information needs that covered Väylävirasto's digital security principles. The information needs included exposure to information security risks, the service provider perspective, i.e., information security in supplier relationships, the operational status of ICT systems, and the trend of information security incidents. The information needs were successfully defined, and the development of metrics was already initiated based on the results. In the future, the information needs and their corresponding metrics should be applied to their appropriate context in either strategic or tactical level information security reporting. The use of the information needs and metrics will enhance data-driven decision-making, promoting the continuous improvement of information security within the organization.

Keywords: information needs, information security, Information Security Management System, ISO/IEC 27001

Sisällys

1 Johdanto 6
2 Kehittämistehtävä ja sen lähtökohdat 7
2.1 Rajaukset 8
2.2 Väylävirasto 8
2.2.1 Digitaalisen turvallisuuden periaatteet 9
2.2.2 Johtamisjärjestelmän mukainen tietoturvaraportointi 11
3 Tietoturvallisuuden hallinta 12
3.1 Tietoturvallisuus 12
3.2 Tietoturvallisuuden hallintajärjestelmä 13
3.3 Standardi ISO/IEC 27001 14
3.3.1 Pakolliset vaatimukset 15
3.3.2 Liite A 17
4 Kokonaiskuva tietoturvallisuudesta 17
4.1 Tietoturvallisuuden mittaaminen 17
4.2 Standardi ISO/IEC 27004 19
4.2.1 Tietotarpeiden tunnistaminen 19
4.2.2 Suorituskyky ja vaikuttavuus 21
4.3 Tietoturvaraportointi 22
4.3.1 Kokonaiskuvan muodostaminen 22
4.3.2 Tietoturvaraportoinnin yleisöt ja sisällöt 23
5 Kehittämistyön menetelmä ja prosessi 24
6 Tulokset 26
6.1 Tunnistaminen 26
6.2 Suojaaminen 28
6.3 Havainnointikyky 31
6.4 Reagointi 32
6.5 Johdon raportointi 34
6.5.1 Vuosiraportointi 35
6.5.2 Väliraportointi 36
7 Johtopäätökset ja pohdinta 37
Lähteet 40
Kuviot 43
Taulukot 43

1 Johdanto

Teknologinen kehitys ja digitalisaation kiihtyminen ovat luoneet uusia mahdollisuuksia, mutta samalla ne ovat tuoneet mukanaan ennennäkemättömiä haasteita. Kehittyvät digitaaliset teknologiat helpottavat organisaatioiden toimintaa, mutta verkottunut maailma, jossa tieto on arvokas resurssi, on hedelmällinen maaperä yhä monipuolisemmille tietoturvauhille. Ne voivat ulottua yksittäisen käyttäjän sähköpostilaatikkoon kilahtamasta tietojenkalasteluroskapostista aina laajamittaisiin valtioiden kriittiseen infrastruktuuriin kohdistuviin kyberhyökkäyksiin saakka.

Tietoturvallisuus usein selitetään tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamisena. Tätä tarkoitusta varten useat organisaatiot ovat ottaneet käyttöönsä tietoturvallisuuden hallintajärjestelmän. Eräs systemaattinen ja kansainvälisesti tunnettu lähestymistapa tietoturvallisuuden hallintajärjestelmän luomiseen ja ylläpitämiseen on ISO/IEC 27001 -standardi. Standardi ei ainoastaan määritä kehystä tietoturvallisuuden hallinnalle, vaan korostaa myös jatkuvan parantamisen merkitystä.

Osana jatkuvaa parantamista ISO/IEC 27001 -standardissa edellytetään, että organisaatiot seuraavat, mittaavat, analysoivat ja arvioivat tietoturvallisuuden hallintajärjestelmänsä toimivuutta. Seurannan ja mittaamisen avulla kerätty tieto on tärkeää raportoinnin näkökulmasta. Tietoturvaraportoinnin tarkoituksena on tarjota päätöksentekijöille kattava kokonaiskuva organisaation tietoturvallisuuden tilasta. Kun seuranta- ja mittausprosessien synnyttämä tieto analysoidaan ja esitetään selkeässä muodossa, se mahdollistaa tietoperustaisen päätöksenteon, jonka avulla tietoturvariskejä ja -uhkia voidaan hallita ja tietoturvallisuuden kehittämistoimia priorisoida.

Tässä opinnäytetyössä selvitetään, mitä tietoa Väyläviraston päätöksentekijät tarvitsevat kokonaiskuvan muodostamiseksi tietoturvallisuuden hallintajärjestelmän toimivuudesta. Tavoitteena on laatia ehdotus tietotarpeista, joiden avulla Väyläviraston tietoturvallisuuden hallintajärjestelmän suorituskykyä ja vaikuttavuutta voidaan seurata ja mitata sekä raportoida niin strategisella kuin taktisellakin tasolla. Tietotarpeet selvitetään teemahaastatteluissa, joissa haastatellaan johtoporrasta ja tietoturvallisuuden parissa työskenteleviä asiantuntijoita. Opinnäytetyö on osa käynnissä olevaa ISO 27001 -kehitysprojektia, jonka lopullisena päämääränä on kehittää Väyläviraston tietoturvallisuuden hallintajärjestelmää siten, että se täyttää kyseisen standardin vaatimukset.

2 Kehittämistehtävä ja sen lähtökohdat

Valtioneuvoston periaatepäätöksessä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (2021, 8) todetaan seuraavaa: "Kriittisten toimialojen suurimpien ja yhteiskunnan keskeisten toimintojen kannalta merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 –sertifioinnilla tai sitä vastaavalla yleiseen tietoturvastandardiin perustuvalla sertifioinnilla vuoden 2025 loppuun mennessä." Väylävirastossa on periaatepäätöksen myötä käynnistetty ISO 27001 -kehitysprojekti, jonka päämääränä on saattaa tietoturvallisuuden hallintajärjestelmä ajantasalle, jotta se voidaan tarvittaessa sertifioida. Tämän opinnäytetyön kirjoitushetkellä keväällä 2024 ei ole varmistunut, edellytetäänkö yhteiskunnan kriittisiltä toimijoilta varsinaista sertifikaattia.

Väylävirastolla on jo käytössään standardin ISO/IEC 27001:2013 -mukainen sertifioimaton tietoturvallisuuden hallintajärjestelmä, mutta standardin tuorein vuonna 2022 julkaistu versio aiheuttaa tarpeen päivittää hallintajärjestelmän prosesseja, tietoturvan hallintakeinoja ja dokumentaatiota. Opinnäytetyö on osa Väyläviraston ISO 27001 -kehitysprojektia, jossa kehitetään tietoturvallisuuden hallintajärjestelmää ISO/IEC 27001:2022 -standardin mukaiselle tasolle.

Työn aiheeksi valikoitui tietoturvallisuuden hallintajärjestelmän nykytila-analyysin pohjalta seurannan ja mittaamisen kehittäminen. ISO/IEC 27001 (2022, 13) esittää luvussa 9 vaatimuksia tietoturvallisuuden hallintajärjestelmän suorituskyvyn arvioinnille. Kappaleen 9.1 a-kohdassa esitetään vaatimus, että organisaation on määriteltävä, mitä sen täytyy seurata ja mitata. Ennen mittarien luontia tulisi kuitenkin tunnistaa tietotarpeet (ISO/IEC 27004:2016, 15), koska mittarien tulisi vastata kyseisiin tietotarpeisiin.

Kehittämistehtävän tarkoituksena on selvittää, mitä tietoa Väyläviraston päätöksentekijät tarvitsevat kokonaiskuvan muodostamiseksi viraston tietoturvallisuuden hallintajärjestelmän toimivuudesta. Tavoitteena on laatia ehdotus tietotarpeista, joiden avulla tietoturvallisuuden hallintajärjestelmän suorituskykyä ja vaikuttavuutta voidaan seurata ja mitata. Tietotarpeiden pohjalle luodaan ISO 27001 -kehitysprojektin myöhemmässä vaiheessa tietoturvamittarit. Mittauksella saadut tulokset raportoidaan Väyläviraston päätöksentekijöille päätöksenteon tueksi. Näin ollen työ kehittää lopulta myös tietoturvaraportointia.

Kehittämistehtävän kysymys on:

- Mitä tietoa Väyläviraston päätöksentekijät tarvitsevat kokonaiskuvan muodostamiseksi tietoturvallisuuden hallintajärjestelmän toimivuudesta?

Kysymykseen etsitään vastausta teemahaastattelujen avulla. Opinnäytetyötä varten haastateltiin paitsi johtoporrasta myös asiantuntijoita, mistä kerrotaan tarkemmin luvussa 5.

Opinnäytetyön tuloksista voivat olla kiinnostuneita Väyläviraston lisäksi muut organisaatiot, jotka toimivat yhteiskunnan kriittisillä toimialoilla ja joita valtioneuvoston periaatepäätös koskettaa. Samoin tuloksista voivat olla kiinnostuneita organisaatiot, jotka aikovat mahdollisesti lähteä ISO/IEC 27001 -sertifiointiprosessiin tai jotka muutoin pyrkivät parantamaan tietoturvallisuuttaan standardin mukaisesti.

2.1 Rajaukset

ISO 27001 -kehitysprojektin ensimmäisessä vaiheessa keskitytään Väyläviraston ydintoimintaa tukeviin prosesseihin sekä niihin liittyviin tietoihin ja tietojärjestelmiin. Opinnäytetyö sijoittuu kehitysprojektin ensimmäiseen vaiheeseen eli tarkastelun kohteena on Väyläviraston hallinnollinen IT-ympäristö, niin kutsuttu toimistoympäristö. Tarkastelun ulkopuolelle jää OT-ympäristö, kuten esimerkiksi rataverkon käyttö, joka tulee mukaan kehitysprojektin toisessa vaiheessa tuonnempana. Sen vuoksi opinnäytetyön aineisto on yhtä poikkeusta lukuun ottamatta kerätty Väylien käyttö, turvallisuus ja tieto -toimialan turvallisuus- ja tieto-osastoilta. Opinnäytetyön tulokset eivät siten ole yleistettävissä Väyläviraston hallinnollisen ympäristön ja tietoturvallisuuden hallintajärjestelmän soveltamisalan ulkopuolelle. Lisäksi kehitysprojekti samoin kuin opinnäytetyökin keskittyy tässä vaiheessa tietoturvallisuuteen, joten tietosuoja on tarkastelun ulkopuolella.

Tämä työ ei rakenna tietoturvallisuuden hallintajärjestelmälle mittareita, vaan ne luodaan kehitysprojektin edetessä myöhemmin. Opinnäytetyö valmistelee tietoturvallisuuden hallintajärjestelmän mittaamista etsimällä tietotarpeet, jotka Väyläviraston päätöksentekijöillä on, jotta he voisivat muodostaa kokonaiskuvan hallintajärjestelmän toimivuudesta päätöksenteon tueksi. Kokonaiskuva viittaa tässä kattavaan ymmärrykseen tietoturvallisuuden hallintajärjestelmän toimivuudesta. Kokonaiskuvassa johdon päätöksenteon näkökulmasta tärkeitä asioita ovat strateginen ja taktinen tietoturvaraportointi, joten tämä työ ei suoranaisesti käsittele operatiivista eli teknistä tietoturvaraportointia.

2.2 Väylävirasto

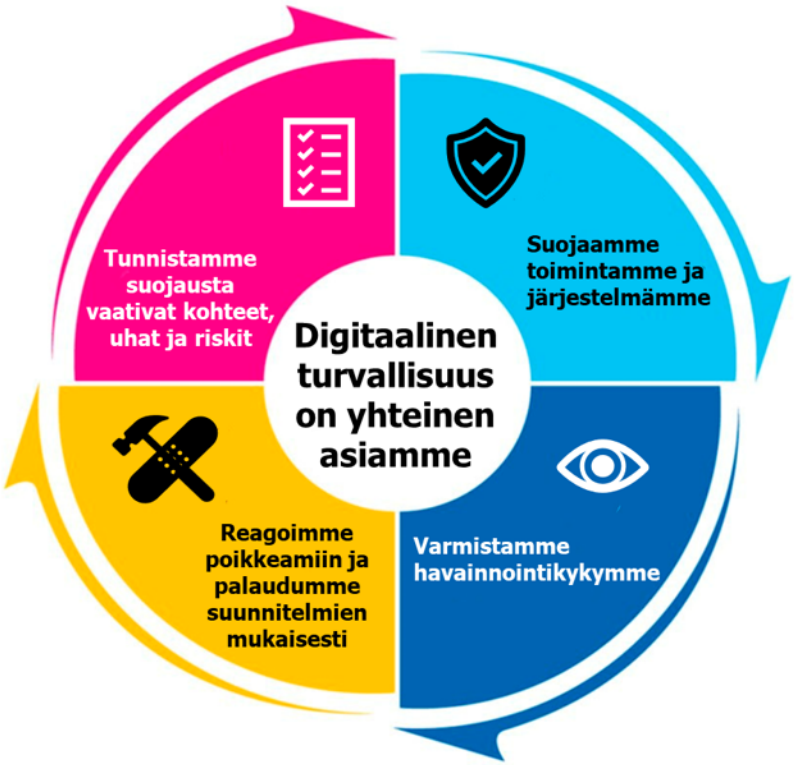
Opinnäytetyön toimeksiantaja on Väylävirasto, joka vastaa valtion tie-, rata- ja vesiväylistä (Väylävirasto 2023a, 2). Se on noin 490 asiantuntijan organisaatio. Väylävirasto on vahvasti tilaajavirasto, joten se työllistää välillisesti jopa 18 000 ihmistä. Viraston vuosibudjetti vuonna 2024 on noin 2,1 miljardia euroa, ja sen hallitseman väyläomaisuuden arvo on 20 miljardia euroa. (Väylävirasto 2024b.)

Laki Väylävirastosta (862/2009) määrittelee Väyläviraston aseman ja toiminta-ajatuksen seuraavasti: Väylävirasto on yksi liikenne- ja viestintäministeriön hallinnonalan organisaatioista, ja sen tehtävänä on käytännössä huolehtia tie-, rata- ja vesiliikenteen väyläverkon suunnittelusta, kunnossapidosta ja kehittämisestä. Lisäksi virasto osallistuu liikenteen ja maankäytön

yhteensovittamiseen sekä järjestää talvimerenkulun ja liikenteenohjauksen. Laissa Väylävirastosta (862/2009) myös todetaan viraston toiminta-ajatukseksi edistää väyläverkon toimivuutta, liikenteen turvallisuutta, automatisaatiota ja kestävää kehitystä osana liikennejärjestelmän kokonaisuutta. Lisäksi Väyläviraston toiminta-ajatuksena on edistää alueiden ja elinkeinoelämän toimintaedellytyksiä ja tasapainoista kehitystä.

2.2.1 Digitaalisen turvallisuuden periaatteet

Digitaalinen turvallisuus on valtionhallinnossa käytössä oleva käsite, joka viittaa tavoitetilaan, jossa digitaaliseen toimintaympäristöön voidaan luottaa (Valtiovarainministeriö 2020). Toiminta digitaalisessa toimintaympäristössä on täten turvallista ja hallittua myös häiriötilanteissa. Digitaalinen turvallisuus on laaja käsite, joka kattaa soveltuvin osin tieto- ja kyberturvallisuuden lisäksi tietosuojan, johtamisen ja riskienhallinnan sekä jatkuvuudenhallinnan. (Digi- ja väestötietovirasto 2022, 68.) Digitaalisen turvallisuuden käsitettä mukaillen Väylävirasto on määritellyt toiminnalleen digitaalisen turvallisuuden periaatteet.



Kuvio 1: Väyläviraston digitaalisen turvallisuuden periaatteet (Väylävirasto 2023b)

Digitaalisen turvallisuuden periaatteet asettavat tavoitteet ja vaatimukset Väyläviraston tieto- ja kyberturvallisuudelle sekä tietosuojalle ylätasolla. Niiden tarkoituksena on varmistaa tietoaineistojen, tietojärjestelmien ja viraston toiminnan turvallisuus (Väylävirasto 2023c), ja ne täydentävätkin viraston turvallisuusperiaatteita (Väylävirasto 2023b). Digitaalisen turvallisuuden periaatteet ovat korvanneet entisen tietoturvapolitiikan ja osan tietosuojaperiaatteista (Väylävirasto 2023c). Digitaalisen turvallisuuden periaatteet ovat julkisesti nähtävillä Väyläviraston nettisivuilla. Ne on esitetty kuviossa 1 jatkuvan parantamisen kehällä.

Tunnistamme suojausta vaativat kohteet, uhat ja riskit -periaatteen mukaan Väylävirastossa tunnistetaan ja luokitellaan suojausta vaativat kohteet, kuten tietojärjestelmät, tietovarannot, tiedot ja tilat. Lisäksi periaate määrittää, että Väylävirastossa tunnistetaan myös uhat ja riskit. (Väylävirasto 2023b.)

Suojaamme toimintamme ja järjestelmämme -periaatteen mukaan Väylävirastossa määritellään suojaustoimenpiteet, jotka perustuvat riskien arviointiin ja tunnistettuihin vaatimuksiin. Vaatimuksia ovat tietoturvaan ja tietosuojaan liittyvät säädökset, velvoitteet ja standardit. (Väylävirasto 2023b.) Julkisen hallinnon toimijana ja viranomaisena viraston toimintaa ohjaavat lainsäädäntö sekä valtionhallinnon ja hallinnonalan ohjeet. Periaate kattaa myös henkilöstön ja palveluntuottajien tietoisuuden ja osaamisen kasvattamisen. Lisäksi Väylävirastossa huomioidaan toiminnan todelliset tarpeet. (Väylävirasto 2023b.)

Varmistamme havainnointikykymme -periaatteen mukaan Väylävirastossa havaitaan mahdolliset poikkeamat, ja niistä ilmoitetaan matalalla kynnyksellä. Havainnointikykyä myös kehitetään jatkuvasti. (Väylävirasto 2023b.)

Reagoimme poikkeamiin ja palaudumme suunnitelmien mukaisesti -periaatteen mukaan Väylävirastossa reagoidaan havaittuihin poikkeamiin poikkeamanhallintaprosessin mukaisesti mahdollisimman ripeästi. Reagoimista niin ikään harjoitellaan säännöllisesti. Periaate myös määrittää, että häiriötilan jälkeen Väylävirastossa palaudutaan normaalitilaan etukäteen laadittujen toipumissuunnitelmien mukaisesti. Lisäksi häiriöistä opitaan ja varautumista parannetaan edelleen. (Väylävirasto 2023b.)

Periaatteet perustuvat pitkälti Digi- ja väestötietoviraston Digitaalisen turvallisuuden arkkitehtuuriin (Digi- ja väestötietovirasto 2022), joka puolestaan perustuu NIST Cyber Security Framework (NIST CSF) -viitekehykseen. NIST CSF on Yhdysvaltain standardisointi- ja teknologiainstituutin (National Institute of Standards and Technology) kehittämä tietoturvaviitekehys, jossa esitetään joukko suosituksia, jotka auttavat organisaatioita ymmärtämään, hallitsemaan ja vähentämään tietoturvariskejään (NIST 2024a). Viitekehys koostuu viidestä funktiosta: tunnistaminen, suojaaminen, havaintokyky, reagointi ja palautuminen (NIST 2024b). Kaksi viimeisimpänä mainittua funktiota on Väyläviraston digitaalisen turvallisuuden periaatteissa yhdistetty yhdeksi periaatteeksi.

Sekä NIST CSF:llä että ISO/IEC 27001:llä, joka on tämän opinnäytetyön keskiössä, on sama tarkoitus: suojata organisaation tietoja ja vähentää tietoturvariskejä. Näiden kahden viitekehyksen välillä onkin monenlaisia yhteneväisiä käytäntöjä sikäli, kun molemmat pohjautuvat laajalti hyväksyttyihin tietoturvallisuuden parhaisiin käytäntöihin. Merkittävimmäksi eroksi voidaan katsoa se, että ISO/IEC 27001 on suunniteltu vaatimustenmukaisuuden osoittamisen standardiksi, kun taas NIST CSF toimii ennemminkin ohjenuorana, eikä siihen voi sertifioitua. (Alexander & Panguluri, 2016, 38.)

Väyläviraston ISO 27001 -kehitysprojektissa tietoturvallisuuden hallintajärjestelmää kehitetään ISO/IEC 27001 -standardin tuoreimman version 2022 mukaiselle tasolle. Standardin luvussa 9 esitetään vaatimuksia tietoturvallisuuden hallintajärjestelmän suorituskyvyn arvioinnista (ISO/IEC 27001:2022, 13). Jotta kyseisessä luvussa esitetyt vaatimukset voitaisiin täyttää, tulee Väyläviraston seurata ja mitata tietoturvatavoitteidensa toteutumista (ISO/IEC 27004:2016, 7). Koska digitaalisen turvallisuuden periaatteet asettavat Väyläviraston tietoturvallisuudelle ylätason tavoitteet ja vaatimukset, on ne valittu opinnäytetyön lähtökohdaksi. Teemahaastatteluiden teemat tulevat digitaalisen turvallisuuden periaatteista ja johdon raportoinnista, mistä kerrotaan enemmän luvussa 5. ISO/IEC 27001 -standardin vaatimuksiin syvennytään tarkemmin kappaleessa 3.3.

Kuten kappaleessa 2.1 todetaan, on tietosuoja tämän opinnäytetyön rajauksen ulkopuolella, vaikka Väyläviraston digitaalisen turvallisuuden periaatteet sisältävätkin myös tietosuojanäkökulman. Lisäksi on todettava, että opinnäytetyössä puhutaan lähinnä tietoturvallisuudesta. Tietoturvallisuus (engl. *Information Security*) tarkoittaa tiedon luottamuksellisuuden, saatavuuden ja eheyden varmistamista (ISO/IEC 2000:2020, 17). Tietoturvallisuuden käsite avataan tarkemmin kappaleessa 3.1.

Opinnäytetyössä tietoturvallisuudesta käytetään myös lyhyempää ilmaisua tietoturva. Sen sijaan opinnäytetyössä ei juuri puhuta kyberturvallisuudesta (engl. *Cyber Security*), jota usein käytetään tietoturvallisuuden synonyymina. Sekä tieto- että kyberturvallisuuden tarkoituksena on suojata tietoja erilaisia uhkia vastaan, mutta käsitteissä on määritelmällisiä eroja, jotka vieläpä vaihtelevat lähteestä toiseen. Taherdoost (2023, 485) esittää eroksi sen, että tietoturvallisuus keskittyy suojaamaan tietoa kaikkialla, kun taas kyberturvallisuus keskittyy erityisesti kyberympäristöön. Kyberympäristö tarkoittaa digitaalisista tietojärjestelmistä ja tietoverkoista muodostuvaa ympäristöä (Kokonaisturvallisuuden sanasto 2017, 66). Tässä opinnäytetyössä puhutaan tietoturvallisuudesta, koska käsite kattaa kaikki tietojen suojaamiseen liittyvät näkökohdat, eikä se keskity nimenomaisesti mainittuun kyberympäristöön.

2.2.2 Johtamisjärjestelmän mukainen tietoturvaraportointi

Väyläviraston johtamisjärjestelmä tarkoittaa menettelyjä, joita viraston toiminnassa ja toiminnan johtamisessa käytetään. Sen tavoite on varmistaa toiminnan vaatimustenmukaisuus,

turvallisuus, laatu ja tehokkuus. (Väylävirasto 2024d.) Viraston sisäisen johtamisen valvonta, seuranta ja raportointi tapahtuu säännönmukaisesti kolme kertaa vuodessa. Johdon raportointi viittaakin opinnäytetyössä Väyläviraston johtamisjärjestelmän mukaiseen säännölliseen raportointiin, jossa digitaalinen turvallisuus on mukana. Vuoden aikana johdolle koostetaan kaksi väliraporttia huhtikuun ja elokuun lopun tilanteista, minkä lisäksi seuraavan vuoden tammikuussa he saavat vuosiraportin vuoden lopun ja koko edellisen vuoden tilanteesta. Raportointi kokoaa tiedot toiminnan vaatimustenmukaisuuden ja vaikuttavuuden arviointia sekä päätöksentekoa varten. (Väylävirasto 2024c.)

ISO/IEC 27001 -standardi vaatii etenkin ylimmältä johdolta aktiivista johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmän tehokkaaseen hallintaan ja jatkuvaan parantamiseen (ISO/IEC 27001:2022, 7). Ylin johto harvemmin kuitenkaan osallistuu jokapäiväiseen päätöksentekoon tietoturvallisuudesta, vaan päätöksiä tehdään monilla organisaation tasoilla. Ylimmän johdon vastuulla onkin määritellä tietoturvallisuuden kannalta tärkeät roolit, vastuut ja valtuudet organisaatiossa (ISO/IEC 27001:2022, 8). Opinnäytetyön näkökulman ja rajauksen mukaisesti päätöksentekijät viittaavat tässä niin strategisen kuin taktisenkin tason tietoturvaraportoinnin yleisöön, josta kirjoitetaan tarkemmin kappaleessa 4.3.2. Päätöksentekijöillä viitataan tässä siis ylimmän johdon lisäksi henkilöihin, joille johto on määrittänyt vastuita tietoturvallisuudesta.

3 Tietoturvallisuuden hallinta

Verkottunut ja yhä digitalisoituva yhteiskunta on haavoittuva. Monimuotoistuvat tietoturvauhat ja niihin vastaaminen voivat aiheuttaa kaikenkokoisissa organisaatioissa hämmennystä. Onneksi organisaatioiden ei tarvitse keksiä pyörää uudelleen, vaan ne voivat hyödyntää tietoturvallisuutensa varmistamisessa ja kehittämisessä alan parhaita käytäntöjä. Standardit kokoavat yhteen nämä parhaat käytännöt, kuten yhteisesti sovitut vaatimukset ja suositukset (SFS 2024a). Tässä luvussa perehdytään tarkemmin tietoturvallisuuteen, tietoturvallisuuden hallintajärjestelmään sekä ISO/IEC 27001 -standardiin, joka käsittelee tietoturvallisuuden johtamista ja hallintaa.

3.1 Tietoturvallisuus

Klassisen määritelmän mukaan tietoturvallisuus koostuu hallinnollisista, teknisistä ja muista järjestelyistä, joilla varmistetaan tiedon luottamuksellisuus (engl. *Confidentiality*), eheys (engl. *Integrity*) ja saatavuus (engl. *Availability*) (Kokonaisturvallisuuden sanasto 2017, 35). Tätä kutsutaan usein tietoturvan CIA-malliksi. Esimerkkejä tietoturvajärjestelyistä ovat kulunvalvonta, asiakirjojen turvallinen säilytys ja hävittäminen, varmuuskopiointi sekä virustorjuntaohjelman ja palomuurin käyttö (Kokonaisturvallisuuden sanasto 2017, 35).

Luottamuksellisuus tarkoittaa sitä, että tieto on saatavilla vain niille, joilla on siihen oikeus (Alexander & Panguluri 2016, 22), eikä kukaan ulkopuolinen pääse siihen käsiksi (Kokonaisturvallisuuden sanasto 2017, 35). Eheydellä puolestaan viitataan siihen, että tieto säilyy alkuperäisenä ja muuttumattomana (Kokonaisturvallisuuden sanasto 2017, 35). Esimerkiksi tiedon muuttuminen vahingossa tai luvaton tahallinen muuttaminen vaikuttavat kielteisesti sen eheyteen (Alexander & Panguluri 2016, 23). Saatavuus taasen takaa, että tietoa voidaan hyödyntää haluttuna aikana (Kokonaisturvallisuuden sanasto 2017, 35). Saatavuus tarkoittaa toisin sanoen luotettavaa ja oikea-aikaista pääsyä tietoon niille henkilöille, joilla on siihen oikeus (Alexander & Panguluri 2016, 23).

Tietoturvallisuuden klassista määritelmää on arvosteltu siitä, ettei siinä huomioida esimerkiksi tiedon alkuperää. Siksi siihen on ehdotettu lisäyksiä, kuten aitous (engl. *Authenticity*), joka tarkoittaa, että tiedon alkuperä voidaan todentaa. Olemassaolon todiste (engl. *Proof of Existence*) taas on aikaviite, joka osoittaa, milloin tieto on ollut olemassa. Kiistämättömyys (engl. *Non-Repudiation*) puolestaan estää tiedon laatijaa tai lähettäjää kiistämästä, että hän on tiedon alkuperäinen laatija tai lähettäjä. (Vigil ym. 2015, 17.) Tässä opinnäytetyössä tietoturvallisuuden määritelmäksi riittää perinteinen CIA-malli, jota ISO/IEC 27001 -standardi käyttää.

3.2 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallinta on käytännössä tietoturvan suunnittelemista, toteuttamista, ylläpitämistä, arvioimista ja kehittämistä. Organisaatio voi hallita tietoturvallisuuttaan tehokkaasti esimerkiksi tietoturvallisuuden hallintajärjestelmän avulla. Tietoturvallisuuden hallintajärjestelmä on organisaation yleisen johtamisjärjestelmän osa, jonka tarkoituksena on luoda, toteuttaa, seurata, arvioida, ylläpitää ja parantaa tietoturvaa. Hallintajärjestelmä on politiikkojen, menettelyjen, prosessien ja niihin liittyvien resurssien kehys, joka pyrkii varmistamaan, että organisaatio saavuttaa tavoitteensa. (Campbell 2016, 12–13.) Siispä tietoturvallisuuden hallintajärjestelmän tulee olla linjassa organisaation strategian kanssa. Lisäksi sen tulisi olla hyvin dokumentoitu (Alexander 2013, 32). Yleensä tietoturvallisuuden hallintajärjestelmän lähestymistapa tietoturvallisuuteen on organisaation tietoturvallisuuteen liittyvien riskien hallitseminen (Campbell 2016, 42).

Tietoturvallisuuden hallinnassa hyvänä käytäntönä pidetään tietoturvallisuuden hallintajärjestelmän luomista siten, että se perustuu johonkin asiaankuuluvaan standardiin, kuten ISO/IEC 27001 (Campbell 2016, 42; Alexander ym. 2013, 7). ISO/IEC 27000 -standardisarjassa, johon ISO/IEC 27001 kuuluu, määritellään tietoturvallisuuden hallintajärjestelmän käsittävän toimintaperiaatteet, menettelytavat, ohjeet, resurssit ja toiminnot organisaation tieto-omaisuuden suojaamiseksi. Standardisarjan mukainen tietoturvallisuuden hallintajärjestelmä perustuu riskeihin ja niiden hallitsemiseen, ja sen pääasiallisena tehtävänä on tukea organisaation

liiketoimintatavoitteiden saavuttamista. (ISO/IEC 27000:2020, 16.) Tietoturvallisuuden hallintajärjestelmän täytyy syntyä kunkin organisaation omista yksilöllisistä tarpeista, mikä tarkoittaa, että hallintajärjestelmän vaatimusten toteuttamistapa määräytyy organisaation koon, rakenteen, tavoitteiden, turvallisuusvaatimusten ja liiketoiminnan prosessien mukaan (ISO/IEC 27000:2020, 18).

3.3 Standardi ISO/IEC 27001

ISO/IEC 27000 on kansainvälisesti tunnettu tietoturvallisuuden johtamisen ja hallinnan standardisarja. Sen on luonut standardointijärjestö International Organisation for Standardisation (ISO) ja International Electrotechnical Commission (IEC) (Disterer 2013, 92). Suomenkielisestä versiosta vastaa Suomen Standardit ry SFS, joka tunnetaan myös nimellä Suomen Standardisoimisliitto (SFS 2023). ISO/IEC 27001 on perusosiltaan yhdenmukainen muiden ISO-standardien, kuten ISO 31000 (riskienhallinta), ISO 9001 (laatujärjestelmät) ja ISO 14001 (ympäristöjärjestelmät), kanssa. Se tarkoittaa, että eri ISO-standardien mukaiset hallintajärjestelmät on helppo sovittaa yhteen.

Standardisarja ISO/IEC 27000 sisältää joukon standardeja, joiden tavoitteena on tarjota hyviä toimintatapoja tietoturvallisuuden hallintajärjestelmän käyttöönottoon, ylläpitoon ja hallinnointiin. ISO/IEC 27000 esittää yleiskuvauksen tietoturvallisuuden hallintajärjestelmästä sekä sanaston (ISO/IEC 27000:2020). ISO/IEC 27001 puolestaan asettaa vaatimukset tietoturvallisuuden hallintajärjestelmän luomiselle, toteuttamiselle, ylläpidolle ja jatkuvalle parantamiselle (ISO/IEC 27001:2022), ja se on niin sanotusti päästandardi (SFS 2023). Sitä täydennetään erilaisilla yksittäisillä ohjeilla ja toimialakohtaisilla standardeilla (ISO/IEC 27000:2020, 24). Tämän työn näkökulmasta ohjestandardeista olennaisin on ISO/IEC 27004, joka opastaa tietoturvallisuuden hallintajärjestelmän seurantaa, mittaamista, analysointia ja arviointia (ISO/IEC 27004:2016).

ISO/IEC 27001 on standardisarjan päästandardi, koska se on sarjan osista ainoa, johon voi sertifioitua. Vaikka opinnäytetyön kirjoitushetkellä ei ole varmaa, edellytetäänkö Väylävirastolta varsinaista ISO/IEC 27001 -sertifikaattia, on hyvä määritellä lyhyesti, mitä sertifikaatilla oikeastaan tarkoitetaan. Sertifikaatti osoittaa, että organisaation tietoturvallisuuden prosessit ja hallintakeinot on toteutettu standardin vaatimusten mukaisesti (Alexander ym. 2013, 76). Sen saaminen edellyttää valtuutetun kolmannen osapuolen tekemän sertifiointimenettelyn läpäisemistä (Disterer 2013, 97). Sertifiointimenettely tarkoittaa käytännössä auditointia eli määrämuotoista riippumatonta arviointia (Alexander ym. 2013, 76). Auditoijat pyrkivät varmentamaan, että vaaditut tietoturvallisuuden prosessit ja hallintakeinot ovat käytössä, kuten organisaatio on ne dokumentoinut. Jos organisaatio saa sertifikaatin, on se kerrallaan voimassa kolme vuotta. Standardin vaatimusten noudattaminen ja tietoturvallisuuden

hallintajärjestelmän jatkuva parantaminen kuitenkin varmistetaan vuosittaisella seurannalla. (Disterer 2013, 97.)

Tietoturvallisuuden hallintajärjestelmä voi auttaa organisaatiota täyttämään lakisääteiset velvoitteensa, hallitsemaan riskejä, suojaamaan tietojansa ja tietojärjestelmiänsä sekä osoittamaan muun muassa sidosryhmille sitoutumisensa tietoturvaan. Hyödyt ovat pitkälti seurausta tietoturvariskien vähentymisestä. (ISO/IEC 27000:2020, 23.) Vaikka organisaatio ei muodollisesti sertifioisi tietoturvallisuuden hallintajärjestelmäänsä, on ISO/IEC 27001 -standardin mukaisen hallintajärjestelmän toteutus sille todennäköisesti eduksi.

3.3.1 Pakolliset vaatimukset

ISO/IEC 27001 -standardi jakautuu kahteen osaan. Ensimmäisessä osassa esitetään pakolliset vaatimukset luvuissa 4–10. Vaatimukset liittyvät tietoturvallisuuden hallintajärjestelmän luomiseen, hallintaan, ylläpitoon ja kehittämiseen (ISO/IEC 27001:2022, 5). Standardin vaatimukset kertovat, mitä tietoturvallisuuden hallintajärjestelmän tulee sisältää. Sertifioinnin näkökulmasta on välttämätöntä, että kaikki vaatimukset toteutuvat organisaation prosesseissa ja toimintatavoissa (ISO/IEC 27001:2022, 6), minkä lisäksi ne on myös dokumentoitu (ISO/IEC 27001:2022, 11). Käytännössä organisaation on pystyttävä esittämään sertifiointiauditoijalle dokumentaation avulla, miten vaatimukset on toteutettu (Disterer 2013, 97).

Standardin pakolliset vaatimukset koskevat toimintaympäristöä (luku 4), johtajuutta (luku 5), suunnittelua (luku 6), tukitoimintoja (luku 7), toimintaa (luku 8), suorituskyvyn arviointia (luku 9) ja parantamista (luku 10) (ISO/IEC 27001:2022, 6–15). Organisaation toimintaympäristö -luvun mukaan organisaation tulee määrittää ne ulkoiset ja sisäiset tekijät, jotka ovat oleellisia organisaation tarkoituksen kannalta, ja jotka vaikuttavat sen edellytyksiin saavuttaa tietoturvallisuuden hallintajärjestelmältään halutut tulokset (ISO/IEC 27001:2022, 6). Johtajuus-luvun mukaan organisaation ylimmän johdon on osoitettava paitsi johtajuutta myös sitoutumista tietoturvallisuuden hallintajärjestelmään (ISO/IEC 27001:2022, 7).

Suunnittelu-luvussa määrätään, että organisaation on suunniteltava tietoturvariskienhallintansa ja asetettava tietoturvatavoitteet (ISO/IEC 27001:2022, 8–10). ISO/IEC 27001 -standardi asettaa riskienhallinnan keskeiseen rooliin tietoturvallisuuden hallintajärjestelmässä. Se vaatii organisaatiota tunnistamaan ja arvioimaan tietoturvariskit sekä suunnittelemaan ja toteuttamaan sopivia riskienhallintatoimenpiteitä. Organisaation on jatkuvasti seurattava ja tarkistettava riskejään, minkä lisäksi sen on parannettava tietoturvallisuuden hallintajärjestelmäänsä tarpeen mukaan. (ISO/IEC 27001:2022.) Tietoturvatavoitteiden on oltava linjassa tietoturvapolitiikan kanssa (ISO/IEC 27001:2022, 10). Ne voivat olla joko strategisia, taktisia tai operatiivisia. Tavoitteet voidaan ilmaista esimerkiksi toivottuna tuloksena, tarkoituksena, toimintakriteerinä tai vaikkapa päämääränä (ISO 27000:2020, 11). Tässä työssä

tavoitteenasetannan lähtökohdaksi on valittu Väyläviraston digitaalisen turvallisuuden periaatteet, jotka asettavat ylätason tavoitteet viraston digitaaliselle turvallisuudelle.

Tukitoiminnot-luvun mukaan organisaation on määriteltävä riittävät resurssit ja pätevyydet sekä huolehdittava riittävästä työntekijöiden tietoisuudesta ja sekä sisäisestä että ulkoisesta viestinnästä. Lisäksi siinä määrätään tietoturvallisuuden hallintajärjestelmän dokumentaatiosta. (ISO/IEC 27001:2022, 10–15.) Toiminta-luvun mukaan organisaation tulee suunnitella, toteuttaa ja ohjata prosessit, joita tarvitaan standardin vaatimusten täyttämiseen (ISO/IEC 27001:2022, 12).

Luku 9 eli suorituskyvyn arviointi on opinnäytetyön kannalta olennainen. Luvussa esitetään vaatimuksia tietoturvallisuuden tason ja tietoturvallisuuden hallintajärjestelmän suorituskyvyn seurannasta, mittaamisesta, analysoinnista ja arvioinnista (ISO/IEC 27001:2022, 13). Seurannan ja mittaamisen avulla varmistetaan, että organisaatio pääsee asettamiinsa tietoturvatavoitteisiin (ISO/IEC 27004:2016, 7). Suorituskykyä täytyy arvioida myös sisäisillä auditoinneilla ja johdon katselmuksilla (ISO/IEC 27001:2022, 13–14). Johdon katselmus -kappaleen mukaan ylimmän johdon on katselmoitava tietoturvallisuuden hallintajärjestelmä suunnitelluin aikavälein. Johdon katselmusten lähtötiedoissa ovat mukana muun muassa seurannan ja mittauksen tulokset. (ISO/IEC 27001:2022, 14.)

Viimeisessä Parantaminen-luvussa puolestaan määrätään jatkuvasta parantamisesta. Organisaation tulee jatkuvasti parantaa tietoturvallisuuden hallintajärjestelmänsä soveltuvuutta, asianmukaisuutta sekä vaikuttavuutta. (ISO/IEC 27001:2022, 14–15.) Jatkuvan parantamisen periaate on siten keskeinen osa ISO/IEC 27001 -standardin lähestymistapaa tietoturvallisuuden hallintaan.

Mainittakoon, että aiemmin ISO/IEC 27001 -standardi sisälsi erityisen vaatimuksen Plan-Do-Check-Act- eli PDCA-mallin käyttämisestä. Mallin Plan-vaiheessa määritellään tietoturvallisuuden hallintajärjestelmän laajuus, tavoitteet ja riskienhallintakeinot (Disterer 2019, 95), mikä vastaa standardin klausuuleja 4-7. Do-vaiheessa toteutetaan suunnitellut politiikat, menettelyt ja hallintakeinot (Disterer 2019, 95), mikä vastaa standardin vaatimuksia luvussa 8. Check-vaiheessa seurataan ja mitataan tietoturvallisuuden hallintajärjestelmän suorituskykyä sekä suoritetaan sisäisiä auditointeja (Disterer 2019, 95), mikä liittyy olennaisesti standardin lukuun 9. Act-vaiheessa analysoidaan edellisen vaiheen tulokset ja tehdään parannustoimenpiteet (Disterer 2019, 95), mikä on ilmaistu luvussa 10. Act-vaiheen suorittamisen jälkeen prosessi alkaa uudelleen Plan-vaiheella (Disterer 2019, 95). Calder (2013, 37) toteaa, että PDCA-malli on edelleen hyvä tapa lähestyä tietoturvallisuuden hallintajärjestelmän toteutusta ja jatkuvaa parantamista. Malli lienee poistettu standardin tuoreimmista versioista, jotta organisaatiot voivat joustavasti valita itselleen sopivimman tavan tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen.

3.3.2 Liite A

ISO/IEC 27001 -standardin toinen osa on Liite A, joka standardin uusimmassa vuoden 2022 versiossa luettelee 93 tietoturvallisuuden hallintakeinoa eli kontrollia (ISO/IEC 27001:2022, 16–23). Hallintakeino (engl. *Control*) tarkoittaa riskiä muuttavaa toimenpidettä eli vaikkapa politiikkaa, laitteita, käytäntöjä tai prosesseja (ISO/IEC 27000:2020, 7). Esimerkiksi tietoturvallisuutta koskevat toimintaperiaatteet, tietoturvakoulutus, kulunvalvonta ja teknisten haavoittuvuuksien hallinta ovat erilaisia liitteessä mainittuja kontrolleja. Hallintakeinot ovat yhteneviä standardin lukujen 5–8 kanssa, ja niitä on käytettävä tietoturvariskien käsittelyyn (ISO/IEC 27001:2022, 16). ISO/IEC 27002 -standardi (2022) tarjoaa tarkempia ohjeita Liite A:n hallintakeinojen täytäntöönpanoon.

Hallintakeinot ovat toimenpiteitä, jotka organisaatio määrittelee ja joiden toteutumista se valvoo. Liite A:ssa ne on jaoteltu neljään kategoriaan: organisaatioturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja teknologinen turvallisuus (ISO/IEC 27001:2022, 16–20). Liite A esittää velvoittavan tietoturvallisuuden hallintakeinojen viiteluettelon, mutta toisin kuin standardin ensimmäisessä osassa esitetyt vaatimukset, organisaation ei tarvitse panna niistä jokaista täytäntöön (ISO/IEC 27002:2022, 9). Listaus on kuitenkin sikäli velvoittava, että organisaation tulee perustella, miksi joku niistä ei ole käytössä. Käytännössä se tarkoittaa, että organisaation osoitettava, ettei kyseinen hallintakeino ole organisaation tietoturvallisuuden hallintajärjestelmälle relevantti. (ISO/IEC 27000:2020, 20–21.) Tässä opinnäytetyössä Liite A toimii osaltaan referenssinä tunnistettujen tietotarpeiden perusteluun.

4 Kokonaiskuva tietoturvallisuudesta

Organisaation on tiedettävä tietoturvallisuutensa taso ja miten hyvin sen tietoturvallisuuden hallintajärjestelmä toimii. Mittaaminen ja raportointi tuottavat tietoa, jota tarvitaan johtamiseen, toiminnansuunnitteluun, häiriötilanteiden hallintaan ja toiminnan kehittämiseen (VAHTI 2016, 61). Tässä luvussa esitellään opinnäytetyön lähestymistapa kokonaiskuvan muodostamiseen tietoturvallisuudesta, mihin mainitut mittaaminen ja raportointi olennaisesti liittyvät.

4.1 Tietoturvallisuuden mittaaminen

Seuranta ja mittaaminen ovat toimenpiteitä, joiden tarkoituksena on tuottaa johdolle ymmärrys siitä, miten tietoturvallisuuden prosessit ja hallintakeinot toimivat (Miller 2022, 139–140). Mittaaminen useimmiten perustuu tietoturvatavoitteisiin tai organisaation merkittävimpiin tietoturvariskeihin, tarkemmin sanottuna muutoksiin niissä (Evesti 2024, suullinen tieto). Tietoturvallisuuden mittaamisella voi olla keskeinen rooli organisaation sisäisen viestinnän ja tietoturvaymmärryksen tarjoamisessa päätöksentekijöille. Mittaamisen avulla saatuja tietoja

voidaan käyttää tietopohjaiseen päätöksentekoon esimerkiksi resurssien allokoimisesta ja riskienhallinnasta. (Schroeder ym. 2024b, 8.)

Brotby & Hinson (2013, 15–26) listaavat lukuisia syitä tietoturvallisuuden mittaamiselle. Ensinnäkin sillä vastataan johdon tarpeeseen tietää, onko organisaatio riittävän suojassa, onko tietoturvariskit käsitelty riittävällä tasolla ja miten organisaatio vertautuu muihin samankaltaisiin organisaatioihin. Lisäksi johdon on tiedettävä, mitkä ovat organisaation vahvuudet ja heikkoudet, kykeneekö organisaatio reagoimaan tietoturvatapahtumiin tehokkaasti ja onko organisaation tietoturvallisuus vaatimustenmukaisella tasolla. Ilman mitattua tietoa tämänkaltaisiin kysymyksiin vastaaminen on haastavaa.

Toinen syy tietoturvallisuuden mittaamiselle on tietysti tietoturvallisuuden systemaattinen parantaminen. Liiketoiminnan ja tietoturvallisuuden integroiminen, riskienhallinnan kehittäminen ja hallintakeinojen päivittäminen ovat muutamia esimerkkejä siitä, miten mittaamisen avulla voidaan parantaa tietoturvallisuutta. (Brotby & Hinson 2013, 19–21.)

Kolmas syy mitata tietoturvallisuutta on sen strateginen, taktinen ja operatiivinen merkitys. Tietoturvallisuuden mittaaminen tukee strategista päätöksentekoa, nimittäin mittaamisen avulla saatava tieto tukee tietoturvallisuuden ja laajemmin organisaation liiketoiminnan pitkän aikavälin suunnittelua ja hallintaa. Taktista päätöksentekoa tietoturvallisuuden mittaaminen tukee, kun se vastaa kysymyksiin siitä, mitä organisaatiossa tulisi ottaa huomioon seuraavien viikkojen ja kuukausien aikana tietoturvaan ja siihen liittyvien kehitysprojektien näkökulmasta. Taktisen tason tavoitteena on varmistaa, että toiminta etenee oikeaan suuntaan strategisten päämäärien saavuttamiseksi ja että sitä varten on käytettävissä tarvittavat resurssit. (Brotby & Hinson 2013, 19–21.)

Operatiivisella tasolla tietoturvallisuuden mittaaminen tukee päätöksentekoa vastaamalla kysymyksiin, mitä tehtäviä tietoturvasta vastaavien asiantuntijoiden tulee suorittaa tulevina tunteina tai päivinä sekä miten ne tulisi priorisoida ja toteuttaa. (Brotby & Hinson 2013, 19–21.) Operatiivinen taso on opinnäytetyön rajauksen ulkopuolella, mutta sitä ei kuitenkaan voi täysin sulkea pois, koska operatiivisella tasolla tapahtuvat asiat voivat saada taktisia tai jopa strategisia merkityksiä. Esimerkiksi operatiivisella tasolla voidaan huomata, että tietojärjestelmään kohdistuu toistuvia tietomurtoyrityksiä, jotka vaativat ICT-tiimiltä jatkuvia korjaustoimenpiteitä ja lisävalvontaa. Tämä operatiivinen ongelma saa taktisen merkityksen, kun organisaatiossa päätetään vaikkapa suorittaa säännöllisiä tietoturva-auditointeja ja kouluttaa henkilöstöä tunnistamaan tietojenkalasteluyritykset. Toisin sanoen operatiivista ongelmaa ratkaistaan tuolloin taktisella tasolla. Sama operatiivinen ongelma voi saada myös strategisen merkityksen, jos organisaation johto päättää esimerkiksi kohdentaa lisää resursseja tietoturvaan.

Neljäs syy tietoturvallisuuden mittaamiselle on Brotbyn & Hinsonin (2013, 22) mukaan vaatimustenmukaisuus ja sen osoittaminen. Tietoturvallisuudelle tulee vaatimuksia paitsi laeista, säädöksistä ja sopimusvelvoitteista myös standardeista, kuten ISO/IEC 27001 -standardista. Tietoturvamittarit tarjoavat todistusaineistoa auditoijille siitä, että organisaation tietoturva- ja riskienhallintakäytännöt ovat kunnossa.

4.2 Standardi ISO/IEC 27004

ISO/IEC 27001 -standardin mukaisen tietoturvallisuuden hallintajärjestelmän pääasiallinen tavoite on tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen. Yksin tietoturvallisuuden hallintajärjestelmän luominen ja ylläpito ei riitä takaamaan, että hallintajärjestelmä saavuttaa sille määritellyt tavoitteet. Sen vuoksi standardin luvussa 9 määrätään tietoturvallisuuden hallintajärjestelmän suorituskyvyn arvioinnista (ISO/IEC 27004 2016, 7).

Standardisarjan osa ISO/IEC 27004 ohjeistaa organisaatioita ISO/IEC 27001 -standardin kohdan 9.1 vaatimusten täyttämisessä (ISO/IEC 27004:2016, 5). Mainitussa standardin kohdassa 9.1 esitetään vaatimuksena, että organisaatioiden on määritettävä seuraavat asiat: mitä tietoturvallisuuden hallintajärjestelmässä seurataan ja mitataan, mitä seuranta-, mittaus-, analysointi- ja arviointimenetelmiä käytetään, milloin seuranta ja mittaus tehdään, milloin tuloksia on analysoitava ja arvioitava, ketkä tekevät seurannan ja mittauksen sekä ketkä analysoivat ja arvioivat saadut tulokset. Valituilla menetelmillä tulisi saada vertailtavia ja toistettavissa olevia tuloksia. Lisäksi organisaatioiden on säilytettävä dokumentoitua tietoa seurannan ja mittaamisen tuloksista. (ISO/IEC 27001:2022, 13.)

Tiivistetysti ISO/IEC 27004 -standardin tarkoituksena on auttaa organisaatioita mittaamaan, raportoimaan ja siten systemaattisesti parantamaan tietoturvallisuuden hallintajärjestelmiään (Brotby & Hinson 2013, 43). Onkin syytä määritellä, mitä mittareilla ja mittaamisella tarkoitetaan. Mittari on muuttuja, joka saa jonkun arvon mittauksen tuloksena. Mittaus on prosessi, jossa tuo arvo määritellään. (ISO/IEC 27000:2020, 11.) Tietoturvallisuuden mittarit voivat olla niin määrällisiä kuin laadullisiakin (Digi- ja väestötietovirasto 2021, 17).

ISO/IEC 27004 -standardissa on kolme liitettä. Liite A opastaa tietoturvallisuuden mittausmallista, Liite B antaa lukuisia mittariesimerkkejä ja Liite C puolestaan antaa esimerkin vapaassa tekstimuodossa olevan mittarin määrittelemisestä. (ISO/IEC 27004:2016, 6.)

4.2.1 Tietotarpeiden tunnistaminen

Opinnäytetyön ytimessä on ISO/IEC 27001 -standardin 9.1 a-kohta. Sen mukaan organisaation on määritettävä, mitä seurata ja mitata tietoturvallisuuden hallintajärjestelmässä (ISO/IEC 27001:2022, 13). Mittareiden kehitys alkaakin tietotarpeiden tunnistamisella (ISO/IEC 27004:2016, 14). Tietotarve viittaa tarpeeseen saada jostakin aiheesta tietoa, joka on

oleellista jollekin henkilölle tai organisaatiolle. Tietotarve kuvaa sitä, millaista tietoa henkilö tai organisaatio tarvitsee päätöksenteon tueksi, jotta kyseinen henkilö tai organisaatio voi saavuttaa tavoitteensa tai hallita riskejään ja ongelmiaan (ISO/IEC 27000:2020, 9). Vasta tietotarpeiden tunnistamisen jälkeen organisaatio voi päättää, millä mittareilla kuhunkin tietotarpeeseen vastataan (ISO/IEC 27004:2016, 5).

ISO/IEC 27004 -standardi toteaa, että mahdollisia seurattavia järjestelmiä ja prosesseja on paljon. Niitä ovat esimerkiksi tietoturvallisuuden hallintajärjestelmän prosessien toteutus, tietoturvahäiriöiden hallinta, haavoittuvuuksien hallinta, tietoturvatietoisuus ja -koulutus, auditointi, riskienhallinta, liiketoiminnan jatkuvuudenhallinta ja fyysisen turvallisuuden hallinta. Seurantatoiminnot tuottavat dataa, kuten vaikkapa lokeja tai koulutustilastoja, joita voidaan käyttää mittarien lähteenä. (ISO/IEC 27004:2016, 9.) Samoin mahdollisia mitattavia tietoturvallisuuden hallintajärjestelmän prosesseja on paljon. Niitä ovat esimerkiksi suunnittelu, johtajuus, riskienhallinta, viestintä, dokumentointi ja auditointi. Tietoturvallisuuden hallintajärjestelmän hallintakeinot, jotka on lueteltu standardin ISO/IEC 27001 Liite A:ssa, ovat niin ikään ilmeisiä mitattavia asioita. Hallintakeinojen tarkoitus on muokata riskiä, joten niiden suhteen mittauksella voidaan esimerkiksi tarkastella, kuinka paljon hallintakeino alentaa jonkin tapahtuman todennäköisyyttä tai lieventää sen seurauksia. (ISO/IEC 27004:2016, 10.)

Koska mitattavia asioita on lähes lukemattomasti, ei ole itsestäänselvyys, mitä niistä kuuluisi mitata. On työlästä, kallista ja jopa haitallista mitata liian monia tai vääriä kohteita. Vaarana on, että keskeiset asiat jäävät varjoon tai tyystin huomaamatta. Niinpä organisaation on päätettävä, mitä se haluaa saavuttaa tietoturvallisuuden hallintajärjestelmän suorituskyvyn ja vaikuttavuuden arvioinnilla (ISO/IEC 27004:2016, 5), eli käytännössä sen on päätettävä, mitä tietoturvallisuuden mittaamisella tavoitellaan (Schroeder ym. 2024b, 9).

Eri ryhmillä on luonnollisesti erilaisia tietotarpeita. Tietoturvallisuuden hallintajärjestelmän toimivuuden ollessa kyseessä nimenomaan johdon tietotarpeet ovat tärkeitä, joten johdon tulee olla mukana prosessissa (ISO/IEC 27004:2016, 18). Tietotarpeet myös vaihtelevat organisaatiosta toiseen, joten kunkin organisaation on löydettävä omat tietotarpeensa. ISO/IEC 27004 (2016, 15) listaa, että tietotarpeet voivat liittyä esimerkiksi sidosryhmien tarpeisiin, organisaation strategiseen suuntaan, tietoturvapolitiikkaan ja -tavoitteisiin tai riskinkäsittelysuunnitelmaan.

Kuten aiemmin todettu, tässä opinnäytetyössä tietotarpeet määritellään Väyläviraston digitaalisen turvallisuuden periaatteiden eli käytännössä tietoturvapolitiikan ja -tavoitteiden kautta. Tietotarpeiden määrittely lähteekin liikkeelle tietoturvallisuuden hallintajärjestelmän ja sen osien tarkastelulla. Siihen kuuluvat luonnollisesti mainitut tietoturvapolitiikka ja -tavoitteet, mutta myös hallintakeinot, vaatimustenmukaisuus (lainsäädäntö ja sopimukset) sekä tietoturvariskien hallintaprosessin tulokset. (ISO/IEC 27004:2016, 15.) Standardi ei määrää,

millä menetelmillä tietotarpeet selvitetään. Eräs keino on haastattelu, jota tässä opinnäytetyössä hyödynnetään.

Kun tietotarpeet on löydetty, ne priorisoidaan eli asetetaan tärkeysjärjestykseen. Priorisoinnin kriteerejä voivat olla vaikkapa riskien hallitseminen, organisaation kyvykkyydet ja resurssit, tietoturvapolitiikka ja -tavoitteet, vaatimustenmukaisuus tai mittauksista saatavien tietojen hyöty suhteessa vaivaan ja kustannuksiin. Priorisoiduista tietotarpeista valitaan sellaiset, joille tarvitaan mittaustoimintoja, minkä jälkeen valitut tietotarpeet dokumentoidaan ja viestitään olennaisille tahoille. (ISO/IEC 27004:2016, 15.) Yksittäinen tietotarve saattaa vaatia useampia eri mittareita (ISO/IEC 27004:2016, 17).

4.2.2 Suorituskyky ja vaikuttavuus

Tietotarpeiden tunnistamisen ja priorisoinnin jälkeen ISO/IEC 27004 ohjeistaa mittarien luomisesta ja ylläpitämisestä, mikä menee tämän opinnäytetyön rajauksen ulkopuolelle. Mainittakoon kuitenkin, että mittarityyppejä on standardin mukaan kahdenlaisia: suorituskykymittarit ja vaikuttavuusmittarit. ISO/IEC 27000 -standardisarjassa puhutaan toisinaan hieman ristiin tietoturvallisuuden hallintajärjestelmän suorituskyvystä, vaikuttavuudesta ja tehokkuudesta. Käsitteet toki liittyvät läheisesti toisiinsa, koska kaikki niistä kuvaavat tietoturvallisuuden hallintajärjestelmän toimivuutta, mutta niiden välillä on määritelmällisiä eroja.

Suorituskyky (engl. *Performance*) viittaa siihen, kuinka hyvin tietoturvallisuuden hallintajärjestelmä toimii eli suorittaa suunnitellut toimet. Suorituskykymittarit kertovat tulokset suunniteltujen toimintojen ominaisuuksina. (ISO/IEC 27004:2016, 12.) Yksinkertainen esimerkki suorituskykymittarista on organisaation henkilöstölleen tarjoaman tietoturvakoulutuksen läpäisyprosentti. Muita suorituskykymittareita ovat muun muassa henkilömäärä, välitavoitteiden saavuttaminen tai tietoturvallisuuden hallintakeinojen toteutustaso (ISO/IEC 27004:2016, 12).

Vaikuttavuus (engl. *Effectiveness*) taas tarkastelee, kuinka hyvin tietoturvallisuuden hallintajärjestelmä saavuttaa toivotut tulokset. Toisin sanoen vaikuttavuus tarkoittaa sitä, missä määrin suunnitellut toimet toteutetaan ja millaisia tuloksia ne tuottavat (ISO/IEC 27000:2020, 8). Näin ollen vaikuttavuusmittarit kertovat, kuinka suunniteltujen toimien toteutuminen vaikuttaa organisaation tietoturvatavoitteiden saavuttamiseen. Esimerkiksi organisaation tavoitteena voi olla kasvattaa henkilöstönsä tietoturvatietoisuutta. Toimena se voi järjestää henkilöstölleen tietoturvakoulutuksen. Mitä todennäköisimmin organisaatio on kiinnostunut siitä, missä määrin koulutuksen osallistujat ymmärsivät koulutuksen sisällön ja kykenevät soveltamaan oppimiaan asioita käytäntöön. Tällöin on kyseessä vaikuttavuuden arviointi, jota mitataan vaikuttavuusmittarein. (ISO/IEC 27004:2016, 13.)

Tehokkuus liittyy oletettavasti siihen, kuinka resurssitehokkaasti tai taloudellisesti tietoturvallisuuden hallintajärjestelmä pystyy saavuttamaan tavoitellun suorituskyvyn ja

vaikuttavuuden (Such ym. 2016). ISO/IEC 27004 -standardissa ei kuitenkaan puhuta erikseen tehokkuusmittareista, eikä tehokkuutta määritellä erikseen ISO/IEC 27000 -standardissakaan, vaikka standardisarjassa tehokkuus toisinaan mainintaankin (ks. esim. ISO/IEC 27000:2020, 18).

Tämän työn kannalta on olennaista huomioida, ettei ISO/IEC 27000 -standardiperhe määrittele käsitettä "toimivuus" tietoturvallisuuden hallintajärjestelmän kontekstissa. Sen sijaan se puhuu suorituskyvyn ja vaikuttavuuden arvioinnista. ISO/IEC 27001 -standardin luku 9 on otsikoitu "Suorituskyvyn arviointi". Kuitenkin samassa luvussa kirjoitetaan myös vaikuttavuuden arvioinnista (ks. esim. ISO/IEC 27001:2022, 13). Näitä kahta tekijää - suorituskykyä ja vaikuttavuutta - tulee standardin mukaan seurata, mitata, analysoida ja arvioida. Opinnäytetyössä ajatellaan, että suorituskyky ja vaikuttavuus muodostavat yhdistelmän, jota voidaan kutsua toimivuudeksi. Koska opinnäytetyössä ei vielä luoda suorituskyky- ja vaikuttavuusmittareita, ei tietotarpeitakaan ole tarpeen erotella tällä jaolla. Opinnäytetyössä riittää ajatus tietoturvallisuuden hallintajärjestelmän toimivuudesta, joka pohjautuu käsitteisiin suorituskyvystä ja vaikuttavuudesta.

4.3 Tietoturvaraportointi

Lukemattomissa organisaatioissa tietoturvaraportointi perustuu raakadatalle, jota saadaan muun muassa palomuureista, roskapostisuodattimista ja virustorjuntajärjestelmistä. Sen sijaan huomiotta jäävät monet ei-tekniset tekijät, jotka ovat yhtä tärkeitä tietoturvallisuuden hallinnassa. (Brotby & Hinson 2013, 3–4.) ISO/IEC 27001 -standardi pyrkii taklaamaan tätä ongelmaa määräämällä tietoturvallisuuden hallintajärjestelmän suorituskyvyn ja vaikuttavuuden arvioinnista (ISO/IEC 27001:2022, 13). Raportoinnin tarkoituksenahan on kuitenkin tuottaa päätöksentekijöille kokonaiskuva, jotta heillä on tarvittavat tiedot tietoturvallisuutta koskevien päätösten tekemiseksi.

4.3.1 Kokonaiskuvan muodostaminen

Kokonaiskuvaa voidaan lähestyä täsmällisemmin tilannekuvan ja tilannetietoisuuden käsitteiden avulla. Vaikka käsitteet usein viittaavat erityisesti häiriötilanteisiin (Yhteiskunnan turvallisuusstrategia 2017), voidaan niitä soveltaa myös raportoinnin kontekstissa. Tilannekuva tarkoittaa tilanteesta tai suorituskyvystä tehtyä esitystä, joka koostuu jonkun tarpeen perusteella valituista yksittäisistä tiedoista (Horsmaheimo ym. 2017, 119). Horsmaheimo ym. (2017, 44–45) löysivät tutkimuksessaan yleisiä edellytyksiä hyvälle tilannekuvalle. Heidän mukaansa tilannekuvan esitysmuodolla ei sinänsä ole väliä, vaan ennemmin sillä, että joku hallinnoi sitä johdonmukaisesti. Tieto tilannekuvaa varten tuotetaan yhteistyönä niin, että jokainen toimija vastaa oman osaamisalueensa tiedon tuottamisesta. Olennaista on, että tieto on systemaattisesti prosessoitua, analysoitua ja ymmärrettävää. Tiedon on oltava

merkityksellistä ja hyödyllistä kohderyhmälle, minkä lisäksi sen tulisi olla esitetty helposti tulkittavassa muodossa (Schroeder ym. 2024a, 14).

Tilannetietoisuus puolestaan perustuu tilannekuvalle. Tilannetietoisuus (engl. *Situational Awareness*) viittaa päätöksentekijöiden ja heitä mahdollisesti avustavien henkilöiden ymmärrykseen tapahtuneista asioista, niihin vaikuttaneista olosuhteista, eri osapuolten tavoitteista ja tapahtumien potentiaalisista kehitysvaihtoehdoista. (Horsmaheimo ym. 2017, 119.) Tilannetietoisuus muodostuukin kolmesta kerroksesta: tilanteen osien hahmottamisesta, nykytilanteen ymmärtämisestä ja tulevaisuuden arvioinnista (Horsmaheimo ym. 2017, 10). Kaikkia näitä asioita tarvitaan tietopohjaiseen päätöksentekoon.

Tilannekuvan tuottaminen ja raportointi tarjoavat tarvittavat tiedot ja työkalut tilannetietoisuuden luomiselle. Horsmaheimo ym. (2017, 44–45) jatkavat, että itsessään tilannekuvan raportoimisella ei ole arvoa, ellei se johda toimenpiteisiin. Tilannekuvan tuleekin olla suunnattu sellaiselle taholle, jolla on valmiudet ja resurssit tehdä ja toimeenpanna päätöksiä. Tarkoitustaan palvelevan raportoinnin turvaamiseksi myös raportoinnissa käytettävät tietoturvamittarit on tarkoituksenmukaista räätälöidä yleisölle (Evesti 2023), sillä tietotarpeet ovat eri organisaatiotasoilla erilaiset. Ylimmän johdon tietotarpeet ovat erilaisia kuin vaikkapa järjestelmävastaavan (ISO/IEC 27004:2016, 17).

4.3.2 Tietoturvaraportoinnin yleisöt ja sisällöt

Tietoturvaraportointi on osa organisaatioiden tietoturvallisuuden hallintaa. Se voidaan jakaa strategiseen, taktiseen ja operatiiviseen tietosisällön, kohderyhmän, aikasyklin ja tarkoituksensa mukaan. Tiivistetysti strateginen raportointi keskittyy johdon päätöksenteon tukemiseen ja pitkän aikavälin tavoitteisiin. Taktinen raportointi palvelee organisaation tietoturvallisuuden hallintaa ja kehittämistä, ja se keskittyy esimerkiksi projektien ja prosessien edistymiseen. Operatiivinen raportointi taas käsittelee päivittäisiä tietoturva-asioita, kuten tietoturvatapahtumien ja poikkeamien seurantaa. (Evesti 2023.)

Strategisen tietoturvaraportoinnin kohdeyleisö on ylin johto, joka tarvitsee korkean tason yhteenvetoja strategisten päätösten tekemistä varten. He keskittyvät vaatimustenmukaisuuteen, riskien asianmukaiseen hallintaan ja sen varmistamiseen, että tietoturvapolitiikka ja siihen liittyvät käytännöt ovat linjassa muiden liiketoimintastrategioiden kanssa. Ylimmän johdon tietotarpeet ja vaatimukset tietoturvamittareille liittyvät tietoon, joka tarjoaa kokonaiskuvan ilman syventymistä yksityiskohtiin. Tämä tarkoittaa sitä, että raportoinnin olisi kyettävä luomaan yleiskuva siitä, miten tietoturvapolitiikat pannaan käytäntöön ja miten hyvin organisaatiossa noudatetaan näitä politiikkoja. Lisäksi heidän on ymmärrettävä nykyinen riskitilanne ja sen hallintaan liittyvät toimenpiteet. Lähtökohtaisesti ylintä johtoa pidetään vastuullisena vakavista laiminlyönneistä tai rikkomuksista, joten ylimmän johdon intresseissä on, että raportointi muilta organisaation tasoilta toimii. (Brotby & Hinson 2013, 53.)

Taktisen tietoturvaraportoinnin kohdeyleisö on keskijohto, tietoturvatiimi ja ICT-osasto. He tarvitsevat tietoa, joka auttaa heitä valvomaan ja johtamaan tietoturvapolitiikkojen ja toimenpiteiden toimeenpanoa (Brotby & Hinson 2013, 54–55). Brotbyn & Hinsonin (2013, 54–55) mukaan he ovat erityisen kiinnostuneita niin tietoturvatoimenpiteiden tehokkuudesta kuin niiden operatiivisesta vaikuttavuudestakin. Se tarkoittaa, että he tarvitsevat mittareita, jotka tarjoavat näkymää siihen, toimivatko tietoturvallisuuden hallintakeinot toivotulla tavalla ja kuinka ne vaikuttavat päivittäiseen toimintaan. Esimerkiksi he voivat olla kiinnostuneita siitä, kuinka monia tietoturvatapahtumia havaitaan ja kuinka moniin niistä vastataan ajoissa, kuinka kauan haavoittuvuuksiin reagoimiseen menee tai noudatetaanko organisaatiossa tietoturvakäytäntöjä. Lisäksi he tarvitsevat tietoa kehityskohteista ja potentiaalisista riskeistä, jotka voivat vaikuttaa organisaation tietoturvan tasoon. Yhteenvetona Brotby & Hinson (2013, 56) korostavat, että tietoturvamittareiden on oltava relevantteja ja riittävän yksityiskohtaisia, jotta päätöksentekijät saavat selkeän kuvan toiminnan tehokkuudesta, mikä mahdollistaa tietoturvakäytäntöjen jatkuvaan parantamiseen tarvittavat oivallukset.

Operatiivisen tietoturvaraportoinnin kohdeyleisö on operatiivinen johto ja suoraan tietoturvan parissa työskentelevä henkilöstö. Vaikka operatiivinen tietoturvaraportointi ei ole tämän opinnäytetyön keskiössä, on kuitenkin hyvä sanoa muutama sana siitä. Operatiivinen henkilöstö tarvitsee tarkkaa ja yksityiskohtaista tietoa päivittäisten tehtäviensä suorittamiseksi. He keskittyvät erityisesti teknisiin tietoturvakontrolleihin, niiden yksityiskohtiin ja siihen, kuinka hyvin ne toimivat reaaliajassa. He tarvitsevatkin tietoa järjestelmien ja laitteiden tilasta sekä käynnissä olevista tietoturvahyökkäyksistä. Tällaisen tiedon avulla operatiivinen henkilöstö voi tunnistaa ja reagoida mahdollisiin uhkiin nopeasti, varmistaa tietoturvakontrollien asianmukaisen toiminnan ja ylläpitää organisaation tietoturvan tasoa. (Brotby & Hinson 2013, 54–55.)

Raportointia koostaessa on pohdittava, mitkä tietotarpeet ja niihin vastaavat mittarit kertovat täsmällistä tarinaa organisaation kohtaamista riskeistä ja mitkä asiat ovat merkityksellisiä ja ymmärrettäviä raportoinnin yleisölle. Kuten todettu, raportoinnin aiheet myös kumpuavat kunkin organisaation yksilöllisistä tarpeista. (Schroeder ym. 2024b, 9.)

5 Kehittämistyön menetelmä ja prosessi

Opinnäytetyö on muodoltaan kehittämistyö, ja sen kysymyksenä on, mitä tietoa Väyläviraston päätöksentekijät tarvitsevat kokonaiskuvan muodostamiseksi tietoturvallisuuden hallintajärjestelmän toimivuudesta. Tavoitteena on laatia ehdotus tietotarpeista, joiden avulla tietoturvallisuuden hallintajärjestelmän suorituskykyä ja vaikuttavuutta voidaan seurata ja mitata sekä raportoida. Esitettyyn kysymykseen etsitään vastauksia teemahaastattelujen avulla.

Tiedonkeruumenetelmäksi on valittu teemahaastattelu, koska aikomuksena on saada hyödynnettyä toimeksiantajan henkilöstön ammattitaitoa laajasti. Haastattelun avulla saadaan syvällistä ja monipuolista tietoa, minkä lisäksi menetelmä tuo esiin yksilöiden erilaiset käsitykset ja kokemukset aihepiiristä. Teemahaastattelulle ominaista on, että haastattelija on perehtynyt kirjallisuuteen ja tutkimukseen tarkasteltavasta aiheesta ja näin ollen selvittänyt ennakkoon siihen liittyvät rakenteet ja prosessit. Haastattelija on etukäteen valinnut teemat, joiden mukaan haastattelu etenee. Haastateltavia kannustetaan tarkentavien kysymysten avulla puhumaan aihepiiristä varsin vapaasti. (Puusa & Juuti 2022.)

Teemat, joita haastatteluissa käsiteltiin, olivat Väyläviraston digitaalisen turvallisuuden periaatteiden mukaiset: tunnistaminen, suojaaminen, havainnointikyky ja reagointi. Lisäksi yhtenä käsiteltävänä teemana oli johdon raportointi. Haastattelut vaihtelivat hieman sisällöllisesti, vaikka kunkin ryhmän välillä haastattelun runko oli samankaltainen. Yksittäinen haastattelu saattoi painottua joko digitaalisen turvallisuuden periaatteisiin tai strategiseen ja taktiseen tietoturvaraportointiin. Haastatteluiden välillä kysymyksiä muokattiin niin, että edeltävistä haastatteluista saatua tietoa hyödynnettiin seuraavissa haastatteluissa. Tällä tavoin toimimalla onnistuttiin välttymään turhalta toistolta ja saamaan esiin uusia näkökulmia. Kaikki haastattelukysymykset olivat avoimia, ja haastateltavia kannustettiinkin keskusteluun.

Haastattelut toteutettiin yksilöhaastatteluina. Haastatellut henkilöt voidaan jakaa karkeasti kolmeen ryhmään: asiantuntijataso, yksikön tai osaston päällikkö/johtotaso (tässä: keskijohto) sekä ylin johto. Kustakin ryhmästä haastateltiin 2–5 henkilöä siten, että henkilöiden kompetenssit kattoivat joko jonkin tietoturvallisuuden näkökulman (asiantuntijat), raportoinnin (ylin johto) tai molemmat (keskijohto). Haastateltaville oli etukäteen lähetetty Digitaalisen turvallisuuden vuosiraportti 2022 sekä Q1 väliraportti vuodelta 2023. Heillä oli halutessaan mahdollisuus tutustua niihin etukäteen, mutta sitä ei velvoitettu. Saateviestissä heille kerrottiin opinnäytetyöstä yleisellä tasolla, kuten kehittämistyön tarkoituksesta ja haastattelun teemoista. Lisäksi heille kerrottiin eettisistä periaatteista, kuten heidän oikeudestaan vetäytyä prosessista koska tahansa ja siitä, että vastauksia käsittelee ainoastaan opinnäytetyöntekijä luottamuksellisesti. Kullekin haastattelulle oli varattu aikaa 50 minuuttia, mutta osaa haastateltavista haastateltiin kahdesti ajan loppumisen vuoksi. Kaikki haastattelut nauhoitettiin, ja materiaalia kertyi yhteensä miltei 13 tuntia. Tämän jälkeen aineisto litteroitiin asiasisältötasolla eli haastattelunauhoitteet purettiin muistiinpanoiksi suurpiirteisesti referoiden.

Analyysiprosessin ensimmäisessä vaiheessa aineiston asiasisällöt jäsentyivät varsin luonnollisesti haastattelurungon teemojen alle. Toisessa vaiheessa ensimmäisen vaiheen tuottamia havaintoja peilattiin opinnäytetyön tietoperustaan eli ISO/IEC 27001 ja 27004 -standardeihin. Tietotarpeiden muotoilun kannalta erityisesti ISO/IEC 27004 -standardin Liite B oli avuksi, nimittäin oli hyödyllistä verrata saatua aineistoa esimerkkimittareihin ja noiden esimerkkimittareiden tietotarpeisiin. Tässä vaiheessa syntyi taulukko, jossa jokaisen haastatellun henkilön

esiin nostamat seikat muotoiltiin tietotarpeiksi kunkin digitaalisen turvallisuuden periaatteen alle. Lisäksi taulukossa oli oma sarakkeensa huomioille johdon tietoturvaraportoinnista.

Kolmannessa vaiheessa kullekin digitaalisen turvallisuuden periaatteelle luotiin oma taulukko, johon tietotarpeet tiivistettiin. Johdon raportointi -teema kirjoitettiin auki väliraportoinnin ja vuosiraportoinnin otsikoiden alle. Lopulta tietotarpeet myös linkitettiin ISO/IEC 27001 -standardiin ja sen Liite A:n hallintakeinoihin, mikä avaa ja perustelee kutakin tietotarvetta. Seuraavassa luvussa esitellään analysoidut tulokset.

6 Tulokset

Tässä luvussa esitetään ehdotukset tietotarpeista, joiden avulla Väyläviraston tietoturvallisuuden hallintajärjestelmän suorituskykyä ja vaikuttavuutta voidaan seurata ja mitata sekä raportoida. Tietotarpeisiin vastaamalla Väyläviraston päätöksentekijät saavat muodostettua kokonaiskuvan Väyläviraston tietoturvallisuuden hallintajärjestelmän toimivuudesta.

Haastateltuja henkilöitä ei yksilöidä, mutta tuloksissa viitataan muutamiin yksittäisiin haastatteluihin. Esitysmuoto noudattelee Väyläviraston digitaalisen turvallisuuden periaatteita. Tuloksia lukiessa on hyvä huomioida, että osa tietotarpeista voisi kuulua useammankin periaatteen alle, joten tietotarpeen kuuluminen tiettyyn periaatteeseen on osin tulkinnanvaraista. Tietotarpeita myös avataan ja perustellaan viittauksilla ISO/IEC 27001 -standardiin ja Liite A:n hallintakeinoihin. Useat tietotarpeista ovat luonteeltaan sellaisia, että niitä voidaan taustoittaa monen muunkin ISO/IEC 27001 -viitteen avulla, mutta tässä on yritetty valita kyseiseen tietotarpeeseen ja Väyläviraston kontekstiin osuvimmat perustelut. Viittaukset standardin vaatimuksiin on ilmaistu kappalenumeroin, kun taas viittaukset standardin Liite A:n hallintakeinoihin on vakiintuneen tavan mukaan ilmaistu etuliitteellä "A." ennen kyseisen hallintakeinon kappalenumeroa.

Luvussa on myös oma osionsa johdon tietoturvaraportoinnille. Siinä tiivistetään, mitä ajatuksia haastatellut henkilöt toivat esille tietoturvaraportoinnista niin vuosi- (strateginen) kuin väliraportoinninkin (taktinen) näkökulmista. Raportointi on kuitenkin ollut tietotarpeiden muotoilussa jatkuvasti mukana, joten sitä ei täysin voi erottaa tietotarpeista ja niiden perusteluista.

6.1 Tunnistaminen

Taulukko 1 esittää tietotarpeet, jotka on laadittu tunnistaminen-teeman pohjalta. Suojausta vaativien kohteiden (tietojärjestelmät, tietovarannot, tiedot ja tilat) tunnistamiselle on luotu omat prosessinsa virastossa, ja varsinkin tietojärjestelmien hankinnan ja tuotantoon viennin

vaiheissa haastatellut kokivat prosessin toimivan erinomaisesti. Keskustelut painottuivatkin pitkälti kysymykseen tietojen luokittelusta.

Taulukko 1: Tietotarpeet "Tunnistamme suojausta vaativat kohteet, uhat ja riskit"-periaatteesta

Tunnistamme suojausta vaativat kohteet, uhat ja riskit	
Tietotarve	**ISO/IEC 27001 -viite**
Suojausta vaativien kohteiden tunnistaminen	A.5.12 Tiedon luokittelu
Järjestelmien elinkaaren hallinta	A.5.12 Tiedon luokittelu A.5.18 Pääsyoikeudet
Toiminnallisille tietoturvariskeille altistuminen	8.2 Tietoturvariskien arviointi 8.3 Tietoturvariskien käsittely
Ohjeiden katselmointi	A.5.37 Dokumentoidut toimintaohjeet

Kuten hallintakeino A.5.12 toteaa, organisaation tulee luokitella tietonsa luottamuksellisuuden, eheyden, saatavuuden ja keskeisten sidosryhmien vaatimusten perusteella. Valtionhallinnossa tietojen luokittelulla tarkoitetaan käytännössä viranomaisen asiankirjan toteamista ja merkitsemistä salassa pidettäväksi tai turvallisuusluokitelluksi, mistä säädetään julkisuuslaissa (Laki viranomaisten toiminnan julkisuudesta 621/1999) ja tiedonhallintalaissa (Laki julkisen hallinnon tiedonhallinnasta 906/2019). Vaadittavat suojaustoimenpiteet pohjautuvat tietojen luokitteluun, joten muutaman haastatellun mielestä olisi tarpeellista löytää mittari sille, miten hyvin suojausta vaativat tiedot ja tietovarannot tällä hetkellä tunnistetaan ja luokitellaan. Toisaalta osa haastatelluista ei katso tarpeelliseksi raportoida johdolle tästä, koska se menee heidän mukaansa liian yksityiskohtaiseksi tiedoksi. Tässä onkin oikein hyvä osoitus siitä, että seuraavaksi on tehtävä tietotarpeiden priorisointia. Joka tapauksessa suojausta vaativien kohteiden tunnistamisen tietotarve on perusteltu, joten se jätettiin tarjolle myöhempää mittarikehitystä varten.

Useissa haastatteluissa keskusteltiin järjestelmien elinkaaresta. Moni ajattelee, että varsinkin uusia järjestelmiä hankittaessa ja tuotantoon viedessä prosessit toimivat hyvin, mutta pitkään tuotannossa olleista järjestelmistä ei ole elinkaaren hallinnan suhteen täyttä varmuutta. Muutamat haastatellut henkilöt haluaisivatkin varmistaa, että hallinnolliset prosessit, kuten käyttöoikeuksien läpikäynti, toimivat. Hallintakeino A.5.18 pääsyoikeuksista sanoo, että pääsyoikeuksia tietoihin on myönnettävä, katselmoitava, muokattava ja poistettava pääsynhallinnan toimintaperiaatteiden ja sääntöjen mukaisesti, joten mittari käyttöoikeuksien läpikäynnistä vastaisi osaltaan tietotarpeeseen. Lisäksi muutaman haastatellun mielestä järjestelmän elinkaaren aikana olisi hyvä tarkistaa, onko tiedon kasaumavaikutusta huomioitu. Kyse on tiedon

luokitteluun (A.5.12) liittyvästä hallintakeinosta, jota avattiin suojausta vaativien kohteiden tunnistamisen yhteydessä. Kasaumavaikutus tarkoittaa sitä, että kun tietoa ikään kuin kasautuu samaan paikkaan, järjestelmässä olevan tietovarannon tai koko järjestelmän luokitus voi muuttua (Valtiovarainministeriö 2021, 35). Tietotarve, joka tähän on muotoiltu järjestelmien elinkaaren hallinnaksi, vaatisi näin ollen ainakin kaksi mittaria.

Haastateltujen yleinen kokemus oli, että Väylävirastossa tunnistetaan tietoturvaan liittyvät uhat ja riskit hyvin. Haastatteluissa huomattiin kuitenkin tarve tuoda johdon raportointiin mukaan merkittäviä tietoturvariskejä. ISO/IEC 27001 -standardi esittää vaatimuksia tietoturvariskien arvioinnille (8.2) ja käsittelylle (8.3). Tietotarpeeksi muotoutui siten organisaation tietoturvariskeille altistuminen. Haastatteluissa esiin tuodut riskit voidaan jakaa karkeasti kahteen ryhmään: toiminnalliset ja tekniset riskit. Toiminnalliset riskit ovat tietoturvariskejä, jotka voivat toteutuessaan olla riski toiminnan jatkuvuudelle. Esimerkiksi maineen vahingoittuminen on eräs mahdollinen toiminnallinen riski, joka voi seurata vaikkapa vakavasta tietoturvapoikkeamasta. Pari haastateltua henkilöä ehdottikin, että raportoinnissa voisi näkyä 3–5 merkittävintä toiminnallista tietoturvariskiä ja se, mihin suuntaan riskit ovat muuttuneet ja millä hallintakeinoilla, jos riskejä on jollain tapaa pyritty hallitsemaan. Tässä kohdassa kuitenkin korostettiin, ettei riskienhallintaa ole tarkoitus tehdä raportoinnin yhteydessä, vaan raporteissa voidaan korkeintaan tarkastella tietoturvariskejä yleisellä tasolla. Raportissa voisi esimerkiksi olla linkki tarkempaan riskien käsittelyyn, joka puolestaan olisi suojattu käyttövaltuushallinnan keinoin.

Viimeiseksi tietotarpeeksi Tunnistaminen-teemasta löytyi ohjeiden katselmointi. Hallintakeino A.5.37 ottaa kantaa siihen, että tietojenkäsittelypalveluita koskevat ohjeet on dokumentoitu, minkä lisäksi niiden tulee olla niitä tarvitsevien saatavilla. Tämä koskee tietysti kaikkia tietoturvaan liittyviä ohjeistuksia. Monessakin haastattelussa todettiin, että ohjeiden liiallinen määrä ja pituus on negatiivinen asia. Kun ohjeita on paljon, osa niistä voi helposti päästä vanhentumaan. Ohjeiden tulisi olla ajantasaisia, selkeitä, tiiviitä ja helposti ymmärrettäviä, jotta niiden noudattaminen on mahdollisimman sujuvaa ja käytännöllistä. Muutama haastateltu henkilö korosti, että on keskeistä varmistaa, että ohjeet myös jalkautetaan käytäntöön. Niinpä olisikin tärkeää löytää tasapaino ohjeiden määrän ja sisällön välillä. Ohjeiden säännöllinen katselmointi voi toimia työkaluna tähän, joten siitä muotoutui eräs ehdotus tietotarpeeksi. On tosin mainittava, että ainakin yksi haastateltava ilmaisi, ettei tämä olisi johdon näkökulmasta erityisen kiinnostavaa.

6.2 Suojaaminen

Suojaaminen-teemasta löytyivät taulukossa 2 esitetyt tietotarpeet. Väylävirasto on tilaajaorganisaatio, joten ei ole yllättävää, että useissa haastatteluissa tuotiin esiin palveluntuottajanäkökulmaa, palveluntuottajat kun muodostavat olennaisen osan Väyläviraston

tietoturvallisuudesta. Haastatellut henkilöt pohtivat, että Väyläviraston toimintaympäristön huomioimatta jättäminen ei palvele kokonaiskuvan muodostamista, vaan antaa pikemminkin valheellista turvallisuudentunnetta. Niinpä suojaaminen-teeman ensimmäinen tietotarve liittyy hallintakeinoihin A.5.19 eli tietoturvallisuus toimittajasuhteissa sekä A.6.1 eli taustatarkistus. Jälkimmäinen hallintakeino muotoilee, että työnhakijoiden taustat on tarkistettava ennen heidän palkkaamistaan sekä jatkuvana prosessina muun muassa lakien ja määräysten mukaisesti. Taustatarkistukset on suhteutettava paitsi liiketoiminnan vaatimuksiin, myös käsiteltävän tiedon luokitukseen ja arvioituihin riskeihin.

Taulukko 2: Tietotarpeet "Suojaamme toimintamme ja järjestelmämme"-periaatteesta

Suojaamme toimintamme ja järjestelmämme	
Tietotarve	**ISO/IEC 27001 -viite**
Palveluntuottajanäkökulma	A.5.19 Tietoturvallisuus toimittajasuhteissa A.6.1 Taustatarkistus
Henkilöstön tietoturvatietoisuus	7.3 Tietoisuus A.6.3 Tietoturvatietoisuus, -opastus ja -koulutus
Sosiaaliseen manipulointiin varautuminen	A.5.17 Tunnistautumistiedot A.6.3 Tietoturvatietoisuus, -opastus ja -koulutus
Vaatimustenmukaisuus	9.2 Sisäinen auditointi A.5.31 Lainsäädäntöön, asetuksiin, viranomaismääräyksiin ja sopimuksiin sisältyvät vaatimukset A.5.35 Tietoturvallisuuden riippumaton katselmointi

Turvallisuusselvityslaissa (726/2014) säädetään henkilöturvallisuusselvityksistä, jotka suojelupoliisi tekee henkilön luotettavuuden ja nuhteettomuuden varmistamiseksi. Niiden palveluntuottajien työntekijöiden, jotka työssään käsittelevät Väyläviraston turvallisuusluokiteltuja tietoja, on oltava turvallisuusselvitetty eli taustatarkistettu. Hallintakeinon A.5.19 mukaan organisaation on määritettävä ja toteutettava prosessit, joiden avulla hallitaan palveluntuottajien palvelujen tai tuotteiden käyttöön liittyviä tietoturvariskejä. Palveluntuottajien turvallisuusselvitykset ovat eräs keino hallita tietoturvariskejä toimittajasuhteissa, joten palveluntuottajanäkökulmaa saadaan tuotua johdon raportointiin luomalla mittari tai mittareita esimerkiksi palveluntuottajista tehtyjen turvallisuusselvitysten voimassaolosta ja/tai hylätyistä turvallisuusselvityksistä.

Toinen tietotarve suojaamisteemasta on henkilöstön tietoturvatietoisuus. Standardin kohdan 7.3 mukaan organisaation työntekijöiden on oltava tietoisia tietoturvapolitiikasta (tässä:

digitaalisen turvallisuuden periaatteista) ja siitä, miten he voivat toiminnallaan parantaa organisaation tietoturvallisuuden tasoa, ja miksi se on tärkeää. Lisäksi kohdassa sanotaan, että organisaation ohjauksessa työskentelevien on oltava tietoisia siitä, että tietoturvallisuuden hallintajärjestelmän vaatimusten laiminlyönnillä voi olla seurauksia. A.6.3-hallintakeino puolestaan ilmaisee, että organisaation ja sen merkittävimpien sidosryhmien henkilöstön on saatava tietoturvakoulutusta ja -opastusta, minkä lisäksi heidän tietojaan on päivitettävä säännöllisesti toimenkuviensa asettamien tarpeiden mukaisesti. Väylävirastossa työstetään parhaillaan palveluntuottajille verkko-oppimisalustaa, mutta näillä näkymin virasto ei voisi helposti toteuttaa palveluntuottajien kouluttautumisen seurantaa. Joka tapauksessa haastateltavat olivat yhtä mieltä siitä, että ainakin oman henkilöstön tietoturvatietoisuus on tärkeä tietotarve. Sitä seuraamalla ja mittaamalla johto saa tietoa siitä, kuinka hyvin koulutus ja muut tietoisuutta parantavat toimet ovat onnistuneet tehtävässään. Tietoisuutta parannetaan Väylävirastossa pakollisen sähköisen tietoturvakoulutuksen lisäksi tietoturvaviestinnällä, kalasteluviestiharjoituksilla ja erilaisilla koulutustilaisuuksilla.

Tietoturvatietoisuus auttaa henkilöstöä tunnistamaan tietoturvaan liittyviä uhkia ja valitsemaan turvallisia työskentelytapoja. Esimerkiksi tietovuodot voivat vahingoittaa organisaation mainetta ja luottamusta sidosryhmien silmissä, ja hyvin koulutettu henkilöstö pienentää tällaisten tapausten todennäköisyyttä. Hyvin koulutettu henkilöstö myös osaa toimia oikein ja ripeästi tietoturvapoikkeaman havaittuaan, mikä pienentää niiden vaikutuksia toimintaan. Pelkkä sähköisen tietoturvakoulutuksen käyneiden lukumäärä ei vielä kuvaa henkilöstön tietoturvatietoisuuden tasoa, joten haastateltujen mukaan olisi voitava todentaa, miten vaikuttavia koulutus ja muut toimet ovat. Yksi haastatelluista ehdottikin henkilöstölle säännöllisesti lähetettävää kyselylomaketta, jonka avulla tätä voitaisiin kartoittaa.

Niin ikään tietoturvatietoisuuteen liittyy Väylävirastossa taannoin järjestetty tietojenkalasteluharjoitus, jonka lukuisat haastatellut toivat esille. Kalasteluviestiharjoituksia aiotaan toteuttaa toistuvasti, koska tietojenkalastelu on nykyään eräs merkittävimmistä tietoturvaan liittyvistä uhkista. Vaikka tekniset tietoturvajärjestelyt suodattavatkin suurimman osan roskapostista, lopullinen suoja tulee kuitenkin henkilön kyvystä tunnistaa varoitusmerkit. Näin ollen kolmanneksi tietotarpeeksi muotoutui sosiaaliseen manipulointiin varautuminen. Sosiaalisessa manipuloinnissa (engl. *Social Engineering*) hyökkääjä huijaa henkilöitä tai yrityksiä tekemään jotain hyökkääjää hyödyttävää tai luovuttamaan hänelle arkaluonteisia tietoja, kuten esimerkiksi salasanan (Salahdine & Kaabouch 2019). Standardin Liite A:n hallintakeinoista ainakin A.5.17 ja A.6.3 perustelevat tätä tietotarvetta. Jälkimmäisenä mainittu on avattu edellä tietoturvatietoisuutta käsiteltäessä. Ensimmäisenä mainittu hallintakeino liittyy tunnistautumistietoihin. Sen mukaan tunnistautumistietoja on hallittava prosessilla, johon sisältyy henkilöstön perehdyttäminen tunnistautumistietojen asianmukaiseen käsittelyyn. Myöhemmin kehitettävät mittarit vastaavat tietotarpeeseen siitä, ovatko henkilöstön

tunnistautumistietojen käsittely ja tietoturvatietoisuus riittävällä tasolla torjumaan sosiaaliseen manipulointiin liittyvää uhkaa.

Haastattelujen perusteella neljäs tietotarve suojaaminen-teemasta on vaatimustenmukaisuuden seuranta. Hallintakeino A.5.31 liittyy olennaisesti tähän tietotarpeeseen. Kyseinen hallintakeino edellyttää, että organisaation on yksilöitävä, dokumentoitava ja pidettävä ajan tasalla lakeihin, asetuksiin, viranomaismääräyksiin ja sopimuksiin perustuvat tietoturvallisuuden kannalta tärkeät vaatimukset sekä organisaation toimintamallit niiden täyttämistä varten. Käytännössä vaatimustenmukaisuutta seurataan riippumattomien ulkoisten toimijoiden tekemien auditointien (A.5.35) ja omavalvonnan (9.2) kautta. Hallintakeino A.5.35 kertoo, että organisaation tietoturvan johtamisen toimintamalli ja toteutus - mukaan lukien prosessit, teknologiat ja henkilöstö - on katselmoitava puolueettomasti ja suunnitellusti tai kun johtamisen toimintamallissa tai toteutuksessa tapahtuu tähdellisiä muutoksia. Standardin kohdassa 9.2 puolestaan määrätään sisäisestä auditoinnista, jota kutsutaan Väylävirastossa omavalvonnaksi. Auditointien ja omavalvonnan tuloksista muodostetut mittarit vastaavatkin tietotarpeeseen vaatimustenmukaisuudesta. Vaatimustenmukaisuus on välttämätöntä, jotta Väylävirasto toimii lain mukaisesti ja välttää mahdolliset seuraamukset, joita vaatimustenmukaisuuden laiminlyönnistä voisi koitua.

6.3 Havainnointikyky

Taulukko 3 esittää tietotarpeet havainnointikyky-teemasta. Etenkin monissa asiantuntijahaastatteluissa havainnointikyvyn teeman kohdalla kuvailtiin Väyläviraston ICT-palvelut-yksikössä kehityksessä olevaa tietoturvallisuuden tilannekuvaa. Kyseessä on operatiivinen raporttinäkymä, joka osoittaa reaaliaikaisesti, missä kunnossa tärkeät järjestelmät ovat tietoturvanäkökulmasta. Tietoturvallisuuden tilannekuva -näkymä näyttää sen liikennevalomallin (vihreä, keltainen, punainen) mukaisesti värien avulla. Tilannekuvapalvelu seuraa kunkin järjestelmän poikkeamia viitearkkitehtuurista, haavoittuvuuksia ja käyttämiä kontrolleja.

Taulukko 3: Tietotarpeet "Varmistamme havainnointikykymme"-periaatteesta

Varmistamme havainnointikykymme	
Tietotarve	**ISO/IEC 27001 -viite**
Tietoturvallisuuden tilannekuva (ICT)	
Kooste SOC-raporteista	A.8.16 Valvontatoiminnot
Henkilöstön havainnointikyvykkyys	A.6.3 Tietoturvatietoisuus, -opastus ja -koulutus A.6.8 Tietoturvatapahtumista raportointi

Tietoturvallisuuden tilannekuvaan liittyy ymmärrettävästi laaja kirjo eri hallintakeinoja, eikä niiden seikkaperäinen käsittely ole tässä tarpeen. Joka tapauksessa tietoturvan tilannekuva pyrkii luomaan yhteisen näkymän liiketoiminnan, johdon ja järjestelmien omistajien kesken. Tietoturvan tilannekuva on siten keino muodostaa yhteinen näkemys tietoturvan tilasta kussakin järjestelmässä. Eräs haastateltu henkilö suositti, että vaikka tietoturvan tilannekuva on operatiivinen ja reaaliaikainen, voisi siitä sopivin aikavälein saada muodostettua yhteenvedon johdon raporttiin, jossa sitä voisi analysoida ylemmällä tasolla.

Haastateltavat kokivat, että raporteilla tulee olla kooste SOC-raporteista. SOC (engl. *Security Operations Center*) on tietoturvavalvomo, joka tarkkailee toimeksiantajansa ympäristöä tietoturvapoikkeamien varalta (TEPA-termipankki 2024). Hallintakeino A.6.16 valvontatoiminnoista määrää, että verkkoja, järjestelmiä ja sovelluksia on valvottava, jotta poikkeamat voidaan havaita, minkä lisäksi mahdolliset tietoturvahäiriöt tulee käsitellä asianmukaisesti. SOC tuottaa operatiivista raportointia, mutta haastatellut olivat pääsääntöisesti yhtä mieltä siitä, että myös taktiselle ja strategisellekin tasolle kuuluu kooste SOC-raporteista. Näkökulmana tulisi kuitenkin olla merkityksellisyys raportoinnin yleisölle. Ylimpään johtoon kuulunut haastateltava totesi, että niin sanotusti taustakohinaan kuuluvat asiat, kuten vaikkapa automaattisesti suodatettujen roskapostien määrä, eivät ole välttämättä tarpeellista tietoa. Eräs asiantuntija konkretisoi merkityksellisyyttä esimerkillä kohdennetuista hyökkäysyrityksistä, jotka ovat varmasti johdon näkökulmasta kiinnostavia.

Teknisten havainnointitoimintojen lisäksi havainnointikykyyn kuuluu henkilöstön kyvykkyys havaita poikkeamia ja ilmoittaa niistä. Jälleen kyse on osin henkilöstön tietoturvatietoisuudesta, -opastuksesta ja -koulutuksesta (A.6.3), jota on avattu monen muunkin tietotarpeen kohdalla. Osin kyse on hallintakeinosta A.6.8, joka ottaa kantaa tietoturvatapahtumista raportointiin. Henkilöstölle on oltava tarjolla mekanismi ja asianmukaiset kanavat havaitsemiensa tai epäilemiensä tietoturvatapahtumien nopeaan raportointiin. Yksinkertaisimmillaan tähän tietotarpeeseen voi vastata raportoimalla henkilöstön tekemien ilmoitusten määrän. Se antaa käsitystä siitä, kuinka aktiivisesti tietoturvaan liittyviä havaintoja tehdään. Lisäksi se kertoo siitä, kuinka hyvin henkilöstö osaa tehdä ilmoituksia. Ajan myötä havaintojen määrien raportointi voidaan muuttaa trendiksi, joka kuvaa pidemmän aikavälin kehitystä. On kuitenkin hyvä pitää mielessä, ettei vaikkapa nouseva trendi yksistään kerro henkilöstön havainnointikyvyn paranemisesta, vaan se voi olla myös seurausta tietoturvatapahtumien lisääntymisestä, josta kerrotaankin seuraavassa kappaleessa lisää.

6.4 Reagointi

Reagointi-teeman tietotarpeet on listattu taulukossa 4. Haastatteluista kävi ilmi, että tietoturvatapahtumien kehityssuunta on olennainen tietotarve. Tietoturvatapahtumat ovat tapahtumia joko tietojärjestelmissä tai organisaation toiminnoissa, joilla saattaa olla vaikutusta

tietoturvaan (Kyberturvallisuuden sanasto 2018, 13). Tietoturvatapahtumien kehityssuunnalla viitataan poikkeamien, häiriöiden ja haavoittuvuuksien määrien ja laadun trendeihin. Laatu tarkoittaa tässä erityisesti vakavia tai merkittäviä tapahtumia, jotka voivat aiheuttaa vahinkoa organisaation toiminnalle. Tietotarve liittyy selkeästi hallintakeinoon A.5.7 eli uhkatiedon seurantaan. Hallintakeino A.5.7 uhkatiedon seurannasta edellyttää, että tietoturvauhkiin liittyvää tietoa on kerättävä ja analysoitava, jotta organisaatiossa kyetään tuottamaan kattavaa uhkatietoa. Tietoturvatapahtumien trendien ymmärtäminen on tärkeää johtotasolla, sillä se voi auttaa ennakoimaan tulevia uhkia. Kehityssuuntien analysointi liittyykin keskeisesti toiminnansuunnitteluun, joten niiden analysointi voi tarjota arvokasta tietoa päätöksenteon tueksi.

Taulukko 4: Tietotarpeet "Reagoimme poikkeamiin ja palaudumme suunnitelmien mukaisesti"-periaatteesta

Reagoimme poikkeamiin ja palaudumme suunnitelmien mukaisesti	
Tietotarve	**ISO/IEC 27001 -viite**
Tietoturvatapahtumien kehityssuunta	A.5.7 Uhkatiedon seuranta
Tietoturvatapahtumiin reagointi tavoiteajassa	A.5.25 Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen A.5.26 Tietoturvahäiriöihin reagointi
Tietoturvahäiriöistä oppiminen	A.5.27 Tietoturvahäiriöistä oppiminen
Toipumissuunnitelmien/toipumisohjeiden katselmointi	A.5.30 Tieto- ja viestintätekniikan valmius liiketoiminnan jatkuvuussuunnittelussa

Muutama haastateltu henkilö toi esille myös tarpeen tietää, kuinka hyvin tietoturvatapahtumiin saadaan reagoitua eli saadaanko korjaavat toimenpiteet suoritettua tavoiteajassa. Ensinnäkin organisaation on arvioitava tietoturvatapahtumat siitä näkökulmasta, luokitellaanko ne tietoturvahäiriöiksi, kuten hallintakeino A.5.25 tietoturvatapahtumien arvioinnista ja niitä koskevien päätösten tekemisestä edellyttää. Tietoturvahäiriö on ei-toivottu ja mahdollisesti odottamaton tietoturvatapahtuma, joka vaarantaa organisaation tietoturvan ja joka voi vaikuttaa organisaation toimintaan haitallisesti (Kyberturvallisuuden sanasto 2018, 14). Toiseksi organisaation tulee hallintakeinon A.5.26 mukaisesti reagoida tietoturvahäiriöihin dokumentoitujen menettelytapojen mukaan. Tietotarve tietoturvatapahtumiin reagoinnista heijastaa pyrkimystä varmistaa tehokas ja sujuva toiminta tietoturvahäiriöiden ilmetessä. Tavoiteajassa reagointi rajoittaa häiriöiden vaikutuksia ja minimoi niiden aiheuttamia vahinkoja. Kokonaiskuvassa se osoittaa, onko organisaatiolla kyvykkyyttä sopeutua nopeasti muuttuviin tietoturvahaasteisiin.

Suurin osa haastateltavista oli sitä mieltä, että Väylävirastossa kerätään kyllä opit ja kokemukset tietoturvahäiriöistä, mutta sitä ei tällä hetkellä varsinaisesti raportoida. Tietoturvahäiriöistä oppimisen todentaminen jää näin ollen vähemmälle huomiolle johdon raportoinnissa. Hallintakeinon A.5.27 mukaan tietoturvahäiriöistä saatuja oppeja tulee hyödyntää tietoturvan hallintakeinojen parantamisessa. Niinpä tietotarve tietoturvahäiriöistä oppimisesta kertookin organisaation pyrkimyksestä jatkuvaan parantamiseen. Tietoturvahäiriöiden analysointi tuottaa arvokasta tietoa siitä, miten tietoturvakäytännöt ovat toimineet todellisissa tilanteissa, joten se auttaa tunnistamaan paitsi heikkoudet myös vahvuudet nykyisissä tietoturvallisuuden hallintajärjestelmän prosesseissa ja tietoturvaratkaisuissa. Esimerkiksi sen raportoiminen, minkälaisia parantamistoimenpiteitä häiriöistä käynnistyy, vastaa tämänkaltaiseen tietotarpeeseen.

Haastatteluissa käytiin myös keskustelua toipumissuunnitelmista ja niitä kevyemmistä järjestelmien toipumisohjeista. Vastuu niiden ajantasaisuuden varmistamisesta on jakautunut järjestelmäomistajille ja -vastaaville. Yleinen käsitys oli, että suunnitelmat ovat pitkälti ajan tasalla. Tätä ei kuitenkaan keskitetysti valvota, joten osa katsoi toipumissuunnitelmien ja -ohjeiden katselmoinnin raportoimisen olevan tarpeellista. Hallintakeino A.5.30 ottaa kantaa tieto- ja viestintätekniikan valmiuteen liiketoiminnan jatkuvuussuunnittelussa. Sen mukaan tieto- ja viestintätekniikan valmius on paitsi suunniteltava, myös toteutettava, ylläpidettävä ja testattava. Toipumissuunnitelmien ja -ohjeiden säännöllinen katselmointi ylläpitää asianmukaisia valmiuksia palautua häiriöistä, minkä lisäksi niiden päivitys voi olla välttämätöntäkin toimintaympäristön ja tietoturvahaasteiden lisääntyessä ja muuttuessa. Katselmoinnissa tulisikin tarkistaa suunnitelmat ja ohjeet uusimpien tietoturvauhkien ja -riskien näkökulmasta sekä varmistaa niiden yhteensopivuus organisaation muiden prosessien kanssa.

6.5 Johdon raportointi

Johdon raportointi -teemassa paneuduttiin tarkemmin kysymykseen siitä, minkälaista raportointia johdon tulisi tietoturvallisuudesta saada päätöksenteon tueksi niin taktisella väliraportoinnin kuin strategisella vuosiraportoinninkin tasolla. Monissa haastatteluissa painotettiin sitä, että on olennaista tiedostaa, mitä raportoinnilla tavoitellaan. Samoin on tulkittavissa, että haastateltavat ovat yhtä mieltä siitä, että asiantuntijoille mielenkiintoinen tieto ei välttämättä ole tarpeellinen johdolle, joten tietoturvaraportoinnin yleisö on pidettävä mielessä raportointia tehdessä.

Useat haastatellut totesivat yleisesti, että toivoisivat raportointia, joka on tehty yhteistyössä turvallisuusosaston, tieto-osaston ja tieto-osastolla toimivan ICT-palvelut-yksikön kanssa. Sekä väliraporttiin että vuosiraporttiin voi tuoda kehittämis- ja toimenpide-ehdotuksia, minkä lisäksi niissä voidaan seurata keskeisimpiä projektikokonaisuuksia. Tässäkin kuitenkin

kehotettiin pitämään näkökulma siellä, mikä on raportoinnin yleisölle tärkeää, eli mistä asioista saatetaan esimerkiksi tarvita johdon linjauksia.

6.5.1 Vuosiraportointi

Vuosiraportointi asettuu strategiselle tasolle organisaation toiminnassa. Se muodostaa perustan strategisen suunnittelun ja päätöksenteon tueksi, joten vuosiraportoinnin ensisijainen yleisö on ylin johto. Haasteena on yleiskuvan muodostaminen koko organisaation toiminnasta, nimittäin johdon muodostama tilannekuva koostuu monista erityyppisistä raporteista, joita Väylävirastossa tuotetaan. Tietoturvaraportointi tulisi osata linkittää muihin strategisiin toimintoihin. Tämä ei aina ole yksinkertaista, sillä tietoturvallisuuden vaikutukset organisaation toiminnan muihin osa-alueisiin ja strategiaan voivat olla vaikeasti hahmotettavissa, minkä lisäksi ylimpään johtoon kuuluvat eivät useinkaan ole tietoturva-alan ammattilaisia. Haastatteluista kävi kuitenkin ilmi, että Väyläviraston ylimmän johdon koettiin olevan riittävän valveutunut tietoturva-asioista ollakseen vastuussa tietoturvallisuutta koskevista strategisista päätöksistä.

Lähtökohtaisesti vuosiraportointi nähtiin paikkana, jossa digitaalisen turvallisuuden periaatteet voisivat olla katettuna, myös otsikkotasolla. Eräs haastateltu henkilö kuitenkin vaikutti olevan jokseenkin eri mieltä. Hänen mukaansa periaatteet ovat ennemminkin suuntaa antavia kuin toimintaa järjestelmällisesti ja määrämuotoisesti ohjaavia tavoitteita. Hän pohti, missä menee raportoinnin ja sen raja, että johdon pitää itse tehdä johtopäätöksiä periaatteiden toteutumisesta. Toisin sanoen ylimmän johdon tehtävänä on peilata periaatteita suhteessa raportointiin sen sijaan, että raportointi pyrkisi tarjoamaan johdolle valmiin tilannekuvan. Hänen mukaansa ideaalitilanteessa raportointi voisi olla pikemminkin johdon tilannekuvaa ja johtopäätöksiä fasilitoiva kuin annettu kokonaisuus. Hän näki, että strategisen tason raportoinnissa tulisi painottaa teknisten asioiden sijaan vaikuttavuutta ja muita asioita, jotka ovat keskeisiä johtamisen näkökulmasta.

Muutkin pohtivat raportoinnin vaikuttavuutta. Näissä pohdinnoissa korostui se, että pelkkä raportointi ei useinkaan riitä saavuttamaan haluttuja tuloksia. Todellinen vaikuttavuus syntyy vasta silloin, kun raportin sisältöä, kuten havaintoja ja suosituksia, käsitellään perusteellisesti keskusteluissa ja päätöksenteossa. Eräs haastateltava tiivisti tämän ajatuksen seuraavasti: ”Pahinta on raportti, joka ei herätä keskustelua.”

Joka tapauksessa vuosiraportilta toivottiin analysoitua yhteenvetoa edellisen vuoden tapahtumista, kuten operatiivisen toiminnan yleistrendeistä. Tämän tarkoituksena on tarjota johdolle selkeä käsitys siitä, miten organisaatio on suoriutunut ja reagoinut mahdollisiin toimintaympäristön muutoksiin. Vuosiraportissa kuuluisi peilata toimintaympäristön muutosta viraston tilanteeseen ja toimintaan, jotta voidaan ymmärtää, miten nämä tekijät ovat vaikuttaneet virastoon. Lisäksi raportissa tulisi esittää vertailua muihin vastaaviin organisaatioihin. Tämä

vertailu auttaisi arvioimaan organisaation tietoturvallisuuden hallintajärjestelmän toimivuutta suhteessa muihin samankaltaisiin toimijoihin samankaltaisessa toimintaympäristössä.

Koska vuosiraportti on strategisen tason raportti, toivottiin monissa haastatteluissa tulevaisuuteen suuntautumista. Ylimmältä johdolta odotetaan, että se kykenee tarkastelemaan organisaation nykytilannetta suhteessa tuleviin haasteisiin ja mahdollisuuksiin. Tulevaisuuteen suuntautumisen merkitys nousee esiin erityisesti tietoturvallisuudessa, jossa uhkien ja riskien kehittyminen on jatkuvaa. Tällöin raportointi toimii toimintasuunnitelman lähtöaineistona seuraavalle vuodelle. Muutamakin haastateltava puhui sitä, että yhtä lailla kuin riskejä ja uhkakuvia, on tärkeää tunnistaa myös viraston vahvuudet tietoturvallisuudessa. Positiivisia havaintoja voi tehdä esimerkiksi panostuksista tietoturvatietoisuuteen, teknisten kontrollien tehokkuudesta, tietojärjestelmien ja tietojärjestelmäympäristön vakaudesta sekä kyvystä reagoida ripeästi tietoturvapoikkeamiin ja -uhkiin. Vahvuuksien tunnistaminen ja esille tuominen osoittaa, että organisaatio ei vain reagoi, vaan pyrkii proaktiivisesti parantamaan tietoturvaansa.

6.5.2 Väliraportointi

Väliraportoinnin voi ajatella asettuvan taktiselle tasolle, joten väliraportoinnin kohdeyleisö on Väylävirastossa ylimmän johdon lisäksi keskijohto, tietoturva-asiantuntijat ja ICT-palvelutyksikkö. Väliraportit tasapainottelevat operatiivisen ja strategisen näkökulman välillä, joten niissä olisi kyettävä tarjoamaan sekä yksityiskohtaista tietoa operatiivisesta toiminnasta että katsaus strategisiin suuntiin. Väliraportoinnin aikajänteen kommentoitiinkin olevan haastavin.

Eräs haastateltu henkilö mainitsi, että operatiivisella tasolla esimerkiksi poikkeamia käsitellään viikoittain, mutta muutaman kerran vuodessa toimitettavan väliraportoinnin tulisi voida tiivistää operatiivisella tasolla tapahtuvia asioita yhteen. Johdon näkökulmasta on siis tärkeää, että vaikka poikkeamat käsitellään yksittäisinä tapauksina, väliraportoinnissa ne tuodaan yhteen. Operatiivisen tason yksittäisistä poikkeamista tulisi voida väliraportoinnissa nostaa esiin niiden strateginen merkittävyys. Merkittävyydellä hän viittasi siihen, millainen vaikutus poikkeamalla on tai olisi voinut olla organisaation toimintaan. Väliraportoinnissa on hänen mukaansa tärkeää tuoda esille, mitä olisi voinut tapahtua, elleivät hallintakeinot olisi onnistuneet estämään vakavan poikkeaman syntymistä.

Ylimpään johtoon kuulunut haastateltava korosti, että väliraportit ovat alustava kooste vuosiraporttiin, joten siksi niissä tulisi keskittyä erityisesti asioihin, jotka ovat merkittäviä ja jotka voivat indikoida tulevia trendejä. Väliraportointi voi parhaimmillaan tarjota arvokasta tietoa siitä, miten operatiivinen toiminta tukee organisaation pitkän aikavälin tavoitteita ja strategiaa. Kyse on siis operatiivisen tason laadullisesta tulkitsemisesta ja sen peilaamisesta taustalla syntyvään vuositason strategiseen toimintaympäristön muutokseen. Väliraportoinnissa pyritään näin ollen ymmärtämään yksittäisten poikkeamien syvällisempi merkitys osana

laajempaa kontekstia ja strategisia tavoitteita. Väliraportointi nähdään ikään kuin välipisteenä kokonaisvaltaisessa tilannekuvassa.

7 Johtopäätökset ja pohdinta

Kehittämistehtävän kysymyksenä oli, mitä tietoa Väyläviraston päätöksentekijät tarvitsevat kokonaiskuvan muodostamiseksi tietoturvallisuuden hallintajärjestelmän toimivuudesta. Opinnäytetyön tavoitteena oli luoda ehdotus tietotarpeista, joiden avulla Väyläviraston tietoturvallisuuden hallintajärjestelmän suorituskykyä ja vaikuttavuutta voidaan seurata ja mitata sekä raportoida. Tietotarpeiden pohjalle oli määrä rakentaa viraston ISO 27001 -kehitysprojektin seuraavassa vaiheessa mittarit. Työssä onnistuttiin, sillä teemahaastatteluista saadun aineiston avulla saatiin muotoiltua tietotarpeet. Mittarikehityskin on jo käynnistynyt onnistuneesti opinnäytetyön tulosten ansiosta.

Ensinnäkin tietotarpeita ovat suojausta vaativien kohteiden tunnistaminen, järjestelmien elinkaaren hallinta, toiminnallisille tietoturvariskeille altistuminen ja ohjeiden katselmointi. Toiseksi tietotarpeita ovat palveluntuottajanäkökulma eli tietoturvallisuus toimittajasuhteissa, henkilöstön tietoturvatietoisuus, sosiaaliseen manipulointiin varautuminen ja vaatimustenmukaisuus. Kolmanneksi tietotarpeita ovat järjestelmien tietoturvallisuuden tilannekuva, kooste SOC-raporteista ja henkilöstön havainnointikyvykkyys. Neljänneksi tietotarpeita ovat tietoturvatapahtumien kehityssuunta, tietoturvatapahtumiin reagointi tavoiteajassa, tietoturvahäiriöistä oppiminen ja toipumissuunnitelmien/-ohjeiden katselmointi. Tietotarpeet on johdettu suoraan Väyläviraston digitaalisen turvallisuuden periaatteista, joten ne ilmentävät ISO/IEC 27001 -standardin vaatimusten mukaisesti organisaation laajempia tietoturvatavoitteita. Tietotarpeita on myös perusteltu ISO/IEC 27001 -standardin kohdilla ja sen Liite A:n hallintakeinoilla.

Ulkoisilta tietoturvakonsulteilta saadun palautteen perusteella löydetyt tietotarpeet ovat pitkälti vastaavia kuin monilla muillakin organisaatioilla. Vaikka ISO/IEC 27001 ja 27004 -standardit korostavat, että tietotarpeet ovat kullekin organisaatiolle yksilöllisiä, osoittavat nämä tulokset ja arviot sen, että monilla organisaatioilla on samankaltaisia tietotarpeita. Varsinaisia yllätyksiä ei siis tullut. Laadullisella menetelmällä saadut tulokset ovat kuitenkin hyvin konteksti- ja tilannesidonnaisia, joten tämän kehittämistyön tuloksia ei silti voi yleistää koskemaan kaikkia organisaatioita. Esimerkiksi eräs nimenomaan Väylävirastolle huomionarvoinen tietotarve on tietoturvallisuus toimittajasuhteissa eli palveluntuottajanäkökulma. Väylävirasto on tilaajaorganisaatio, joten palveluntuottajilla on suuri merkitys viraston tietoturvallisuuden kannalta. Jossain toisessa organisaatiossa kyseinen tietotarve ei välttämättä korostu. Lisäksi kehittämistyön lähtökohtanakin on ollut Väyläviraston digitaalisen turvallisuuden periaatteet, joten tuloksia ei siksikään voi irrottaa asiayhteydestä.

Yhtäältä suurin haaste opinnäytetyön toteutuksessa oli, että Väyläviraston digitaalisen turvallisuuden periaatteet olivat sen lähtökohtana. Digitaalisen turvallisuuden periaatteet ovat strategisen tason periaatteita, eivätkä toimintaa määrämuotoisesti ohjaavia konkreettisia tavoitteita, kuten eräässä haastattelussakin tuli ilmi. Kysymys kuuluukin, olisiko opinnäytetyön aihe voinut olla tällaisten konkreettisten tietoturvatavoitteiden muotoilu, vaikka sitten kunkin digitaalisen turvallisuuden periaatteen alle. Tietotarpeet olisivat todennäköisesti tulleet tietoturvatavoitteissa sisäänrakennettuina, joten mittarikehitys olisi voinut lähteä liikkeelle tälläkin lähestymistavalla, joka olisi voinut olla helpompi. Toisaalta kuten tunnettu Goodhartin laki sanoo: "When a measure becomes a target, it ceases to be a good measure." Jos mittarin tavoitteen täyttämisestä tulee tavoite itsessään, kyseessä ei enää ole hyvä mittari. Määrämuotoiset mitattavat tietoturvatavoitteet voivatkin siten toimia tarkoitustaan vastaan. Kumpikin lähestymistapa aiheuttaa omat ongelmansa.

Haasteena oli myös opinnäytetyön rajaus hallinnolliseen IT- eli toimistoympäristöön. OT-ympäristö on Väyläviraston kaltaiselle toimijalle aivan yhtä tärkeä, mitä korostettiin haastatteluissakin. OT-ympäristöä on siten vaikea täysin jättää huomioimatta. Monet liiketoimintaprosessit linkittyvät OT-ympäristöön, minkä lisäksi OT-ympäristö on riippuvainen IT-ympäristöstä. Keskittyminen vain hallinnolliseen toimistoympäristöön voi vääristää raportoinnin antamaa kuvaa tietoturvallisuudesta. Toki on muistettava, että OT-ympäristö on tulossa mukaan ISO 27001 -kehitysprojektiin myöhemmin, jolloin se puoli tulee todennäköisesti myös mukaan raportointiin. Monien haastateltujen henkilöiden oli niin ikään hankala ajatella tietoturvaa, sen mittaamista ja raportointia omana erillisenä kokonaisuutenaan. Sen sijaan he pohtivat, tulisiko tietoturvan olla ennemminkin osa normaaleja linjaorganisaatioiden prosesseja, eikä niinkään yksin turvallisuusosaston prosessi, mikä on itse asiassa erinomaista pohdintaa.

Kehittämistyön voidaan arvioida olevan validiteetiltaan hyvä, sillä valitulla menetelmällä ja toteutetulla analyysiprosessilla saatiin tuloksia, joiden pohjalta voitiin sujuvasti jatkaa mittarikehitykseen. Tämä ei olisi ollut mahdollista, mikäli tulokset eivät olisi olleet osuvia. Validiteettia tukee myös se, että opinnäytetyössä haastateltiin useita henkilöitä kolmelta eri organisaatiotasolta. Haastattelut eri organisaatiotasoilla ja osin eri painotuksilla lisäsivät aineiston monipuolisuutta, minkä lisäksi valittujen haastateltujen henkilöiden eri näkökulmat edustavat kokonaisuutta kattavasti. Haastatteluvastauksista tehtyjä havaintoja on myös peilattu ISO/IEC 27001 -standardiin, mikä vahvistaa niiden pätevyyttä.

Kehittämistyön prosessi on dokumentoitu, minkä lisäksi tehdyt valinnat on pyritty perustelemaan huolellisesti. Tulokset eivät välttämättä ole kuitenkaan toistettavissa. Esimerkiksi haastattelurungon muokkaaminen edellisten haastattelujen pohjalta on vaikuttanut seuraavissa haastatteluissa saatuihin vastauksiin. Vaikka haastattelurungon muokkaaminen voi lisätä validiteettia tekemällä kysymyksistä tarkempia ja kohdennetumpia, se voi samalla heikentää tulosten luotettavuutta, koska haastattelut eivät ole identtisiä keskenään. Toisaalta laadullisen

kehittämistyön kohdalla ei varsinaisesti voidakaan ajatella, että tulosten pitäisi olla reliaabeleja. Lisäksi haastattelukysymyksiä on todennäköisesti muokattava tulevaisuudessa OT-ympäristön raportoinnin tietotarpeiden selvitystä varten.

Kuten todettu, kehittämistyön tulokset eli tietotarpeet toimivat pohjana mittarikehityksessä. Tietotarpeiden pohjalta voi syntyä suurikin määrä mittareita. Osana mittarikehitystä tuleekin tehdä niin tietotarpeiden kuin mittareidenkin priorisointia. Mittareiden valinnassa on myös huomioitava datan saatavuus. Jos tiettyyn mittariin tarvittavaa dataa ei ole helposti saatavilla tai sen kerääminen on liian kallista tai aikaa vievää, ei mittari ole käyttökelpoinen. Jatkoa ajatellen on näin ollen tärkeää arvioida yksittäisen mittarin hyöty-panos-suhde. Tämä viittaa siihen, kuinka paljon hyötyä mittarista on verrattuna sen kehitykseen ja käytännön toteuttamiseen vaadittaviin resursseihin. Hyöty-panos-suhteen arviointi auttaa Väylävirastoa keskittymään mittareihin, jotka tuottavat suurimman lisäarvon suhteessa niiden kehittämiseen ja ylläpitoon vaadittaviin panostuksiin.

Seuraavaksi tietotarpeet ja kehitetyt mittarit tulisi sovittaa oikeaan yhteyteensä, joko strategiseen tai taktiseen tietoturvaraportointiin. Mittareita kannattaa testata käytännössä, ja niistä samoin kuin strategisesta ja taktisesta tietoturvaraportoinnista olisi hyvä ottaa vastaan kehitysehdotuksia. On myös hyvä huomioida, että niin tietotarpeiden kuin mittareidenkin täytyy elää ja muuttua organisaation ja toimintaympäristön muutosten mukana.

Kun mittarit tulevat käyttöön strategisessa ja taktisessa tietoturvaraportoinnissa, parantuvat päätöstentekijöiden mahdollisuudet tehdä päätöksiä tietoperusteisesti. Päätösten vaikuttavuutta seurataan sitten seuraavissa raporteissa. Näin ollen Väyläviraston tietoturvallisuuden hallintajärjestelmän toimivuudesta saadaan tietoa, jonka perusteella tietoturvallisuutta voidaan jatkuvasti parantaa. Opinnäytetyöhön voi olla tyytyväinen, koska se on aidosti edistänyt Väyläviraston ISO 27001 -kehitysprojektia. Näillä eväillä otetaan merkittäviä askelia kohti tehokkaampaa tietoturvallisuuden hallintaa.

Lähteet

Alexander, D., Finch, A., Sutton, D. & Taylor, A. 2013. Information Security Management Principles. 2 ed. Swindon: BCS Learning & Development Limited, 1-81.

Alexander, R. D. & Panguluri, S. 2016. Cybersecurity Terminology and Frameworks. Teoksessa Clark, R. M. & Hakim, S. (toim.). Cyber-physical security: Protecting critical infrastructure at the state and local level. Sveitsi: Springer, 19–47.

Brotby, W. K., Hinson, G. & Kabay, M. E. 2013. PRAGMATIC Security Metrics. Hoboken: Auerbach Publishers, Incorporated, 13–58.

Calder, A. 2013. ISO27001 / ISO27002 - A Pocket Guide. 2nd ed. Cambridgeshire: IT Governance Publishing, 37–41.

Campbell, T. 2016. Practical Information Security Management - A Complete Guide to Planning and Implementation. Burns Beach: Apress, 1–95.

Digi- ja väestötietovirasto 2022. VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään. VAHTI Hyvät Käytännöt -tukimateriaali. Viitattu 2.11.2023. https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf/6d71d86f-c7bc-6683-9b36-c55d16d4c1f0/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf?t=1674484177085

Disterer, G. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, Vol. 4 No. 2, 92-100. Viitattu 27.10.2023. https://www.scirp.org/journal/paperinformation?paperid=30059

ISO/IEC 27000. 2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. 2. painos. Suomen Standardit SFS ry.

ISO/IEC 27001. 2022. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardit SFS ry.

ISO/IEC 27002. 2022. Information security, cybersecurity and privacy protection — Information security controls. 3rd ed. ISO/IEC.

ISO/IEC 27004. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. 2. painos. Suomen Standardit SFS ry.

Kokonaisturvallisuuden sanasto 2017. Sanastokeskus TSK. Helsinki. Viitattu 1.11.2023. https://sanastokeskus.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf?file=pdf/Kokonaisturvallisuuden_sanasto_2.pdf

Kyberturvallisuuden sanasto 2018. Sanastokeskus TSK. Helsinki. Viitattu 14.5.2024. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Laki julkisen hallinnon tiedonhallinnasta 906/2019.

Laki viranomaisen toiminnan julkisuudesta 621/1999.

Laki Väylävirastosta 862/2009.

Miller, L. C. 2022. CISSP for Dummies. Newark: John Wiley & Sons, Incorporated.

NIST 2024a. Frameworks. Viitattu 14.3.2024. https://www.nist.gov/frameworks

NIST 2024b. The CSF 1.1 Five Functions. Viitattu 14.3.2024. https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions

Puusa, A. & Juuti, P. 2022. Laadullisen tutkimuksen näkökulmat ja menetelmät. Gaudeamus.

Salahdine, F. & Kaabouch, N. 2019. Social Engineering Attacks: A Survey. Future Internet 2019, 11, 89. Viitattu 8.5.2024. https://doi:10.3390/fi11040089

Schroeder, K., Trinh, H. & Pillitteri, V. 2024a. Measurement Guide for Information Security: Volume 1 - Identifying and Selecting Measures. NIST SP 800-55 Vol 1. Initial Public Draft. Viitattu 19.5.2024. https://doi.org/10.6028/NIST.SP.800-55v1.ipd

Schroeder, K., Trinh, H. & Pillitteri, V. 2024b. Measurement Guide for Information Security: Volume 2 — Developing an Information Security Measurement Program. NIST SP 800-55 Vol 2. Initial Public Draft. Viitattu 19.5.2024. https://doi.org/10.6028/NIST.SP.800-55v2.ipd

SFS 2023. ISO/IEC 27000 Tietoturvallisuuden standardisarja. Viitattu 26.10.2023. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

SFS 2024. Mitä standardi tarkoittaa? Viitattu 5.3.2024. https://sfs.fi/standardeista/mika-on-standardi/

Such, J. M., Gouglidis, A., Knowles, W., Misra, G. & Rashid, A. 2016. Information assurance techniques: Perceived cost effectiveness. Computers & Security, 60, 117–133. Viitattu 19.5.2024. https://doi.org/10.1016/j.cose.2016.03.009

Taherdoost, H. 2022. Cybersecurity vs. Information Security. Procedia Computer Science 2015. Elsevier B.V., 483–487. Viitattu 30.4.2024. https://doi.org/10.1016/j.procs.2022.12.050

TEPA-termipankki 2024. SOC. Viitattu 30.4.2024. https://termipankki.fi/tepa/fi/haku/soc

VAHTI 2016. Toiminnan jatkuvuudenhallinta. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä – VAHTI 2/2016. Valtiovarainministeriö. Viitattu 28.2.2024. https://julkaisut.valtioneuvosto.fi/handle/10024/75168

Valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla 2021. Viitattu 2.10.2023. https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80732d82

Valtiovarainministeriö 2020. Julkisen hallinnon digitaalinen turvallisuus. Julkisen hallinnon ICT. Valtiovarainministeriön julkaisuja – 2020:23. Helsinki. Viitattu 5.5.2024. https://julkaisut.valtioneuvosto.fi/handle/10024/162169

Valtiovarainministeriö 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Tiedonhallintalautakunta. Valtiovarainministeriön julkaisuja 2021:5. Helsinki. Viitattu 14.5.2024. https://julkaisut.valtioneuvosto.fi/handle/10024/162649

Vigil, M., Buchmann, J., Cabarcas, D., Weinert, C. & Wiesmaier, A. 2015. Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey. Computers & Security, 50, 16–32. Viitattu 1.11.2023. https://doi.org/10.1016/j.cose.2014.12.004

Väylävirasto 2023a. Väylävirasto vastaa valtion väyläverkosta. Viitattu 3.11.2023. https://vayla.fi/documents/25230764/35414514/v%C3%A4yl%C3%A4esitely+taitto_V14.pdf/beb3ad01-c571-5441-7343-719f101a2edd/v%C3%A4yl%C3%A4esitely+taitto_V14.pdf?t=1686745242699

Väylävirasto 2023b. Digitaalisen turvallisuuden periaatteet. Viitattu 3.11.2023. https://vayla.fi/palveluntuottajat/turvallisuus/digitaalisen-turvallisuuden-periaatteet

Väylävirasto 2023c. Digitaalisen turvallisuuden periaatteet Väyläviraston toiminnan tueksi. Viitattu 5.5.2024. https://vayla.fi/-/digitaalisen-turvallisuuden-periaatteet-vaylaviraston-toiminnan-tueksi

Väylävirasto 2024a. Väyläviraston strategia. Viitattu 14.3.2024. https://vayla.fi/tietoa-meista/tapamme-toimia/visio-strategia-arvot

Väylävirasto 2024b. Väylävirasto vastaa valtion väyläverkosta. Viitattu 12.4.2024. https://vayla.fi/tietoa-meista/tapamme-toimia

Yhteiskunnan turvallisuusstrategia 2017. Valtioneuvoston periaatepäätös. Turvallisuuskomitea. Viitattu 18.5.2024. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/

Julkaisemattomat lähteet

Evesti, A. 2023. Tietoturvan mittaaminen ja raportointi. Esitys 3.10.2023.

Evesti, A. 2024. Suullinen tieto.

Digi- ja väestötietovirasto 2021. Digiturvallisuuden hallinta – tukimateriaali digiturvan kehittäjille. VAHTI hyvät käytännöt tukimateriaali. Viitattu 28.2.2024. https://dvv.fi/documents/16079645/0/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf/

Väylävirasto 2024c. Raportointi. Viitattu 30.4.2024.

Väylävirasto 2024d. Johtamisjärjestelmät. Viitattu 16.5.2024.

Kuviot

Kuvio 1: Väyläviraston digitaalisen turvallisuuden periaatteet (Väylävirasto 2023b) 9

Taulukot

Taulukko 1: Tietotarpeet "Tunnistamme suojausta vaativat kohteet, uhat ja riskit"-periaatteesta 27
Taulukko 2: Tietotarpeet "Suojaamme toimintamme ja järjestelmämme"-periaatteesta..... 29
Taulukko 3: Tietotarpeet "Varmistamme havainnointikykymme"-periaatteesta 31
Taulukko 4: Tietotarpeet "Reagoimme poikkeamiin ja palaudumme suunnitelmien mukaisesti"-periaatteesta 33