Aalto-yliopisto
Sähkötekniikan
korkeakoulu

Paavo Tapani Hietanen

Sähkökaupan keskitettyyn tiedonvaihtopalveluun kytkeytyvään tietojärjestelmään asetettavat tietoturvavaatimukset

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten.

Espoossa 3.4.2020
Valvoja: Professori Matti Lehtonen
Ohjaaja: Fredrik Södö

Aalto-yliopisto
Sähkötekniikan korkeakoulu

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi

Diplomityön tiivistelmä

Tekijä Paavo Tapani Hietanen

Työn nimi Sähkökaupan keskitettyyn tiedonvaihtopalveluun kytkeytyvään tietojärjestelmään asetettavat tietoturvavaatimukset

Maisteriohjelma Advanced Energy Solutions **Koodi** ELEC3048

Työn valvoja Matti Lehtonen

Työn ohjaaja(t) Fredrik Södö

Päivämäärä 3.4.2020 **Sivumäärä** 74 **Kieli** Suomi

Tiivistelmä

Datahub on Suomen sähkön vähittäismarkkinoita varten toteutettava keskitetty tiedonvaihtojärjestelmä. Datahubin käyttöönotto tapahtuu vuonna 2022, jonka jälkeen kaikki suomalaiset sähkön vähittäismarkkinoiden osapuolet tulevat hoitamaan markkinaprosessinsa sen avulla. Samalla datahub tulee tallentamaan sähkönkulutus-, asiakas- ja osoitetiedot Suomen 3,7 miljoonasta sähkönkäyttöpaikasta tukeakseen näitä markkinaprosesseja. Datahubin toteutus on määrätty Fingrid Datahubin lakisääteiseksi velvollisuudeksi. Lisäksi laki määrää Fingrid Datahubin järjestämään järjestelmän tietoturvan asianmukaiseksi. Datahubin tietoturvan asianmukainen järjestäminen sisältää järjestelmän omien suojauksien lisäksi tietoturvavaatimusten asettamisen siihen liittyville markkinaosapuolille.

Tässä työssä selvitettiin, millaisia tietoturvavaatimuksia Fingrid Datahubin tulee asettaa datahubiin liittyville markkinaosapuolille. Tarvittavien tietoturvavaatimusten määrittämisen pohjana käytettiin Fingrid Datahubin sisäisesti suoritettua riskiarviota. Riskiarvio muodostettiin tarkastelemalla datahubiin liittyviä osapuolia, näiden tulevia toimintoja datahubissa, sekä tietoturvauhkien yleistä luonnetta. Riskiarvion jälkeen työssä suoritettiin kirjallisuustutkimus sekä asiantuntijahaastatteluita tarvittavien tietoturvavaatimusten määrittämisen ymmärtämiseksi. Edellä mainittujen vaiheiden lopputuloksena kehitettiin datahubiin liittyville osapuolille asetettavien tietoturvavaatimusten viitekehys. Viitekehys todennettiin datahubin tarpeita vastaavaksi esittämällä se järjestelmän tunteville asiantuntijoille ja muokkaamalla sitä palautteen perusteella, kunnes sen sopivuudesta saavutettiin yksimielisyys.

Kehitetty viitekehys edistää datahub-projektia toimimalla pohjana järjestelmään liittyville osapuolille luotavan sopimuksen tietoturvavaatimuksille. Lisäksi työ nostaa esille puutteita tietoturva-alan tutkimuksessa. Suurimmat puutteet nousevat esille useiden tutkimusten kyvyttömyydessä todistaa tulostensa toimimista käytännössä. Samaan aikaan tietoturvauhat kehittyvät vakavammiksi ja arvaamattomammiksi. Näin ollen alan tutkimuksella on suuri tarve pysyä mukana kehittyvässä uhkakentässä sekä kyetä todentamaan, että tutkimuksissa käytetyt menetelmät tuottavat käytännössä toimivia tuloksia.

Avainsanat sähkön vähittäismarkkinat, tietoturva, datahub

Aalto University
School of Electrical
Engineering

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi

Abstract of master's thesis

Author Paavo Tapani Hietanen

Title of thesis Information security requirements for a system connecting to electricity markets' centralised information exchange system

Master programme Advanced Energy Solutions **Code** ELEC3048

Thesis supervisor Matti Lehtonen

Thesis advisor(s) Fredrik Södö

Date 3.4.2020 **Number of pages** 74 **Language** Finnish

Abstract

Datahub is a centralised information exchange system for the Finnish electricity retail market. Datahub will go live on the year 2022, after which all participants in the Finnish electricity retail market will conduct their business processes with it. At the same time datahub will store electricity consumption, customer and address information from Finland's 3,7 million electricity metering points to support these processes. The implementation of datahub is a legal responsibility of Fingrid Datahub. Furthermore, the law orders Fingrid Datahub to organise the information security of the system in an adequate manner. Organising the information security of datahub in an adequate manner includes organising the security of the system itself, as well as placing information security requirements to market participants that will establish a connection to it.

This work studied the nature of information security requirements that Fingrid Datahub should place on connecting market participants. Fingrid Datahub's internally conducted risk analysis served as a basis for measuring the needed information security requirements. The risk analysis was done by examining the connecting market participants, the ways in which they will use the system in the future as well as information security threats in general. After the risk analysis was conducted, this work proceeded to conduct a literature study as well as a series of expert interviews in order to understand how to determine the correct information security requirements. As the result of the aforementioned phases, a framework of information security requirements for market participants that will establish a connection to datahub was developed. The framework was ascertained to meet datahub's needs by presenting it to experts who were familiar with datahub and modifying it according to received feedback until a consensus of its validity was reached.

The developed framework will advance the datahub project by working as a basis for information security requirements that will be included to datahub's market participant service agreement. In addition, this work presents faults in the scientific research of information security. The biggest fault is the lack of evidence of operability that is present in many of the studies. At the same time, information security threats are becoming more severe and unpredictable. This means that the scientific research has a great need to keep up with the developing range of threats as well as be able to ascertain that the used research methodology produces working solutions.

Keywords electricity retail market, information security, datahub

Alkusanat

Tämä diplomityö tehtiin osana datahub-projektia Fingrid Datahubin toimeksiannosta. Haluan kiittää esimiestäni Pasi Ahoa sekä ohjaajaani Fredrik Södöä mahdollisuudesta osallistua tähän tärkeään hankkeeseen näkökulmasta, joka on ollut itselleni kiehtova.

Olen kiitollinen myös muulle Fingrid Datahubin henkilökunnalle, joka diplomityön kirjoittamisen aikana oli suureksi avuksi aina sitä tarvitessani. Erityisesti haluan kiittää ohjausryhmäni jäseniä, Saku Palannetta, Pinja Kimaria ja Jyrki Pennasta. Haluan myös kiittää työhön apuaan antaneita Fingrid Datahubin asiantuntijoita Marjut Puukangasta, Otto Kuurannetta, Antti Kivipuroa sekä Pasi Lintusta.

Kiitos työn onnistumisesta kuuluu myös useille Fingrid Datahubin ulkopuolisille apuaan tarjonneille henkilöille ja tahoille. Haluan kiittää kaikkia kanssani yhteistyössä toimineita asiantuntijaorganisaatioita ja itsenäisesti toimineita asiantuntijoita heidän neuvoistaan diplomityöni tekemisessä. Haluan myös kiittää perhettäni, erityisesti isääni Seppo Hietasta, sekä professori Matti Lehtosta kaikesta heidän tarjoamastaan avusta.

Lopuksi haluan antaa suurimmat kiitokseni Christina Alexanderille. Ilman sinua elämässäni ei tämäkään työ olisi tällä hetkellä lukijan edessä tarkasteltavana.

Espoo 3.4.2020

Paavo Tapani Hietanen

Sisällysluettelo

Lyhenteet

AIAA	American Institute of Aeronautics and Astronomics
APT	Advanced Persistent Threat
B2B	Business to Business
C2	Command and Control
CEA	Cybersecurity Enhancement Act
CEN	Comité Européen de Normalisation
CSIRT	Computer Security Incident Response Team
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EU	Euroopan unioni
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
NIST	Network and Information Systems Technology
NSA	National Security Authority
OID	Object Identifier
PDF	Adobe Portable Document Format
PKI	Public Key Infrastructure
SCADA	Supervisory Control and Data Acquisition
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USB	Universal Serial Bus
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VRK	Väestörekisterikeskus
XML	eXtensible Markup Language

1 Johdanto

Digitalisaatio on erityisesti viime vuosina ollut kansainvälisesti kasvava ilmiö [1][2][3]. Energiasektorilla tämä näkyy esimerkiksi niin sanottujen älykkäiden sähköverkkojen kehityksenä, jolla viitataan sähkönjakelujärjestelmien tehostamiseen tietotekniikalla [4][5][6][7]. Joillakin energiasektorin osa-alueilla, kuten energiamarkkinoilla, koetaan samalla kuitenkin tarpeita myös puhtaasti digitaalisille palveluille [8][9]. Tällä tarkoitetaan sellaisia palveluita, joilla ei välttämättä ole suoraa yhteyttä fyysiseen infrastruktuuriin toisin kuin energianjakelua säätelevillä järjestelmillä. Esimerkkejä edellä mainituista ovat erilaiset data-analytiikka- ja kommunikaatiojärjestelmät kuten kysyntäjouston mahdollistamat ohjelmistot. Suomessa on lähiaikoina valtion toimeenpanemana aloitettu useita eri aloja koskevia digitalisaatioprojekteja, joista yksi on sähkön vähittäismarkkinoita varten toteutettava datahub-järjestelmä [2][10].

Datahubin tarkoituksena on valmistuessaan toimia keskitettynä tiedonvaihtojärjestelmänä kaikille sähkön vähittäismarkkinoiden markkinaosapuolille [11][12]. Toisin sanoen, datahubin käyttöönoton jälkeen esimerkiksi kaikki sähkönmyyntisopimukset ja mittaustiedot tulevat liikkumaan osapuolilta järjestelmään. Samalla se tulee tallentamaan sähkönkulutus-, asiakas- ja osoitetiedot Suomen 3,7 miljoonasta sähkönkäyttöpaikasta tukeakseen sähkön vähittäismarkkinoilla suoritettavia toimintoja kuten edellä mainittua sähkösopimusten laatimista. Järjestelmää tulee hallinnoimaan suomalaisen kantaverkkoyhtiö Fingrid Oyj:n tytäryhtiö Fingrid Datahub Oy ja se on suunniteltu käyttöönotettavaksi vuonna 2022 [11][13]. Datahubin toteutus ja sen valmistumisen jälkeinen käyttö ovat Fingrid Datahubin sekä muiden sähkön vähittäismarkkinoiden osapuolten lakisääteisiä velvollisuuksia [14]. Nämä velvollisuudet on kirjattu osaksi toimialaa säätelevää sähkömarkkinalakia. Sähkömarkkinalaki velvoittaa myös Fingrid Datahubia suojelemaan järjestelmää ja varmistamaan sen oikeanlainen toiminta. Tähän velvollisuuteen kuuluu oleellisesti datahubin tietoturvan asianmukainen järjestäminen.

Tietoturvan kehittämisen tarve energia-alan tietojärjestelmille on koettu tarpeelliseksi jo pidemmän aikaa [15][16][17]. Tietoturvahyökkäysten nähdään yleisesti lisääntyvän ja muuttuvan taitavammin tehdyiksi ympäri maailmaa [18][19]. Lisäksi energianjakelun järjestelmät sekä energian tuotanto- ja siirtojärjestelmät määritellään yleisesti niin sanotuksi kriittiseksi infrastruktuuriksi [20][21][22]. Valtioneuvosto määrittelee kriittisen infrastruktuurin "perusrakenteiksi, palveluiksi ja niihin liittyviksi toiminnoiksi, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi" [20, s. 4]. Energiasektorilla on myös keskeinen rooli muussa kriittisessä infrastruktuurissa siksi, että se mahdollistaa muun kriittisen infrastruktuurin toimivuuden [21]. Tämä tekee energiasektorin kiinnostavaksi kohteeksi rikollisryhmille, terroristeille ja valtioiden tukemille hyökkääjille.

Vaikka esimerkiksi sähkönmyyjät sekä erilaiset palveluntarjoajat eivät omista kriittistä infrastruktuuria, kasvava digitalisointi lisää näiden yhteyttä koko ajan muun muassa jakeluverkkoyhtiöihin [17]. Löyhemmin sidoksissa olevat yhteistyökumppanit saattavat päätyä iskujen kohteiksi hyökkääjän etsiessä tietä varsinaiseen kohteeseensa [23]. Sähkömarkkinoiden mekanismien kehittyessä niiden toiminta myös integroituu keskeisemmäksi osaksi tavanomaisen kriittisen infrastruktuurin toimintaa, hämärtäen näiden rajoja ja tehden markkinoiden häiriöttömästä toiminnasta kriittisempää [24]. On jo tavallista, että rikolliset kohdistavat tietoturvahyökkäyksiä markkinatoimijoita kohtaan hyödyn tavoittelemiseksi [18][19]. Datahubin käyttöönoton myötä myös se itse tulee olemaan yksi

hyökkääjiä kiinnostavista kohteista järjestelmän toiminnan ollessa keskeistä sähkömarkkinoiden toiminnalle. Se tulee olemaan myös yksi tärkeä tekijä edellä mainitussa tavanomaisen kriittisen infrastruktuurin sekä markkinatoimintojen integroitumisessa.

Aiemmin mainittu sähkömarkkinalaki ei kuitenkaan ole täsmällinen siinä, mitä datahubin tietoturvan asianmukainen järjestäminen tarkoittaa [14]. Yllä mainitun toimialaa koskevan yleisen uhkatilanteen valossa voidaankin esittää kysymys siitä velvoittaako sähkömarkkinalaki Fingrid Datahubin vaatimaan datahubiin liittyviltä osapuolilta tietoturvatoimia. Datahubin yhdistäessä kaikki sähkömarkkinoiden osapuolet itsensä kautta toisiinsa on selvää, että monet datahubiin kohdistuvista tietoturvahyökkäyksistä saattavat tulla muun muassa kytkeytyvien osapuolten kautta. Toisaalta laki asettaa myös rajoitteita osapuolille kohdistettaville vaatimuksille. Datahubin on tarkoitus toimia koko toimialaa hyödyttävänä järjestelmänä niin, että se ei syrji esimerkiksi pienempiä toimijoita. Tasapainon löytäminen turvallisuuden sekä markkinoiden tehokkuuden välillä on yksi Fingrid Datahubin tunnistamista haasteista koskien datahub-järjestelmän käyttöönottoa.

1.1 Tavoitteet ja niiden toteutumisen määritelmä

Tämän työn tavoite on selvittää, millaista tietoturvan tasoa datahubiin liittyviltä markkinaosapuolilta pitää vaatia. Datahub-järjestelmän oma tietoturva rajataan pois työn laajuudesta. Tavoitteeseen pyritään seuraavien osavaiheiden kautta:

- Osoitetaan työn tärkeys voimassa olevan lainsäädännön tulkinnan sekä yleisten tietoturvauhkien vakavuuden valossa.

- Tehdään tarpeeksi kattava arvio niistä datahubiin kohdistuvista riskeistä, joita liittyvät osapuolet voivat siihen kohdistaa. Tämä riskiarvio suoritetaan turvallisuuden vuoksi Fingrid Datahubissa sisäisesti.

- Tutkitaan tietoturvavaatimusten määrittämisen menetelmiä erilaisissa viitekehyksissä, kuten kirjallisuudessa ja käytännössä. Tätä osuutta nimitetään työssä tästä eteenpäin "kirjallisuustutkimukseksi".

- Edellä mainitun riskiarvion ja kirjallisuustutkimuksen pohjalta luodaan viitekehys, jolla voidaan lähestyä datahubiin liittymistä varten vaadittavia tietoturvakäytäntöjä. Viitekehys toteutetaan sellaisten tietoturvavaatimuksien listana, jotka nähdään datahubiin liittymisen kannalta tarpeellisiksi, sekä ohjeistuksina kuinka niitä tulisi soveltaa.

- Viimeiseksi, viitekehys käydään läpi eri datahubin tuntevien asiantuntijoiden kanssa niin monta kertaa, että saavutetaan yksimielisyys viitekehyksen sopivuudesta sen tehtävään.

Rajauksena edellä mainituille tietoturvavaatimuksille on osapuolien taloudellinen ja teknologinen syrjimättömyys. Kaikkien osapuolten on pystyttävä toteuttamaan määritellyt tietoturvavaatimukset ilman, että ne kokevat vakavia tai keskenään epäsuhtaisia rasitteita liiketoiminnassaan. Samasta syystä pyritään myös vaatimusten teknologianeutraaliuteen niin, ettei yksi osapuoli voi saada markkinaetua toiseen nähden teknologiasijoitustensa vuoksi. Työn lopputuloksena muodostettavia tietoturvavaatimuksia on tarkoitus soveltaa

palvelusopimuksessa, jonka allekirjoittamista tullaan vaatimaan datahubiin liittyviltä osapuolilta.

1.2 Rakenne ja metodologia

Tutkimusmenetelmänä käytetään kirjallisuustutkimusta ja haastatteluja. Tämä tehdään seuraavasti: Ensin esitetään työn tavoitteiden yhteys voimassa olevaan lainsäädäntöön. Tämän lisäksi tarkastellaan hieman sähkön vähittäismarkkinoiden osapuolia sitovaa lainsäädäntöä sen osalta, miten se ohjaa niiden tietoturvaa. Seuraavaksi esitellään datahubjärjestelmä ja sen rooli vanhan sanomaliikenteen korvaajana sähkön vähittäismarkkinoilla. Samalla esitellään sen tulevat käyttäjät siltä osin, miten ne tulevat käyttämään datahubia sekä miten tämä käyttö tulee tapahtumaan teknisesti osapuolten järjestelmän ja datahubin välillä. Tämän jälkeen tutkitaan tietoturvauhkiin liittyvää kirjallisuutta ja tutkimusta, pyrkien hahmottamaan markkinaosapuolia kohtaavat tietoturvauhat ja niiden vakavuudet. Tästä siirrytään luomaan katsaus saatavilla olevaan lähdekirjallisuuteen koskien tietoturvan asianmukaista määrittämistä erilaisille järjestelmille. Kirjallisuuskatsauksen jälkeen esitetään tämän työn lopputuloksena koottu viitekehys, sen tarkoituksenmukainen sovellustapa sekä sen muodostamat tietoturvavaatimukset perusteluineen. Lopputulosten esittelyn jälkeen käsitellään edellisessä luvussa määritellyn tietoturvan todentamista ja sen haasteita. Työ päättyy yhteenvetoon tärkeimmistä huomioista ja tuloksista.

2 Laki ja datahubiin liittyvät velvoitteet

Tässä luvussa esitetään perustelut sille, miksi Fingrid Datahubin velvollisuuksiin kuuluu lakisääteisesti asettaa datahubiin liittyville osapuolille erillisiä tietoturvavaatimuksia. Aluksi luodaan katsaus yksityiskohtaisemmin johdannossa mainitun sähkömarkkinalain mukaisiin velvollisuuksiin koskien Fingrid Datahubia. Lain tulkinnassa kiinnitetään erityisesti huomiota niihin asioihin, jotka liittyvät datahubin tietoturvan suojaamiseen. Samalla luodaan katsaus myös niihin määräyksiin, jotka asettavat rajoitteita Fingrid Datahubille koskien sen kykyjä esittää vaatimuksia datahubiin liittyville markkinaosapuolille.

Lopuksi tullaan katsomaan tarkemmin, mitä velvoitteita muu voimassa oleva lainsäädäntö kohdistaa näihin osapuoliin jo ennen datahubin käyttöönottoa. Tässä kohdassa kiinnitetään huomiota siihen, määrääkö voimassa oleva lainsäädäntö osapuolten tietoturvan jo tyydyttävälle tasolle datahubin käyttöä ajatellen. Lisäksi arvioidaan, kuinka varmoja voidaan olla siitä, että toimiala seuraa annettua lainsäädäntöä.

2.1 Fingrid Datahub Oy:n vastuu lainsäädännössä

Sähköenergian vähittäismarkkinoita säätelee Suomessa niitä varten määrätty sähkömarkkinalaki [14]. Vuonna 2013 laki uudistettiin velvoittamaan kantaverkkoyhtiö Fingrid Oyj:tä kehittämään sähkökaupan sekä siihen oleellisesti kuuluvan taseselvityksen vaatimaa tiedonvaihtoa [10]. Muutoksen myötä yritys aloitti vuonna 2014 selvityksen erilaisista tarjolla olevista kehitysvaihtoehdoista. Tämän selvityksen sekä sidosryhmien kuulemisen pohjalta Työ- ja elinkeinoministeriö päätyi huhtikuussa 2015 pyytämään Fingridiä aloittamaan sähkökaupan keskitetyn tiedonvaihdon järjestelmän toteutuksen. Toteutus aloitettiin, ja järjestelmä sai nimen datahub.

Datahubin toteuttamisesta on säädetty sähkömarkkinalaissa. Sähkömarkkinalain 49 a §:n mukaan Fingridin on sekä järjestettävä datahubin toteutus, että huolehtia sen toiminnasta, muun muassa tietoturvasta. Pykälän mukaan tietoturva on järjestettävä asianmukaisesti niin, että sähkön vähittäismarkkinoiden tehokkaan toiminnan edellytykset voidaan turvata (momentti 2) [14]. Pykälän 3 momentissa täsmennetään tätä ja määrätään Fingrid huolehtimaan siitä, että “sen tietojärjestelmissä käsiteltävien henkilötietojen ja liikesalaisuuksien sekä maanpuolustuksen, poikkeusoloihin varautumisen ja väestönsuojelun sekä tieto- ja viestintäjärjestelmien turvajärjestelyjen kannalta arkaluontoisten tietojen tietoturva on järjestetty asianmukaisesti”. Pykälän 4 momentin kohdissa 1, 2 ja 3 taas määrätään, että järjestelmän riskienhallinnassa otetaan huomioon järjestelmien (ja tilojen) turvallisuus, tietoturvauhkien ja häiriöiden käsittely sekä liiketoiminnan jatkuvuuden hallinta.

Edellä mainitun sähkömarkkinalain 49 a §:n momentissa 3 annettu määräys järjestää tietoturva asianmukaisesti sekä riskienhallintaa koskevat määräykset nostavat kuitenkin kysymyksiä lain tulkinnasta. Ei esimerkiksi ole itsestäänselvää, mitä asianmukaisesti järjestetty tietoturva tarkoittaa. Tätä kysymystä lähestyessään Fingrid Datahub on sisäisissä riskiarvioissaan todennut datahubiin liittyvien osapuolten kohdistavan tietoturvauhkia datahubiin [25][26][27]. Suuri osa datahubiin kohdistuvista riskeistä ei johdu osapuolten itsensä tarkoituksenmukaisesta toiminnasta, vaan osapuolien järjestelmien mahdollisesta hyväksikäytöstä. Osapuolia voidaan esimerkiksi käyttää hyökkäysrajapintana datahubia kohtaan. Tällä tarkoitetaan sitä, että datahubille vihamielinen osapuoli saattaa yrittää esimerkiksi kaapata osapuolen datahub-yhteyden, jotta se pääsisi aloittamaan varsinaisen tietoturvahyökkäyksensä datahubiin itseensä. Toisaalta on myös otettava huomioon, että jotkin vihamieliset tai osittain rikollisia tarkoitusperiä omaavat osapuolet saattavat pyrkiä

hankkimaan varmennetun datahub-yhteyden ja käyttää datahubia väärin. Nämä seikat huomioon ottaen sähkömarkkinalain 49 a § tulee luonnollisesti tulkita siten, että Fingrid Datahubin velvollisuuksiin kuuluu muun muassa asettaa tietoturvavaatimuksia datahubiin liittyville markkinaosapuolille.

Fingrid Datahub ei kuitenkaan voi määritellä liittymiselle asetettavia vaatimuksia harkitsemattomasti. Pykälän 3:ssa momentissa painotetaan sitä, että Fingrid Datahubin palvelujen tarjonta tulee olla tasapuolista ja syrjimätöntä eri markkinaosapuolille [14]. Myös lain 49 §:ssä määrätään syrjimättömyys ja tasapuolisuus koskemaan koko Fingridin järjestämää tiedonvaihdon kehittämisprosessia, ja sallimaan myös pienimuotoisen sähköntuotannon verkkoon pääsy sekä lisäarvopalvelujen kuten kysyntäjouston kehityksen edistäminen. Nämä määräykset voidaan tulkita siten, että vaikka tietoturva koskee kriittisimmissä tapauksissaan jopa maanpuolustusta, on tietoturvan valvonta pyrittävä järjestämään niin että negatiivinen vaikutus tehokkaiden markkinoiden toteutumiseen minimoituu. Tämän tasapainon löytäminen on yksi tämän työn avainkysymyksistä. Työ tulee lähestymään minimitietoturvavaatimuksia sekä niiden valvontaa niin, että lopulliset ehdotukset pyrkivät mahdollistamaan markkinoiden tehokkuuden mahdollisimman monella alueella pitäen kuitenkin tietoturvan ensimmäisenä prioriteettina. Jos valinta on tehtävä varteenotettavan tietoturvauhan minimoinnin ja suhteellisen kohtuullisen markkinarasitteen välillä tullaan ensimmäistä vaihtoehtoa suosimaan jälkimmäisen kustannuksella.

2.2 Markkinaosapuolia koskeva muu lainsäädäntö

Datahubiin liittyviin markkinaosapuoliin kohdistuu jo ennalta joitakin tietoturvaan liittyviä lakisääteisiä velvoitteita. Keskeisimmät näistä tulevat Euroopan unionin (EU) tasolta, kuten yleinen tietosuoja-asetus (GDPR, englannin sanoista General Data Protection Regulation) [28]. Suomessa yleistä tietosuoja-asetusta täydentää myös tietosuojalaki [29]. Yleinen tietosuoja-asetus ja tietosuojalaki velvoittavat henkilötietoja säilyttävien ja käsittelevien tahojen noudattavan tiettyjä säännöksiä niille luovutettuja tietoja koskien [28][29]. Henkilötietojen säilyttäjistä käytetään termiä rekisterinpitäjä [30]. Monessa tapauksessa Suomen sähkömarkkinoilla samoilla tahoilla on rekisterinpitäjän ja käsittelijän roolit esimerkiksi myyjien tallentaessa ja hallinnoidessa asiakastietojaan. On kuitenkin tilanteita, joissa tietojen käsittelijä saatetaan ulkoistaa esimerkiksi valtuuttamalla kolmas osapuoli hoitamaan yrityksen laskutusta. Näissä tapauksissa valtuutetut käsittelijät tulee sitoa myös rekisterinpitäjään kohdistuviin määräyksiin sopimuksen kautta.

Yleinen tietosuoja-asetus ja tietosuojalaki velvoittavat rekisterinpitäjiä ja käsittelijöitä muun muassa toteuttamaan asianmukaiset ja tarvittavat tekniset sekä organisatoriset toimet tietojen suojelemiseksi [28][29]. Näihin kuuluvat muun muassa tietojen oikeanlainen hävittäminen sekä käsittelyn tarpeeksi tyydyttävä läpinäkyvyys [28][29][30]. Nämä säädökset ovat olleet olemassa jo vuodesta 2016 ja ne koskevat ainakin osittain lähes kaikkia sähkömarkkinoiden osapuolia näiden toiminnan liittyessä erottamattomasti henkilötietoihin. Täten voitaisiin odottaa, että osapuolet kykenevät henkilötiedon käsittelyn ja suojaamisen osalta hyvään tietoturvaan, eikä datahubin käyttöönotto toisi tähän muutosta. Asiasta ei kuitenkaan voida tehdä vahvoja ja yleistäviä oletuksia. Yleisen tietosuoja-asetuksen ja tietosuojalain toteutumista eri tahojen kohdalla valvoo tietosuojavaltuutettu [30]. Tietosuojavaltuutettu ei ole tähän mennessä toimeenpannut kattavia selvityksiä siitä, millä tasolla sähköalan toimijat noudattavat näitä. Voidaan siis nähdä, että henkilötiedon käsittelyn osalta datahubin on vaadittava joitakin vastuita osapuolille järjestelmässä liikkuvan henkilötiedon suojaamiseksi.

EU:n verkko- ja tietoturvadirektiivissä, joka tunnetaan myös nimellä Network and Information Systems (NIS) -direktiivi, annetaan myös ohjeistuksia jäsenvaltioiden eri yritysten tietoturvalle [31][32]. Suomessa direktiivi on sähkömarkkinoiden osalta implementoitu sisällyttämällä sähkömarkkinalakiin vain yksi pykälä, sähkömarkkinalain 29 a § [14][30]. Lakipykälä koskettaa ainoastaan sähkömarkkinoilla toimivia verkkoyhtiöitä kuten Fingridiä ja jakeluverkkoyhtiöitä. Käytännössä se velvoittaa verkkoyhtiöt vastaamaan viestintäverkkojensa ja tietojärjestelmiensä riskienhallinnasta sekä ilmoittamaan näihin liittyvistä häiriöistä Energiavirastolle sellaisissa tilanteissa, joissa sähkönjakelu voi keskeytyä jakeluverkossa laajasti. Vaikeissa tietoturvatilanteissa ilmoitus menisi myös kyberturvallisuuskeskukselle, joka toimii kansallisena Computer Security Incident Response Team (CSIRT) -toimijana [30][33]. CSIRT-toimijat ovat tietoturvaloukkauksiin reagoivia ja niitä tutkivia ryhmiä, joita NIS-direktiivi ohjaa jokaisen Euroopan unionin jäsenmaan määräämään vähintään yhden yksikön [32]. Voidaan siis olettaa, että datahubiin liittyvistä markkinaosapuolista ainakin jakeluverkkoyhtiöt ovat valmistautuneet raportointiin vakavien tietoturvaloukkausten sattuessa. Lakipykälä ei kuitenkaan ota kantaa sähkönmyyjiin eikä kolmansiin osapuoliin, ja on todettava, että myös tietoturvaloukkaukset, jotka saattaisivat katkaista sähkönjakelun laajalta alueelta voivat olla silti vakavia muista syistä. Esimerkiksi mittauslukemien korruptoituminen jakeluverkonhaltijan järjestelmissä voi aiheuttaa vakavia taloudellisia seurauksia, vaikka ne eivät suoraan vaikuta sähkönjakeluun [27][34].

Sähkömarkkinalaissa on myös joitakin muita kohtia, jotka ottavat hyvin yleisellä tasolla kantaa toimijoiden tietoturvaan. Esimerkiksi sähkömarkkinalain 75 b §:n mukaan sähköalan yhtiöiden on ylläpidettävä ja kehitettävä eri toimintojaan niin, että asianmukainen tietoturva täyttyy [14]. Tämä määräys on kuitenkin ympäripyöreä, ja jättää avoimeksi sen miten asianmukainen tietoturva määritetään. Kuten edellä sivuttiin, yleisen tietosuoja-asetuksen, tietosuojalain sekä sähkömarkkinalain 29 a §:n tulkinnoilla on samanlaisia ongelmia, kun mietitään yltääkö sähkömarkkinoiden osapuolien tietoturva tarpeelliselle tasolle datahubia varten [30]. Lisäksi yleistä tietosuoja-asetusta, tietosuojalakia ja edellä mainittuja lakipykäliä koskee yksi yhteinen hyvin konkreettinen datahubin tietoturvaan kohdistuva ongelma. Jokaiseen edellä mainittuun velvoitteita asettavaan tekijään on määritelty tarkasti taho, jolle osapuolet on velvoitettu tarvittaessa raportoimaan. Mikään näistä tahoista ei ole Fingrid Datahub tai siihen välttämättä suoraan yhteydessä oleva taho. Tehokkaan tietoturvan varmistamiseksi on tärkeää, että osapuolet toteuttavat nimenomaan datahubin käyttöön liittyviä riskejä vastaavan tietoturvan sekä ovat velvollisia olemaan yhteydessä näistä asioista Fingrid Datahubin kanssa. Tämän sekä muiden yllä olevien näkökulmien valossa on selvää, että vaikka voimassa oleva lainsäädäntö saattaa parantaa markkinaosapuolten tietoturvaa, se ei datahubin kannalta ole riittävä. Osapuolten luotetaan kuitenkin tuntevan voimassa olevat lakisääteiset velvoitteensa. Täten tässä työssä tietoturvavaatimuksien käsittelyn turhaa päällekkäisyyttä edellä mainitun lainsäädännön kanssa pyritään välttämään. Esimerkiksi henkilötiedon suojaamiseen tullaan puuttumaan enemmän datahubin oikeanlaisen toiminnan varmistamisen kannalta ottamatta siihen kantaa yhtä laajasti kuin yleisessä tietosuoja-asetuksessa ja tietosuojalaissa.

3 Datahub-järjestelmä ja sen käyttäjät

Jotta voitaisiin analysoida osapuolten aiheuttamia uhkia datahubille ja näin ollen niille tarpeelliseksi nähtyjä vaatimuksia, on datahubin toimintaperiaatteet ymmärrettävä riittävällä tavalla. Tässä luvussa kuvataan tarkemmin, mikä datahub-järjestelmä on ja miten se toimii markkinaosapuolten käytössä. Ensin esitellään datahubin tuleva rooli sähkömarkkinoilla sekä ne markkinamekanismit, jotka se tulee korvaamaan. Seuraavaksi esitellään tarkemmin datahubiin liittyvät osapuolet ja miten ne tulevat käyttämään järjestelmää. Lopuksi esitellään teknisempi kuvaus siitä, miten osapuolten ja datahubin välinen kommunikaatio sekä markkinaprosessien suoritus datahubissa tulevat tapahtumaan.

3.1 Datahubin rooli sähkömarkkinoilla

Sähkömarkkinoiden keskeinen toimintamekanismi on markkinaprosessien suorittaminen välittämällä sanomia eri osapuolten kesken [35]. Tätä osapuolten välistä kommunikaatiota markkinoilla tapahtuvista toimenpiteistä kutsutaan yleisesti sanomaliikenteeksi. Kun asiakas esimerkiksi allekirjoittaa sopimuksen sähkönmyyjän kanssa, lähettää sähkönmyyjä tästä digitaalisen sanoman asiakkaan jakeluverkon haltijalle [36]. Jakeluverkonhaltija reagoi sanomaan varmistamalla asiakkaan nykyiseltä myyjältä, jos tällainen on olemassa, voiko uuden sopimuksen tehdä. Jos uusi sopimus on sallittu tehdä, osapuolet rekisteröivät muutokset asianmukaisesti omiin järjestelmiinsä. Sanomaliikenne toimii kulmakivenä myös muille markkinoilla tapahtuville jokapäiväisille toiminnoille. Jakeluverkonhaltijat esimerkiksi vastaanottavat säännöllisesti toteutuneet sähkönkulutuslukemat hallinnoimistaan sähkömittareista. Tämän jälkeen ne ilmoittavat kulutustiedot omilla digitaalisilla sanomillaan myyjille ja muille asianmukaisille tahoille.

Nykyinen sanomaliikenne suomalaisilla sähkön vähittäismarkkinoilla tapahtuu noin 20 vuotta sitten käyttöönotetun hajautetun tiedonvaihdon mukaisesti [37]. Teknisesti tämä tarkoittaa sitä, että osapuolet lähettävät itsenäisesti tai yhteistyökumppaniensa kautta sanomia jokaiselle liikekumppanilleen erikseen. Sanomat noudattavat Electronic Data Interchange For Administration, Commerce and Transport (EDIFACT) -nimistä sähköistä tiedonsiirtokieltä. Sanomien välitys tapahtuu tarkoituksen mukaisten operaattoreiden kautta hyödyntäen File Transfer Protocol (FTP) -menetelmää Transmission Control Protocol (TCP) -yhteyden yli. Tässä menettelytavassa on kuitenkin useita heikkouksia. Tällä hetkellä sanomaliikenteen laatua ja toimivuutta ei valvota keskitetysti, joten jokainen markkinaosapuoli on itse vastuussa omasta tietoturvastaan ja mahdollisten loukkausten seurannasta [35]. Tämän lisäksi joihinkin suosituksiin ja menettelyohjeisiin sisältyy tulkinnan varaa. Nämä saattavat johtaa tilanteeseen, jossa osia sanomaliikenteestä häiriintyy tai prosesseissa esiintyvät puutteet aiheuttavat kitkaa markkinaosapuolten välillä. Vastuuta sanomaliikenteen toiminnasta voi kuitenkin olla vaikeata langettaa millekään tietylle taholle.

Datahub tulee käyttöönottonsa myötä muuttamaan sanomaliikenteen luonteen merkittävästi [13]. Sen sijaan, että osapuolet lähettävät toisilleen sanomansa suoraan avaten mahdollisesti useita yhteyksiä eri järjestelmiin, ne tulevat toimittamaan muille osapuolille välitettävät sanomat ainoastaan datahubiin. Monien välitettävien tietojen kohdalla lähettäjän ei tarvitse erikseen määrittää omassa järjestelmässään jokaista oikeutettua vastaanottajaa, vaan datahub tunnistaa nämä automaattisesti [35]. Datahub ottaa sanomat vastaan niin sanottuina Simple Object Access Protocol (SOAP) eXtensible Markup Language (XML) -sanomina tähän tarkoitetussa Business to Business (B2B) -rajapinnassaan [38]. Viestit siirtyvät rajapinnasta datahubin sisäisiin järjestelmiin, joissa viestien käsittely tapahtuu.

Lopulta datahub toimittaa viestit tai niitä koskevan tarpeellisen tiedon oikeille osapuolille.

Osapuolten sanomien välityksen yhteydessä datahub tallentaa tarvittavat tiedot viesteistä omaan rekisteriinsä. Tämä vuorostaan tehostaa ja varmistaa tulevien markkinaprosessien toimivuuden esimerkiksi siten, että osapuolen liiketoiminnan vaatimat tiedot löytyvät valmiiksi datahubista jos osapuoli on oikeutettu tähän [13][35]. Monet prosessit, jotka tällä hetkellä riippuvat osapuolien manuaalisesta vahvistamisesta ja käsittelystä, tulevat automaattisiksi ja synkronisiksi [12][13][35]. Esimerkiksi myyjän vaihdossa uusi myyjä saa vahvistuksen ja tarvittavat tiedot asiakkaastaan datahubista heti ilmoittaessaan uudesta sopimuksesta. Koska kaikki markkinaprosessit käsitellään samalla lailla ja tasavertaisesti osapuolten väliltä poistuu vaara väärinymmärryksistä ja tulkintaerojen synnyttämistä eroavaisuuksista osapuolten toiminnassa sanomaliikenteessä. Yksinkertaistamalla ja tehostamalla prosesseja datahubin on tarkoitus tukea sähkömarkkinoita ja edistää kilpailukykyä.

3.2 Datahubiin kytkeytyvät osapuolet

Datahub tulee jakamaan siihen kytkeytyvät markkinaosapuolet karkeasti ottaen sähkön vähittäismyyjiin, jakeluverkonhaltijoihin sekä kolmansiin osapuoliin [39]. Sähkönmyyjien pääasiallisiin toimintoihin datahubissa tulevat kuulumaan myyntisopimusten luonti ja hallinnointi sekä asiakastietojen ylläpito [12]. Myyjät voivat myös pyytää sähköjen katkaisua jakeluverkkoyhtiöltä esimerkiksi laskujen perintätilanteissa, sekä jälleenkytkentää maksuvelvoitteiden täyttyessä. Datahub tulee tehostamaan myyjien toimintaa sen sisältäessä valmiiksi myyjille hyödyllistä tietoa esimerkiksi sopimuksen luonnin aikana. Tällaista tietoa ovat esimerkiksi asiakkaan käyttöpaikka-, verkkotuote- ja mittaustiedot. Asiakkaan valtuuttamana myyjä voi hakea tämän tiedon datahubista ennen sopimuksen luomista ja räätälöidä asiakkalleen sopivan tuotteen. Samalla myyjiltä poistuu monia nykyisin ongelmaksi koettuja tilanteita. Esimerkkinä tästä on tilanne, jossa myyjän on pääteltävä, onko sopimuksen luonnissa kyseessä asiakkaan muutto vai myyjänvaihto. Datahubin sisältäessä aina käyttöpaikan tilatiedot valmiiksi myyjien ei tarvitse käyttää ylimääräisiä resursseja tämän selvittämiseen erikseen.

Jakeluverkonhaltijat ovat sähköverkkotoimintaa harjoittavia markkinaosapuolia, jotka hallinnoivat jakelu- ja/tai suurjännitteistä jakeluverkkoa [12][40]. Jakeluverkoiksi lasketaan ne sähköverkot, joiden nimellisjännite on pienempi kuin 110 kilovolttia, kun taas 110 kilovoltin nimellisjännitteellä toimivia verkkoja kutsutaan suurjännitteisiksi jakeluverkoiksi. Jakeluverkonhaltijoiden tärkeimpiä datahubiin siirtyviä toiminnallisuuksia ovat erilaisten rakenteellisten tietojen kuten käyttöpaikkojen, rajapisteiden ja tuotantoyksiköiden hallinta sekä verkkosopimusten hallinta [12]. Jakeluverkonhaltijat ovat myös vastuussa mittaustietojen toimittamisesta datahubiin, josta ne välitetään automaattisesti edelleen oikeille osapuolille. Suorittaessaan käyttöpaikkojen sähköjen kytkentöjä tai katkaisuja jakeluverkonhaltija tulee toimittamaan datahubin kautta ilmoitukset tästä asianmukaisille osapuolille, kuten käyttöpaikan asukkaiden sähkönmyyjälle. Itse kytkentöjä tai katkaisuja jakeluverkonhaltija ei tee datahubin avulla, vaan ainoastaan kytkennän tilaan liittyvän kommunikaation [13].

Taulukossa 1 on kuvattu sähkön vähittäismyyjien ja jakeluverkonhaltijoiden pääasialliset sekä toissijaiset toiminnot datahubissa [39]. Taulukko ei kuvaa yksityiskohtaisesti jokaista komentoa, jonka osapuoli voi suorittaa datahubissa omassa roolissaan. Esimerkiksi myyjien kohdalla käyttöpaikka- ja asiakastietojen haulle on olemassa omat komentonsa

nykyisille ja uusille myyjille. Toiminnot ovat selkeyden vuoksi kuvattu tarpeeksi yleisluontoisella tasolla esitykseksi siitä, mihin markkinaosapuolet tulevat datahubia käyttämään.

Taulukko 1. Vähittäismyyjien sekä jakeluverkonhaltijoiden toiminnot.

	Vähittäismyyjät	**Jakeluverkonhaltijat**
Pääasialliset toiminnot	Myyntisopimusten luonti, päättäminen ja tietojen ylläpito	Verkkosopimuksen vahvistaminen, tietojen päivitys, peruutus ja päättäminen
	Toimituksen kytkentä- ja katkaisupyynnöt	Ilmoitus toimituksen kytkennästä ja katkaisusta
	Asiakastietojen ylläpito	Verkkosopimukseen liitetyn tuotetiedon ylläpito
	Käyttöpaikkatietojen haku	Käyttöpaikkojen, tuotantoyksiköiden ja rajapisteiden luonti, poisto sekä tietojen ylläpito
	Mittaustietojen ja taseselvitystietojen haku	Mittaustiedon toimitus datahubiin
		Taseselvitystietojen sekä häviöihin kirjattujen kulutusten ja tuotantojen haku
Toissijaiset toiminnot	Asiakkaan valtuutuksen ilmoitus asiakas- ja käyttöpaikkatietojen hakuun	Asiakkaan valtuutuksen ilmoitus asiakas- ja käyttöpaikkatietojen hakuun
	Osapuolitietojen haku	Osapuolitietojen haku
	Laskurivitietojen ilmoitus (laskutustavasta riippuen)	Laskurivitietojen ilmoitus (laskutustavasta riippuen)
	Laskurivitietojen haku	Laskurivitietojen haku
	Käyttöpaikkatietojen päivityspyynnöt	Asiakastietojen päivityspyynnöt

Kolmannet osapuolet ovat sekalaisempi joukko erilaisia palveluntarjoajia [39]. Ne ovat muita jakeluverkonhaltijoita, sähkönmyyjiä tai täysin muilla tavoin liiketoimintaa harjoittavia tahoja. Ne käyttävät datahubia silloin, kun loppuasiakas tai toinen markkinaosapuoli valtuuttaa ne suorittamaan joitakin toimintoja puolestaan. Mahdolliset toiminnot kolmannen osapuolen valtuuttamiseksi on listattu taulukossa 1. Näihin kuuluvat kolmannen osapuolen valtuutuksen ilmoitus datahubiin valtuuttajan puolesta sekä erilaisten tietojen hakeminen. Kolmannet osapuolet voivat kuitenkin saada toimeksiannon toiselta markkinaosapuolelta, joka eroaa prosessina taulukossa esitetyistä valtuutuksella suoritettavista toiminnoista. Jos toinen markkinaosapuoli antaa toimeksiannon kolmannelle osapuolelle, tämä markkinaosapuoli voi antaa kolmannelle osapuolelle oikeudet suorittaa samoja toimintoja datahubissa kuin se itse. Esimerkkinä tästä on esimerkiksi mittaustiedon toimitus datahubiin jakeluverkonhaltijan puolesta. Toimeksianto markkinaosapuolelta toiselle tapahtuu siten, että toimeksiannon saaja tekee sopimuksen sekä toimeksiantajan, että data-

hubin kanssa. Toimeksiannon saajan suorittaessa esimerkiksi edellä mainitun mittaustiedon toimituksen datahubiin tarkistetaan sanoman juridisen lähettäjän eli toimeksiannon antajan oikeellisuus, sekä sanoman teknisen lähettäjän toimeksiannon voimassaolo.

Kolmansien osapuolten toiminnot on listattu Taulukkoon 2 erilleen muista, koska niitä ei voi luokitella pääasiallisiin tai toissijaisiin toimintoihin mielekkäästi [35]. On huomioitavaa, että kolmansien osapuolien kohdalla esiin on nostettu vain toiminnot, joita asiakas, myyjä tai jakeluverkonhaltija voi sille valtuuttaa. Käytännössä sähkönmyyjä tai jakeluverkonhaltija voi antaa kolmannelle osapuolelle toimeksiantona luvan suorittaa minkä tahansa omista toiminnoistaan [35].

Taulukko 2. Kolmansien osapuolten toiminnot datahubissa asiakkaan, myyjän tai jakeluverkonhaltijan valtuuttamana [39][41].

	Kolmannet osapuolet	
Osapuolen tai asiakkaan valtuuttamana	Asiakkaan valtuutuksen ilmoitus	Asiakastietojen päivityspyyntö
	Käyttöpaikkatietojen haku	Asiakastietojen haku
	Mittaustietojen haku	Tuotetiedon haku
	Hintatietojen haku	Laskurivitietojen haku
	Osapuolitietojen haku	

3.3 Datahubin toiminta

Jokainen markkinaosapuolen datahubissa suorittama markkinaprosessi voidaan ajatella SOAP XML-viestin lähettämisenä datahubin tarjoamaan B2B-rajapintaan [38]. Toimintamalli on teknisesti suureksi osaksi aina samanlainen, mutta joissain tapauksissa saattaa esiintyä pieniä eroja. Tällaisia eroja voivat olla esimerkiksi se, käsitelläänkö prosessi asynkronisesti vai synkronisesti. Asynkronisissa prosesseissa ensisijaisen sanoman välityksen jälkeen datahub jatkaa prosessin käsittelyä ja välittää ilmoituksia osapuolen järjestelmään käsittelyn edetessä. Tällöin viestin ensisijainen vastaanotto saattaa esimerkiksi onnistua, mutta käsittely voi epäonnistua myöhemmin, jolloin datahub ilmoittaa erikseen kummastakin. Prosessit ovat yleisesti kuitenkin synkronisia prosesseja, joissa datahub vaihe kerrallaan vastaanottaa sanoman, tarkastaa sen oikeellisuuden, suorittaa sen ja palauttaa osapuolen järjestelmään vahvistuksen suorituksesta. Jotkin prosesseista saattavat myös ennen sanoman muodostusta kerätä tietoa markkinaosapuolen muista järjestelmistä. Yksityiskohtaisemmin prosessi toimisi edellä tehdyin oletuksin seuraavanlaisesti [38][42]:

0. Vaihtoehtoisessa tiedonkeräämisvaiheessa osapuoli kerää muista järjestelmistään tietoja prosessin suoritusta varten. Tällainen prosessi voisi esimerkiksi olla uuden myyntisopimuksen tai käyttöpaikan luonti, jossa prosessin aloittava SOAP-viesti tarvitsee tietoja osapuolen asiakastietojärjestelmästä tai muusta rekisteristä.

1. Tarvittavan sisällön kokoamisen jälkeen osapuolella on oltava jokin järjestelmä, joka muodostaa datahubin tukeman SOAP-viestin. Viestin luonnin aikana tarkistetaan viestin oikeellisuus mallina toimivasta skeemasta. Jos viesti sisältää SOAP XML-viestistä eroavaa sisältöä tai datahubiin kelpaamatonta sisältöä, osapuolen järjestelmä lopettaa viestin muodostamisen.

2. Jos viestin luonti onnistuu, se allekirjoitetaan digitaalisesti, jotta varmistutaan viestin sisällön muuttumattomuudesta välityksen aikana.

3. Tietosisällön allekirjoituksen jälkeen osapuolella on oltava järjestelmä joka suorittaa viestin välityksen datahubiin. Tämä alkaa salatun Hypertext Transfer Protocol Secure (HTTPS) / TCP -yhteyden muodostamisella datahubin SOAP-rajapintaan.

4. Yhteyden salauksen varmistamiseksi suoritetaan Transport Layer Security (TLS)-kättely, jossa osapuolen järjestelmä toimittaa sille myönnetyn sertifikaatin.

5. Datahub tarkistaa osapuolen Secure Socket Layer (SSL) -sertifikaatin. Sertifikaatilla datahub tunnistaa osapuolen olevan rekisteröity ja luvallinen yhteydenmuodostaja. Jos sertifikaatti puuttuu tai se on viallinen, yhteydenmuodostus estetään.

6. Sertifikaatin onnistuneessa tunnistamisessa TLS-kättely etenee hyväksyttyyn tilaan, ja ilmoittaa tästä osapuolen järjestelmälle.

7. Osapuolen järjestelmä tunnistaa hyväksytyn TLS-kättelyn, ja lähettää viestinsä.

8. Osapuolen viesti välitetään datahubin SOAP-rajapintaan HTTPS/TCP-yhteyden yli.

9. Datahubin SOAP-rajapinta vastaanottaa viestin, ja itse viestisisällön tarkistuksen vaiheet alkavat.

10. Ensiksi SOAP-viestin allekirjoitus tarkistetaan. Datahubin havaitessa virheellisen allekirjoituksen suoritusketju katkeaa, ja datahub ilmoittaa tästä takaisin osapuolen järjestelmälle.

11. Jos allekirjoitus hyväksytään, viesti etenee datahubin sisäisten järjestelmien käsittelyyn.

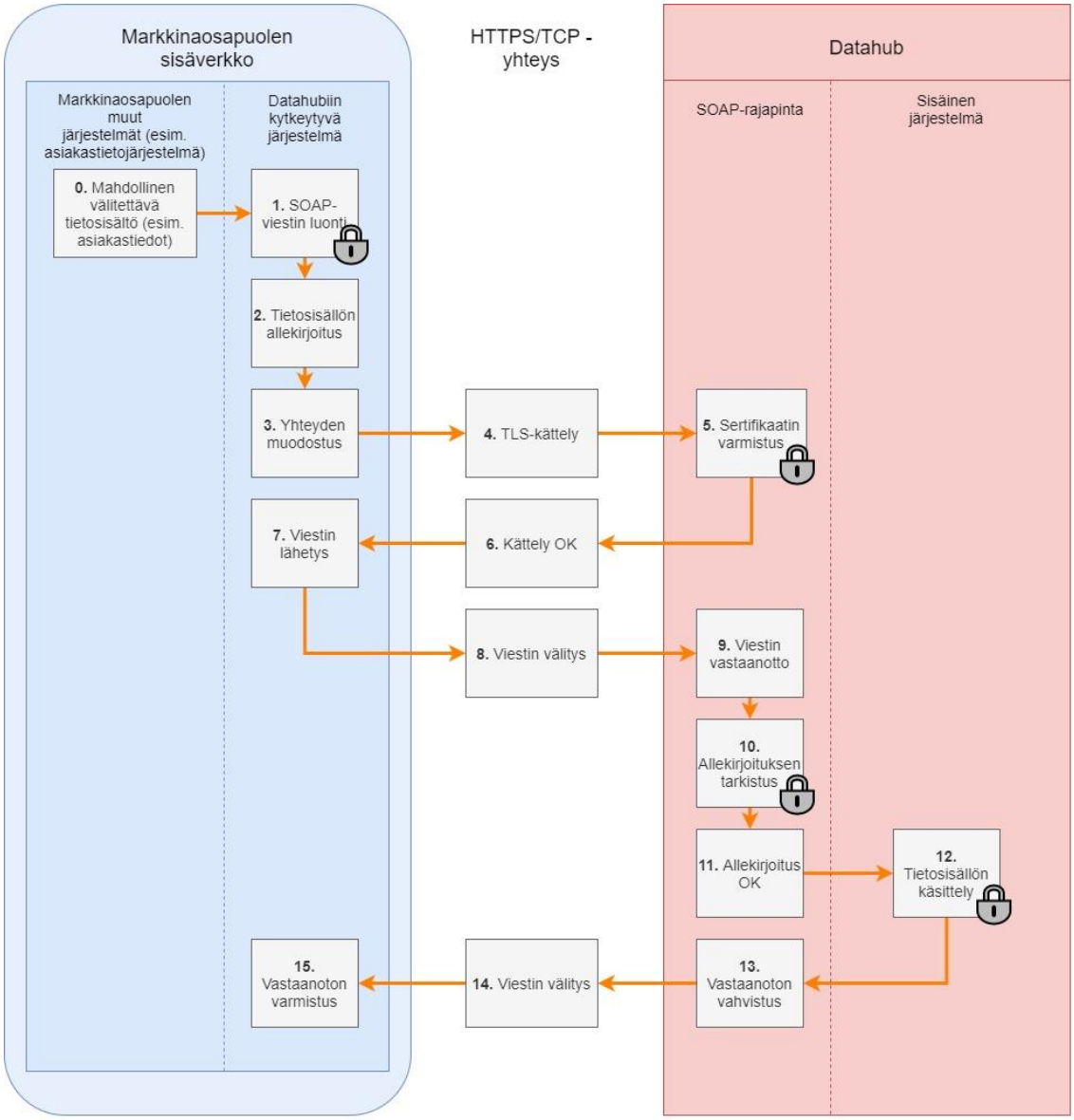
12. Datahub aloittaa viestin käsittelyn. Jos osapuoli yrittää suorittaa kielletyn toiminnon (esimerkiksi jos jakeluverkkoyhtiöksi tunnistettu osapuoli yrittäisi luoda myyntisopimuksen) datahub lähettää osapuolen järjestelmälle viestin suorituksen epäonnistumisesta asianmukaisen virhekoodin kera.

13. Jos tietosisältö on sallittu osapuolelle, datahub jatkaa sen käsittelyä lähettäen osapuolelle vahvistuksen operaation onnistumisesta.

14. Vahvistus kulkee saman HTTPS/TCP-yhteyden yli osapuolen järjestelmään

15. Osapuolen järjestelmä vahvistaa datahubin vahvistuksen siitä, onko operaatio onnistunut vai ei.

Yllä kuvattu prosessi on esitetty Kuvassa 1. Kaikki lukko-symbolilla merkityt kohdat kuvassa, kuten kohta 1, ovat tarkistuksia, jotka epäonnistuessaan palauttavat virheviestin osapuolen järjestelmälle. Asynkronisissa prosesseissa kohta 12 eli tietosisällön käsittely tapahtuisi samanaikaisesti kohdan 13 eli vastaanoton vahvistuksen kanssa. On myös huomioitavaa, että kuvattu prosessi olettaa markkinaosapuolen datahubiin kytkeytyvän järjestelmän sijaitsevan osapuolen sisäverkossa. Joissakin tapauksissa markkinaosapuoli saattaa käyttää järjestelmiensä suojaukseen muuta menetelmää kuin sisäverkkoa.



Kuva 1. Datahubin B2B-rajapinnan kautta suoritettavien markkinaprosessien toimintaperiaate. Hahmotelmassa on oletettu synkroninen markkinaprosessi, jonka sanomaan käytetään osapuolen muista järjestelmistä kerättyä tietoa osapuolen sisäverkon sisällä [38].

4 Tietoturvauhat

Lähestyttäessä kysymystä siitä, miten osapuolet saattavat lopulta aiheuttaa datahubin toiminnalle tietoturvauhkia, on tärkeää tutustua teollisuutta kohtaavaan tietoturvauhkien kenttään. Tässä luvussa tarkastellaan tarkemmin niitä toimijoita ja mekanismeja, jotka asettavat tarpeen tietoturvan toteuttamiselle. Ensimmäiseksi avataan hieman tietoturvasanastoa, jota käytetään kuvatessa eri tietoturvauhkien osa-alueita. Seuraavaksi luodaan yleinen kuva tietoturvauhkia aiheuttavista toimijoista sekä näiden motiiveista. Samalla nostetaan esiin se, miksi edellä mainittujen tarkempi kategorisointi on hyvin haasteellista. Kolmantena käsitellään joitakin yleisiä hyökkäysmenetelmiä tietojärjestelmiä kohtaan. Samalla argumentoidaan, että hyökkääjällä on lähtökohtaisesti aina etulyöntiasema suhteessa puolustajaan, joka perustuu suuresti arvaamattomuuteen.

4.1 Olennainen tietoturvasanasto

Valtionhallinnon tietoturvasanasto määrittelee sanan "uhka" seuraavasti: "Haitallinen tapahtuma, joka voi mahdollisesti toteutua, tai useampi mahdollinen häiriö, joka tapahtuessaan voi aiheuttaa sen, että tiedoille, muulle omaisuudelle tai toiminnalle tapahtuu eitoivottua" [43, s. 122]. "Riski" taas määritellään joko uhan toteutumisen todennäköisyytenä tai vaihtoehtoisesti sen vahingon odotusarvona (uhan tapahtumisen todennäköisyys kerrottuna vahingon rahallisella arvolla). Tässä työssä riski hahmotetaan jälkimmäisen määrittelyn mukaisesti, jotta keskustelu edes uhkien arvioiduista vakavuuksista olisi mahdollista. Näiden määritelmien perusteella voimme todeta, että toimialan ymmärtäessä hyvin siihen kohdistuvat uhat myös riskien tarkempi määrittely on mahdollista.

Tietojärjestelmiin kohdistuvat uhat voidaan jakaa "ihmislähtöisiin" ja "ihmisistä riippumattomiin uhkiin". Tässä työssä ihmislähtöisillä uhilla tarkoitetaan niitä uhkia, jotka aiheutuvat ihmisen joko tahallisesta tai tahattomasta toiminnasta tai toimimatta jättämisestä. Ihmisistä riippumattomiin uhkiin luetaan sellaiset uhat, joiden toteutumisen ennakointiin ei voida vaikuttaa arvioimalla ihmisen toimintaa. Esimerkiksi myrskyjen aiheuttamia vaurioita datakeskuksiin, joissa yrityksen palvelimia sijaitsee, ei lasketa ihmislähtöisiksi uhiksi. Tällaisten tapausten huomiointi jätetään tässä työssä vähemmälle. Sen sijaan ihmislähtöisiä uhkia ovat esimerkiksi sellaiset suunnitteluviat järjestelmissä, jotka paljastavat arkaluontoista tietoa muuten normaaleissa toimintaolosuhteissa. Ne johtuvat ihmissuunnittelijasta ja/tai toteuttajasta. Tällaisia uhkia tullaan käsittelemään työssä tarpeen vaatiessa.

Ihmislähtöisistä uhista keskusteltaessa keskeisimpiä toimijoita ovat "hyökkääjät". Valtionhallinnon tietoturvasanaston mukaan hyökkääjä on "taho, jonka katsotaan aiheuttavan tai aiheuttaneen uhan tai hyökkäyksen" [43, s. 38]. "Hyökkäyksellä" viitataan yritykseen "vahingoittaa tai rajoittaa tietojärjestelmän tai tietoverkon toimintaa, esimerkiksi tunkeutumalla suojattuun tietojärjestelmään" [43, s. 12]. Tässä työssä hyökkäyksen määritelmää laajennetaan tarkoittamaan myös muuta tahallista rikollista toimintaa tietojärjestelmää kohtaan, esimerkiksi henkilötietojen varastamista. Hyökkääjä-termiä käytetään lähinnä kontekstissa, jossa toiminta on ollut tahallista. Muissa tapauksissa käytetään yleisluontoisempaa termiä "tietoturvaloukkaus", jonka valtiohallinnon tietoturvasanasto määrittelee seuraavasti: "Tahallinen tai vahingossa tapahtunut tietoturvallisuuden tai viestintäsalaisuuden rikkoutuminen" [43, s. 109].

4.2 Uhkia aiheuttavat toimijat ja näiden motiivit

Kirjallisuudessa tunnistetaan useita eri motiiveilla ja tavoilla toimivia ihmisyksilöitä ja ryhmiä, jotka saattavat olla uhaksi yritysten tietoturvalle ja liiketoiminnalle. Joidenkin

hyökkääjien luokittelu ja näiden motiivit hyökkäyksille toistuvat lähes samanlaisina useissa lähteissä [15][18][19][44]. Samalla kirjallisuus välittää kuitenkin myös toisenlaisen viestin. Yhteiskuntien digitalisoituessa yhä enemmän myös yhteiskuntien tietoturvaan kuuluvien haavoittuvuuksien määrä lisääntyy. Mahdollisuuksien kasvaessa myös motiivit muuttuvat, ja esimerkiksi erilaisilla kostoiskuilla saattaa olla odottamattomia seurauksia [45][46]. Tässä alaluvussa kuvataan aluksi yksi tapa luokitella hyökkääjiä ja näiden motiiveja. Tämän jälkeen esitetään perusteluja sille, miksi erilaisiin luokittelutapoihin liittyy myös epävarmuutta.

4.2.1 Toimijoiden ja näiden motiivien yleinen luokittelu

Urquhart ja McAuley ovat vuoden 2018 älykkäiden energiajärjestelmien tietoturvauhkia koskevassa työssään lajitelleet erilaisia teollisuuden tietojärjestelmiä uhkaavia ihmistoimijoiden ryhmiä neljään eri luokkaan [15]. Alempana on tästä sovellettu versio, jossa Ulquhart ja McAuleyn neljäs yksilöitä koskeva luokka on jaettu kahteen osaan: Yksin toimiviin hakkereihin ja sisäpiiriuhkiin. Lisäksi alla olevassa luokittelussa on hyödynnetty maailmanlaajuisesti toimivan tietoturvayhtiö Symantecin vuoden 2016 ja 2019 tietoturvaraportteja sekä professori Jarno Limnéllin 12. marraskuuta 2019 pitämän seminaarin aineistoa [18][19][44].

- **Valtion rahoittamat hakkerit**. Toteuttavat iskuja esimerkiksi vierasmaalaisten infrastruktuurien tietojärjestelmiin kohdennetuilla ja järjestelmällisillä hyökkäyskampanjoilla varastaakseen sotilassalaisuuksia, levittääkseen propagandaa sekä harjoittaakseen sabotaasia tai teollisuusvakoilua [15]. Teollisuusvakoilu voi liittyä esimerkiksi edun saamiseen kaupankäynnissä käyttäen hyväksi varastettua sisäpiiritietoa tai aiheuttamalla häiriöitä markkinatoiminnoissa. Tällaisten toimijoiden käyttämisessä valtioiden vihamielisissä operaatioissa on etuna se, että tekijöiden ja sponsorin välistä yhteyttä on vaikea osoittaa [44]. Vieraat vallat saattavat palkata hyökkääjiä operaatioihinsa esimerkiksi toiselta puolelta maapalloa. Vielä todistusaineiston kerääntyessäkin hyökkäyksen rahoittanutta vierasta valtiota voi olla lähes mahdotonta saada vastuuseen kansainvälisen lain ollessa jäljessä tämän tapaisten iskujen tuomitsemisessa.

- **Organisoidut rikollisryhmät**. Hyökkäävät organisaatioihin teollisuusvakoilun nimissä, esimerkiksi varastaakseen kauppasalaisuuksia, julkaisemattomia immateriaalioikeuksia tai todisteita epäeettisestä toiminnasta [15]. Kuten valtion rahoittamat hakkerit nämä toimijat saattavat käyttää varastettua informaatiota tarjotakseen kilpailuedun esimerkiksi eniten maksavalle markkinatoimijalle. Esimerkkinä on Symantecin vuoden 2016 raportista "Butterfly"-nimellä tunnettu rikollisryhmä [18]. Ryhmän tiedetään vakoilleen suuria yrityksiä kuten Facebookia ja Applea, sekä myyneen yritysten luottamuksellisia tietoja ostajille, jotka tavoittelivat hyötyä pörssikaupassa. Symantecin vuoden 2019 raportti antaa taas esimerkin "Dragonflyna" tunnetusta ryhmästä [19]. Dragonflyn tiedetään vakoilleen erityisesti energia-alan yhtiöitä ja pyrkineen saamaan häirintään mahdollistavan jalansijan näiden järjestelmissä. Eri rikollisryhmät saattavat myös kiristää yrityksiä varastamallaan informaatiolla tai ottamalla järjestelmiä panttivangiksi [18][19]. Niin kutsutussa Ransomware hyökkäyksessä hyökkääjä lukitsee tai kaappaa yrityksen toiminnot vaatien rahaa niiden vapautusta vastaan [43]. Kuuluisa esimerkki voidaan löytää norjalaisen alumiinivalmistaja Norsk Hydron tapauksesta vuoden 2019 maaliskuulta, jossa yhtiön kieltäydyttyä lunnasvaatimuksista vahinkojen arvioidaan nousevan 75 miljoonaan dollariin [47].

- **Kollektiiviset, puoli-itsenäisesti toimivista jäsenistä koostuvat hakkeriryhmät**. Esimerkkeinä Lulzsec tai Anonymous, jotka saattavat hyökätä yritysten kimppuun esimerkiksi kostoina epäeettisenä nähdystä liiketoiminnasta [15]. Erona edellisiin toimijoihin voidaan nähdä se, että hyökkäyksellä ei välttämättä haluta tavoitella mitään omaa hyötyä vaan ainoastaan vahingoittaa kohdetta. Näin ollen hyökkäyksellä saavutettu vaikutus voi olla paljon sattumanvaraisempi. Toimijat saattavat esimerkiksi kaataa yritysten verkkosivuja, toteuttaa palvelunestohyökkäyksiä tai aiheuttaa muuta häirintää tavoitteenaan kiusanteko, kohteen maineen vahingoittaminen tai rahallinen tappio. Taitavammat ryhmät saattavat kyetä myös yllä kuvaillun kaltaisiin hyökkäyksiin ja täten aiheuttaa vakavaakin vahinkoa, esimerkiksi julkaista yritykseltä varastettua salaista tietoa vain vahingoittaakseen kohdettaan.

- **Yksin toimivat hakkerit**. Taitava yksilö saattaa kyetä toteuttamaan joitakin yllämainituista rikoksista myös ilman ryhmiä ainakin jossain määrin, riippuen kohteen suojauksista [15]. On huomionarvoista, että tällaisten henkilöiden motiivit saattavat olla vielä arvaamattomampia. Jotkin hyökkääjistä saattavat harjoittaa hakkerointia rahan vuoksi, taitojensa kehittämiseksi, harrastukseksi tai paljastaakseen kuvittelemiaan salaliittoteorioita. Urquhart ja McAuley nostavat esille muun muassa sotilaallisiin infrastruktuureihin murtautuvat hakkerit, jotka etsivät todisteita avaruusolentojen olemassaolosta, ja saattavat taistella kiinniottoa vastaan vuosia.

- **Sisäpiiriuhat**. Tämä ryhmä koostuu niin sellaisista työntekijöistä, jotka haluavat aiheuttaa vahinkoa entiselle tai nykyiselleen työnantajalleen, kuin niistä, jotka tietämättään aiheuttavat uhkia [15]. Tietoisesti toimivat nykyiset tai aiemmat työntekijät ovat erityisen vaarallisia, jos yrityksessä ei noudateta tarpeeksi hyvin suunniteltua käyttäjäoikeuksien hallintaa. Yksi tällaisen henkilön helposti aiheuttama uhka on luottamuksellisen tiedon vuotaminen vääriin käsiin. Symantecin vuoden 2016 raportissa vuonna 2015 noin 10 % kaikista tietovuodoista tapahtui yritysten omien työntekijöiden tahallisista toimista [18]. Tietämättään uhkia aiheuttavat työntekijät saattavat aiheuttaa tietoturvaloukkauksen puutteellisen tietoturvakoulutuksen tai pelkän inhimillisen virheen kautta. Työntekijä saattaa esimerkiksi avata hyökkääjien haittaohjelmilla aseistamia sähköposteja tai vuotaa luottamuksellista tietoa julkisuuteen ottamansa valokuvan välityksellä.

Datahubin riskienhallinnassa vieraiden valtioiden nimiin toimivien hyökkääjien hyökkäyskyvyt, -motivaatio ja hyökkäykselle omistautuminen on luokiteltu korkeimpien joukkoon arvioiduista mahdollisista hyökkääjäluokista [25]. Erilaisten hakkeriryhmien kyvyt ja omistautuminen on myös arvioitu korkeimpien kategorioiden joukkoon, tosin niiden motivaatio on arvioitu hieman vieraiden valtioiden hyökkääjiä matalammaksi. On kuitenkin huomionarvoista, että kummallakin hyökkääjäluokalla on historiaa useista ja jatkuvista hyökkäyksistä kriittisiä infrastruktuureita kohtaan.

4.2.2 Toimijoiden ja näiden motiivien arvaamattomuus

Kuten luvun alussa mainittiin, yllä kuvattu toimijoiden luokittelu on tapa nostaa esille eri hyökkääjien motivaatioita ja aikeita. On kuitenkin selvää, että monet kuvailluista ryhmistä ja yksilöistä saattavat etenkin ajan kuluessa sulautua tai toimia sekoituksina toisistaan. Yksi esimerkki tästä ovat vieraiden valtioiden palkkaamat rikollisorganisaatiot tai itsenäiset hakkerit [44]. Vieraille valtioille tällainen menettelytapa on tehokas taktiikka

esimerkiksi siinä mielessä, että niiden osallisuutta hyökkäykseen voi jälkiselvityksissä olla lähes mahdotonta todistaa. Toisaalta yksinäisistä hakkereista saattaa rakentua ryhmittymä, joka myöhemmin järjestäytyy ammattimaiseksi rikollisorganisaatioksi. Tärkeintä hahmottaessa eri hyökkääjien kategorioita ja näiden motiiveja onkin ymmärtää, että hyökkääjä saattaa olla motivaatioiltaan täysin arvaamaton eikä sen resursseja tai kykyjä kannata aliarvioida perustuen jäykkään kategorisointiin.

Toimijoiden luokittelun lisäksi myös hyökkäysten kohdistaminen ja niillä haettu vaikutus voi olla hankalaa analysoida. Yhtenä esimerkkinä tästä voidaan nähdä Viroa kohdannut laajamittaisten tietoturvahyökkäysten sarja, joka tapahtui noin kolmen viikon aikana vuonna 2007 [45][48]. Useisiin virolaisiin yrityksiin, kuten pankkeihin, uutistoimistoihin sekä Viron valtion verkkosivuihin kohdistettiin sarja tietoturvahyökkäyksiä. Suuri osa hyökkäyksistä oli palvelunestohyökkäyksiä, jotka muuttuivat ilmiön loppupuolella hajautetuiksi toimijoiden hyökätessä arviolta 85000 kaapatulta tietokoneelta kohteisiinsa. Palvelunestohyökkäyksellä tarkoitetaan järjestelmien toiminnan häirintää tai lamauttamista syöttämällä niille enemmän viestejä kuin ne kykenevät käsittelemään [43]. Hajautettu palvelunestohyökkäys on laajamittaisempi variaatio edellä mainitusta, jossa hyökkäys suoritetaan usealta eri verkkoasemalta.

Tietoturvahyökkäykset tapahtuivat päällekkäin Tallinnassa sijaitsevan venäläisen Pronssisoturi-patsaan siirtämisestä aiheutuneiden mellakoiden aikana [48]. Ilmoitetut aikeet Pronssisoturin siirtämisestä aiheuttivat pahennusta osassa Viron venäläisväestöä, joka piti patsasta kunnianosoituksena Toisessa maailmansodassa kuolleille venäläissotilaille [45]. Joidenkin raporttien mukaan tilanteen aikana tietyillä venäjänkielisillä keskustelupalstoilla jaettiin ohjeita, kuinka suorittaa tietoturvahyökkäyksiä virolaisiin järjestelmiin. Viro väitti tietoturvahyökkäysten tapahtuneen Venäjän hallituksen toimesta, mutta tätä ei ole pystytty todistamaan. Hyökkäyksien hienostuneisuus on raportoitu varsin alhaiseksi, mutta ne aiheuttivat haittaa useiden erilaisten palvelujen käytössä ja saivat aikaan yhteiskunnallista kaaosta [45][46]. Tapaus osoittaa, että esimerkiksi sisäpoliittisissa kiistoissa siviilit saattavat pyrkiä aiheuttamaan haittaa yksinkertaisesti kostoksi. Tällaisissa tilanteissa vähemmänkin kriittiset palvelut saattavat joutua kohteiksi, jos niiden tietoturva on huono. Ei ole mahdotonta kuvitella, että suomalaista teollisuutta vastaan saatettaisiin kohdistaa pienempiä kostoiskuja. Tällaisissa tilanteissa markkinaosapuolten on ymmärrettävä, että ne saattavat muuttua houkuttelevaksi kohteeksi jos niillä on huono tietoturva riippumatta niiden roolin kriittisyydestä.

4.3 Erilaiset hyökkäystavat

Hyökkääjien käyttämiä tapoja murtautua kohteensa järjestelmiin on mahdotonta ennustaa kaikilta osin. On virhe olettaa, että tietoturva on mahdollista järjestää löytämällä tietyt suojautumiskeinot, jotka passiivisesti tulevat torjumaan kaikki tulevaisuuden hyökkäysyritykset [49]. Tietotekniikan jatkuva kehittyminen ja uusien teknologioiden nopea leviäminen tuovat mukanaan uusia haasteita muun muassa verkkoyhteyden muodostavien laitteiden lisääntyessä [16][50][51]. Joidenkin yleisten hyökkäystapojen tunteminen on silti hyödyllistä, koska monien hyökkäyksien voidaan nähdä noudattavan joitakin ennalta määrättyjä kaavoja. Alla keskitytään kuvaamaan, miten järjestelmiin tunkeutuminen haittaohjelmien välityksellä toimii. Samalla esitetään, kuinka abstrakti tunkeutumisprosessi voi käytännössä toteutua monilla eri tavoin, sekä annetaan joitakin historiallisia esimerkkejä.

Hutchins et al. kuvaavat artikkelissaan "Intrusion Kill Chain" -mallin, jonka asevalmistaja Lockheed Martin on luonut jäljitellen Yhdysvaltojen armeijan kuvaamaa systemaattista

hyökkäysprosessia [49]. Työryhmä esittää, että kuten armeijan hyökkäys, kyberhyökkääjän tunkeutumismenettely voidaan nähdä toisiaan seuraavien vaiheiden ketjuna. Ketjussa hyökkääjän on suoritettava jokainen vaihe onnistuneesti kaapatakseen kohteensa järjestelmän perusteellisesti. Vastaavasti yhden vaiheen estyessä ketju katkeaa estäen pääsyn viimeisimpiin menettelyvaiheisiin. Alla kuvataan Hutchinsin tutkimusryhmän määrittelemän tunkeutumismenettelyn mallin vaiheet muutamin lisätiedoin Symantecin vuoden 2019 raportista [19][49]:

1. **Tiedustelu**. Kohteen tai kohteiden valinta sekä näiden tutkiminen. Tapahtuu esimerkiksi läpikäymällä automaattisilla ohjelmilla sähköpostilistoja ja verkosta löytyviä konferenssitiedotteita, sosiaalisten suhteiden tutkimisella tai tiettyjen teknologioiden täsmällisellä tutkimisella.

2. **Aseistaminen**. Etäyhteyteen kykenevän troijalaisen yhdistäminen lähetettävään tietosisältöön. Tähän käytetään yleensä automatisoitua aseistamistyökalua. Eri ohjelmistojen käyttämät tiedostoformaatit, kuten Adobe Portable Document Format (PDF) sekä Micosoft Office -dokumentit toimivat kasvavassa määrin aseistettuina tietosisältöinä. Vuonna 2018 Office-dokumentteja käytettiin 48%:ssa tällaisia tapauksia.

3. **Toimitus**. Aseistetun tietosisällön toimittaminen kohdeympäristöön. Lockheed Martinin mukaan vuosina 2004 - 2010 yleisimmät aseistetun tietosisällön toimitustavat ovat olleet sähköpostien liitetiedostot, verkkosivut ja Universal Serial Bus (USB) -tallennuslaitteet.

4. **Hyväksikäyttö**. Toimituksen onnistuttua hyväksikäytettävä toiminto (esimerkiksi kohdejärjestelmän käyttäjän tekemä toimenpide tai toimitetun haittaohjelman automaattinen toiminnallisuus) käynnistää aseistetun tietosisällön sisältämän koodin kohteen ympäristön sisällä. Hyväksikäytön onnistuminen perustuu yleisesti haavoittuvuuteen ohjelmistossa tai käyttöliittymässä, mutta se saattaa ilmetä myös niin, että käyttäjiä huijataan tekemään tiettyjä toimintoja.

5. **Asennus**. Etäyhteyteen kykenevän troijalaisen tai takaoven asentaminen kohteen järjestelmiin, jotta ympäristöön kyetään tunkeutumaan.

6. **Komento ja kontrolli** (C2, englannin sanoista Command and Control). Yleisesti saastutettu järjestelmä on saatava luomaan yhteys ulospäin toiselle palvelimelle, jotta C2-kanava saadaan muodostetuksi. Kanavan muodostuttua hyökkääjällä on kuitenkin saman tasoinen kontrolli ympäristöstä kuin sisään kirjautuneella käyttäjällä.

7. **Toiminnot päämäärien saavuttamiseksi**. Hyökkääjä aloittaa toimintansa varsinaisen päämääränsä saavuttamiseksi. Tähän voi kuulua esimerkiksi tiedon varastaminen, sabotointi tai toimintojen estäminen. Vaihtoehtoisesti hyökkääjä saattaa käyttää kohdeympäristöä vain jalansijana siirtyäkseen muihin järjestelmiin tavoitetussa sisäverkossa.

On huomioitavaa, että tämä malli kuvaa hyvin perusteellista hyökkäysprosessia, jossa saavutettava päämäärä on manuaalinen kontrolli kohdejärjestelmästä. Monet vakavistakin hyökkäyksistä saattavat vahinkoa aiheuttaakseen tarvita esimerkiksi vain ketjun alku-

vaiheiden saavuttamisen. Malli tarjoaa kuitenkin hyvän viitekehyksen lähestyä niin lievempiä haittaohjelmien levitystä tai kalastelua, kuin vakavia tunkeutumishyökkäyksiäkin. Vaiheista tiedustelu ja aseistaminen voivat olla täysin yrityksen tietoturvan estämättömissä. Sen sijaan tämän jälkeiset vaiheet ovat tietoturvan torjuttavissa, jos vastuussa oleva henkilöstö omaa tarpeellisen ymmärryksen aiheesta ja hyökkäyksen etenemisen tekniikoista.

4.3.1 Hyökkäyksessä käytettävien työkalujen toimitus

Erilaiset sosiaaliseen manipulointiin perustuvat keinot kuten niin sanotut phishing- ja spear phishing -sähköpostit ovat yksi tunnettu tapa toimittaa aseistettu tietosisältö [18][19][49]. Keinoja käytetään yleisesti myös pienempiin hyökkäyksiin, kuten luottamuksellisen tiedon kalasteluun. Ero termien välillä määritellään siten, että spear phishing -hyökkäykset ovat kohdistettuja usein tiettyihin yksilöihin laajemman yleisön sijaan, toisin kuin phishing-hyökkäykset [52]. Kummassakin hyökkäyksessä pyritään lähestymään yleensä kohdeyrityksen työntekijöitä sähköposteilla, jotka on puettu mahdollisimman autenttisen näköisiksi. Ne saattavat vedota kohteen tunteisiin tai muuten saada kohteen avaamaan sähköpostin sisällön, vastaamaan luovuttaen luottamuksellista tietoa tai jopa siirtämään rahaa hyökkääjälle.

Sosiaalinen manipulointi tällaisten hyökkäysten takana voi olla hyvinkin järjestäytynyttä ja pitkälle vietyä, varsinkin niin kutsutuissa Advanced Persistent Threat (APT) -hyökkäyksissä [18][49]. APT-hyökkäyksellä tarkoitetaan kohdennettua, suunnitelmallista ja usein pitkäaikaista hyökkäyskampanjaa. Niihin kuuluu usein myös pitkäaikainen tiedusteluvaihe, joissa selvitetään muun muassa kohteen henkilökunnan ammatteihin liittyvää käyttäytymistä. Hyökkäyksissä saatetaan käydä läpi jopa kohteiden henkilökohtaista internetkäyttäytymistä sekä profiileja sosiaalisessa mediassa [18][52].

Hutchins et al. kuvaavat artikkelissaan tarkasti kolme APT-kampanjaan yhdistettyä tunkeutumisyritystä [49]. Näistä kahdessa ensimmäisessä hyökkääjät lähettivät kohdeyrityksen työntekijöille sähköpostia koskien todellista American Institute of Aeronautics and Astronomics (AIAA) -instituutin järjestämää konferenssia [49]. Kummatkin sähköpostit sisälsivät PDF-tiedoston, jotka olivat alkuperältään aitoa AIAA:n materiaalia. Tarkemmissa analyyseissa kuitenkin selvisi, että PDF-tiedostot oli aseistettu piilotetuilla skripteillä, jotka olisivat tiedostojen avaamisen yhteydessä asentaneet avaajan tietokoneelle piilotetun, ulkopuoliselle C2-palvelimelle dataa lähettävän takaovikomponentin. Hyökkääjät onnistuivat siis tunkeutumismenettelyn kolmessa ensimmäisessä vaiheessa, tiedustelussa, aseistamisessa ja kuljetuksessa. Valpas tietoturvavalvonta kuitenkin pysäytti tunkeutumisyrityksen kolmanteen vaiheeseen eli aseistetun tiedoston toimittamiseen kohdejärjestelmään.

Symantec analysoi vuoden 2019 raportissaan 65 %:n tunnetuista hyökkäysryhmistä käyttävän spear phishing -tekniikkaa pääasiallisena hyökkäystapanaan [19]. Vuoden 2016 raportissaan Symantec tunnisti myös hyökkäysten kohdistamisissa muutoksia [18]. Ensinnäkin vuosina 2011 - 2015 alle 250 henkilön yrityksiä kohtaan kohdistuvat spear phishing -hyökkäykset kasvoivat 18 prosentista 43 prosenttiin kaikista. Toiseksi, spear phishing -kampanjat yksittäisiä työntekijöitä kohtaan kasvoivat vuonna 2015 edellisvuoteen verrattuna 55 %. Tämä saattaa tarkoittaa sitä, että hyökkääjät ovat siirtyneet kohdentamaan enemmän pieniä, heikomman tietoturvan omaavia yrityksiä ja näiden osia saadakseen ensimmäisen jalansijan lopullisen kohdetoimialan sisällä. Tähän viittaa myös se, että spear phishing -hyökkäykset kohdennettiin vuonna 2015 pienempään määrään kohteita. Hyökkäyskampanjoiden lukumäärät kasvoivat samalla kun niiden kohdekenttä tarkentui. Tämä

mahdollisti myös sen, että hyökkääjien oli helpompi piilottaa jälkensä. Hyökkääjien havaittiin myös vaihtavan nopeammin epäonnistuneita taktiikoitaan.

USB-tallennuslaitteiden käyttö toimitusta varten vaatii fyysisen kontaktin laitteistoon, jolla on pääsy kohdejärjestelmään. Näin ollen voidaan ajatella, että kriittisten fyysisten laitteiden perusteellinen vartiointi on riittävä toimenpide tällaisen toimituksen estämiseksi. Asia ei välttämättä ole kuitenkaan näin yksinkertainen. Työntekijät saattavat epähuomiossa kytkeä järjestelmiin tallennuslaitteita, joiden saastumisesta heillä ei ole tietoa. Näin tapahtui muun muassa vuonna 2010 Iranissa, kun Stuxnet-haittaohjelmisto tuhosi arviolta tuhat uraanin rikastamiseen tarkoitettua sentrifugia valtion Natanzin rikastamislaitoksella [53]. Stuxnet on tiettyä Siemensin Supervisory Control and Data Acquisition (SCADA) -ohjelmistoa vastaan suunniteltu haittaohjelma, joka kommunikoi levittäjänsä kanssa C2-kanavan kautta ja kykenee moniin edistyneisiin toimenpiteisiin kohdejärjestelmässä. Tarkkaa tietoa sen leviämisestä Natanzin sentrifugien ohjaussysteemeihin ei ole, mutta sen epäillään levinneen alihankkijan asettaman USB-laitteen kautta koska se on ainoita tapoja joilla Stuxnet voi saavuttaa päämääränsä. Tämä saastuttaminen on voinut tapahtua työntekijän tietämättä, sillä haittaohjelman oli havaittu levittäytyneen tietojärjestelmiin maailmanlaajuisesti levittäjien odottaessa sen saavuttavan nimenomaisesti Natanzin rikastamon.

4.3.2 Toimituksen onnistumisen jälkeiset vaiheet

Stuxnet aseistettuna tietosisältönä on esimerkki haittaohjelmasta, joka käyttää hyväkseen niin kutsuttuja zero-day haavoittuvuuksia [53]. Näillä tarkoitetaan haavoittuvuuksia ohjelmistoissa, joita niiden kehittäjä ei ole ehtinyt ymmärtää ja korjata [15]. Myös Hutchins et al. kuvaamat hyökkäysyritykset pyrkivät hyväksikäyttämään PDF-tiedostoissa havaittua haavoittuvuutta, jota ei oltu ehditty korjata [49]. Symantec raportoi vuonna 2015 löydettyjen zero-day haavoittuvuuksien kasvaneen 125 % vuoteen 2014, joka oli suurin kasvu tutkittujen 10 vuoden ajalta [18]. Neljä viidestä haavoittuvuudesta löydettiin Adobe Flash ohjelmistosta, jolla oli jo ollut kyseisenä vuonna vuosien historia lukuisten zero-day haavoittuvuuksien kanssa. Vuonna 2018 Symantecin mukaan zero-day haavoittuvuuksia hyödynsivät 23 % tunnetuista hyökkäysryhmistä [19].

Suurin vaara zero-day haavoittuvuuksissa on se, että niitä todennäköisesti on olemassa puolustajan osaamatta odottaa niitä. Ne kuvaavat hyvin tietoturvaan suhtautumisen luonnetta: Vaikka puolustautuja ottaisi huomioon kaiken toimintaympäristöstä tietämänsä strategiset ja taktiset yksityiskohdat, toimintaympäristö on niin monimutkainen ja muuttuva, että hyökkääjät löytävät aina uusia haavoittuvuuksia ennen puolustajaa. Tämä epäsymmetria hyökkääjän ja puolustajan voimatasapainossa tarkoittaa sitä, että vaikka tunnetut haavoittuvuudet on syytä korjata, uusien haavoittuvuuksien spekulointi ei ole riittävä valmistautumistoimenpide. Tietoturvan on lähdettävä liikkeelle siitä, että hyökkääjä kykenee läpäisemään ainakin osan järjestelmien puolustuksesta ennemmin tai myöhemmin.

On huomionarvoista, että tietomurron tapahduttuakin ei ole itsestään selvää, että puolustaja ymmärtää reagoida tähän. IBM Securityn arvion mukaan pohjoismaissa yrityksellä kestää keskimäärin 225 päivää havaita tietomurto ja 74 päivää eristää tämän leviäminen [44]. Jos vihamielinen toimija pyrkii aiheuttamaan vakavan hyökkäyksen ja on saanut paljon aikaa selvittääkseen kohteensa heikkoudet, itse hyökkäystilanne taas voi kestää muutaman sekunnin. Näin ollen ilman kunnollista valvontaa hyökkääjät kykenevät kokoamaan operaatiolleen tärkeät resurssit ja suorittamaan sen valmistelut perusteellisesti niin, että kun kohde havaitsee tietomurron, vahinkoa ei enää kyetä estämään.

Yhteenvetona esitetään, että toimialan on tärkeää hahmottaa tietoturva yhdistelmänä yleisesti hyväksi todettuja peruskäytäntöjä ja -toimintatapoja sekä varautumisena muuttuvaan uhkakenttään ja vastatoimenpiteisiin. Mitkään valmiiksi toteutetut tietoturvakäytännöt eivät riitä varmaksi suojaksi asialleen omistautuneita hyökkääjiä vastaan. Avainlähtökohtana on, että jotkut hyökkääjät pyrkivät aina löytämään haavoittuvuudet kohteidensa järjestelmässä, ja tämän tiedusteluprosessin havaitseminen saati siihen puuttuminen voi olla jopa mahdotonta.

5 Luotettavan tietoturvan määrittäminen

Tietoturvakirjallisuutta lukiessa voidaan tunnistaa toistuvia ja hyväksi koettuja tietoturvakäytäntöjä monista eri lähteistä [54][55][56][57]. Toisaalta kirjoituksissa, joissa ohjataan luotettavan tietoturvan määrittämiseen, nostetaan esille myös käyttötarkoituskohtaisen arvion olennainen rooli prosessissa [54][55]. Täten voidaan nähdä, että hyvä tietoturva koostuu kahdenlaisista käytännöistä: yleisesti hyväksi koetuista käytännöistä, sekä tapauskohtaisista erityisvaatimuksista. Tämän työn päätavoitteena on määrittää sellainen viitekehys, jolla datahub-järjestelmään liittymiseen vaadittava tietoturvaa kyettäisiin määrittelemään tarkemmin. Tämän vuoksi on järkevää tuntea edellä mainitut yleisesti hyvät käytännöt. Toisaalta datahub, kuten muutkin tietojärjestelmät, omaa tarkoitukseltaan ja toiminnaltaan lukuisia erityispiirteitä. Tämän vuoksi on siis syytä myös löytää lähestymistapa, jolla voitaisiin ottaa nämä erityispiirteet huomioon järjestelmään liittymiseen edellyttävissä tietoturvavaatimuksissa.

Tämän luku lähestyy edellä mainittua teemaa käymällä kolmenlaista lähdeaineistoa läpi. Ensiksi luodaan katsaus tietoturvan tämänhetkiseen akateemiseen kirjallisuuteen ja tutkimukseen. Seuraavaksi tarkastellaan konkreettisia esimerkkejä tietoturvavaatimuksista kolmen suomalaisen referenssijärjestelmän kautta. Referenssijärjestelmät on valittu siten, että kuten datahubilla, kaikilla niistä on tarve esittää vaatimuksia nimenomaan niihin liittyville tahoille. Viimeiseksi käsitellään kolmea eri asiantuntijaorganisaation kehittämää viitekehystä, joilla on meriittejä kansainvälisesti suositeltuina ja käytettyinä työkaluina.

5.1 Akateeminen tutkimus

Tietoturvaa voidaan pitää tieteenalana, jolla ei ole selkeää konsensusta siitä kuinka tarpeelliset järjestelmien suojaukset tulee eri tilanteissa suorittaa. Erilaisia malleja luotettavan tietoturvan määrittämiseksi on esitetty eri tutkimuksissa ja kirjallisuuslähteissä [58][59][60]. Monet kirjallisuuslähteet esittävät myös huolensa tutkimuksen puutteista [58][59]. Tällaisia puutteita ovat muun muassa kehitettyjen mallien toimivuuteen liittyvän tiedon vähäisyys sekä suositusten ja tärkeäksi nähtyjen alueiden eroavaisuudet. Osa tutkimuksista esimerkiksi keskittyy määrittämään täysin organisaation työntekijöiden käyttäytymistä, kun taas osassa on rakennettu kriteeristöjä kokonaisten valtioiden tietoturvan tason määrittämiseksi [58][59][60]. Toisaalta myös samoista lähtöolettamuksista tehdyt tutkimukset saattavat erota tutkimustavoiltaan [58][60]. Tämä eroavaisuus sekä edellä mainittu tiedon puute lopputulosten pätevyydestä muodostavatkin suurimman ongelman arvioitaessa tutkimusten luotettavuutta. Alla tarkastellaan kolmea eri tutkimusta, joiden tavoitteena on ollut jonkin yleisen tietoturvan määrittämiseksi tarkoitetun teorian muodostaminen.

Vishwanathin tutkimusryhmä lähtee liikkeelle oletuksesta, jonka mukaan turvallinen tietoturva pohjautuu työntekijöiden ymmärrykseen mahdollisista riskeistä [59]. Oletuksen mukaan työntekijöitä valistamalla rationaaliset yksilöt koordinoivat toimintaansa yritykselle turvalliseen suuntaan. Tämän pohjalta tutkimusryhmä määrittelee "cyber hygiene" -käsitteen mallin, jonka tarkoitus on kuvata työntekijän tietoturvallisen toiminnan eri osa-alueet ja arvioida näiden toteutumista yksilötasolla. Tutkimusryhmä käyttää mallinsa muodostamiseen asiantuntija-arvioihin perustuvaa “Concept Mapping” -menetelmää. Concept Mapping -menetelmä on ryhmän mukaan useilla eri aloilla käytetty tilastollinen menetelmä, jonka tarkoituksena on “visualisoida erilaisten rakenteiden käsitteellisiä suhteita, empiirisesti kehittää niiden määrityksiä ja tutkia kompleksisia ilmiöitä” [59]. Tämän jälkeen tutkimusryhmä käyttää mallinsa validointiin 404:ltä tutkijoiden kyselyyn vastanneilta henkilöiltä kerättyä dataa, johon sovelletaan erilaisia tilastollisia menetelmiä.

Ryhmä väittää kehittämänsä menetelmän olevan tehokas työkalu arvioimaan organisaation tietoturvan tasoa, ja toteavat muun muassa kriteeristönsä ennustevaliditeetin eli kyvyn ennustaa odotettuja tuloksia tilastollisesti pätevästi suurimmalta osalta [61].

Trimin tutkimusryhmä soveltaa sosiaalipsykologian tutkimusta rakentaakseen yritysmarkkinoinnissa toimiville työntekijöille tarkoitetun tietoturvatietoisuuden kehityksen ohjelman [60]. Tutkimusryhmä rakentaa työnsä perustuen laajaan kirjoon kirjallisuuslähteitä, jotka käsittelevät muun muassa motivaatiota ja tiedon vaikutusta käyttäytymisen muuttumiseen. Pääasiallinen datan keruu toteutuu asiantuntijahaastatteluina, joiden kohteet on valittu tarkasti seuraten edellä mainitusta sosiaalipsykologian kirjallisuudesta sovellettua teoriaa. Tutkijat analysoivat käytyjä haastatteluja samanaikaisesti Grounded Theory -menetelmällä, jossa data pyritään kategorisoimaan ja jäsentelemään tutkimuksen aihetta lähestyväksi teoriaksi. Lopullisen teoriansa tietoturvatietoisuuden kehittämisen ohjelmasta tutkijaryhmä rakentaa niin sanotulla Grounded Theory -menetelmällä [62]. Grounded Theory -menetelmässä dataa kerätään ja analysoidaan samanaikaisesti pyrkien kategorisoimaan se ja tältä pohjalta luomaan yleispätevä teoria, jolla tutkimuksen aihetta voidaan lähestyä. Toisin kuin Vishwanathin tutkimusryhmä, Trimin tutkimusryhmä ei tee kvantitatiivisiin menetelmiin perustuvaa pitkää validointiprosessia [60]. Sen sijaan se tyytyy tarkastelemaan muun muassa haastateltavien kesken syntyneitä konsensuksia, haastateltavien suhteita toisiinsa sekä sitä, kuinka vapaa keskustelukulttuuri haastateltavien kesken vallitsi.

Karabacakin tutkimusryhmä tavoittelee tutkimuksessaan mallia, jolla kyettäisiin arvioimaan kansallisen kriittisen infrastruktuurin tietoturvan tasoa, tai kypsyyttä kuten ryhmä sitä kutsuu [58]. Työryhmä lähestyy tavoitettaan hyödyntäen ensiksi samaa Grounded Theory -menetelmää kuin Trimin tutkimusryhmä. Näin ryhmä pyrkii muodostamaan käsityksensä kriittisten infrastruktuurien tietoturvahaavoittuvuuksien perussyistä. Grounded Theory -menetelmän vaatiman datan analysointiin ryhmä käyttää Turkin kriittisen infrastruktuurin tietoturvaa koskevaa projektidataa. Määriteltyään perussyyt, tutkimusryhmä siirtyy käyttämään Delfoi-menetelmää muodostakseen kerätyn datan pohjalta tietoturvan kypsyyskriteeristön. Delfoi-menetelmällä tarkoitetaan valikoidulle asiantuntijaryhmälle esitettyä suunniteltujen kyselyjen sarjaa, jonka päämääränä on saada konsensus asiantuntijaryhmän näkemyksistä koskien tutkittavaa kohdetta [63]. Lopuksi ryhmä muodostaa tavoitteenaan olleen kypsyysmallinsa kehitetyn kypsyyskriteeristön pohjalta [58].

Yllämainittujen sosiaalipsykologian menetelmien soveltuvuus tietoturvan kehittämiseksi, tai sellaisten tilastollisten tunnuslukujen kuten ennustevaliditeetin oikeanlainen muodostaminen ovat tämän työn rajauksen ulkopuolella. Samalla on tarpeellista olla kriittinen tällaisten menetelmien esittämisestä pätevänä lähestymistapana kyseiseen aiheeseen. Ensinnäkin monien edellä mainituissa tutkimuksissa käytettyjen tilastotieteen tai psykologian menetelmien soveltuvuutta tietoturva-alalle ei voida todentaa. Ne on kerätty enemmän tai vähemmän muiden tieteenalojen menetelmistä, ja jokainen tutkimus korostaa pyrkivänsä tuottamaan uutta tietoa alalle [58][59][60]. Tämä viittaisi siihen, että ainakin osa käytetyistä menetelmistä on uusia lähestymistapoja. Menetelmät myös eroavat toisistaan osittain suuresti, josta voidaan päätellä, ettei käsitystä yleisesti hyvän tietoturvan määrittämisestä lähestytä yhteisesti hyväksi koetuilla tutkimusmenetelmillä.

Jokainen edellä mainittu tutkimusryhmä aloittaa teoriansa rakentamisen asiantuntijahaastatteluilla. Jos haastatellut asiantuntijat voidaan olettaa pitkään työssä toimineiksi henkilöiksi, voidaan myös olettaa, että heidän näkemyksensä kuvastavat vahvasti testattuja,

käytännössä todennettuja huomioita tietoturvasta. Mikään tutkimusryhmistä ei kuitenkaan tyydy asiantuntijoiden välillä vallitseviin konsensuksiin, vaan sen sijaan ne käyttävät edellä mainittuja eri aloilta poimittuja data-analytiikan tai psykologian menetelmiä jalostaakseen vastauksia. Jos jälkeenpäin käytettyjen menetelmien soveltuvuudesta tutkimusasetelmaan ei voida olla varmoja, on riski, että lopputuloksena on pikemminkin vääristynyt käsitys hyvästä tietoturvasta. Lopuksi, minkään tutkimuksien lopputuloksina esitetyn viitekehyksen toimivuudesta ei ole todisteita. Erityisesti viimeksi mainitun valossa työtä varten tarkasteltujen tutkimusryhmien viitekehyksiä ei voida hyödyntää tässä työssä. Työn lopputuloksena on tarkoitus päätyä ohjeistuksiin, joilla voidaan lähestyä aidosti hyväksi todettuja tietoturvakäytäntöjä.

Jotkin esimerkkeinä käytettyjen tutkimusten huomioista ovat silti hyvin perusteltuja ja todennettavissa. Vishwanathin sekä Trimin tutkimusryhmät saattavat keskittyä osittain liiaksikin työntekijöiden rooliin hyvän tietoturvan muodostamisessa. Silti ei voida kieltää, etteivätkö työntekijät ole tärkeä osa hyvää tietoturvaa. Tätä näkökulmaa tukevat esimerkiksi tavat, joilla järjestelmiin tunkeudutaan haittaohjelmilla [19][49]. Molemmat tutkimusryhmät esittävät myös omia lähteitään erilaisille tärkeille huomioille, kuten tietoturvavaatimusten tutkimuksen puutteille sekä tietoturvaloukkausten aiheuttamille mahdollisille vahingoille maineelle [59][60]. Suppeammat akateemiset tutkimukset, jotka eivät pyri laajamittaisten toimenpiteiden harjoittamisen teoriaan, esittävät myös hyviä huomioita joiltain yksityiskohtaisilta tietoturvan osa-alueilta. Esimerkkinä on Wagnerin tutkimusryhmän tietoturvauhkien jakamisen käytäntöjä koskeva tutkimus [64]. Tutkimusryhmä tuo esille hyviä huomioita sille, miksi uhkiin liittyvän tiedon tehokas jakaminen eri toimijoiden kesken on tehokas tapa estää uhkien leviämisen riskejä laajemmin eri piireissä. Vastapainoksi tutkimusryhmä nostaa myös esille tehokkuutta haittaavan ongelman luottamuksellisen tiedon hallinnassa muun tiedon jakamisen yhteydessä. Nämä ovat konkreettisia ongelmia, joita datahub-projektissakin on otettava huomioon [65].

Yhteenvetona voidaan todeta, että tietoturvatutkimus akateemisissa piireissä on vielä liian alussa, jotta se voisi tarjota kokonaisvaltaisia ohjeita hyvän tietoturvan määrittämiseksi. Tutkimukset kuitenkin tarjoavat hyviä kannanottoja ja tietoja eri puolilta tietoturva-alaa, jotka ovat huomioon ottamisen arvoisia. Nämä voivat toimia apuvälineinä päätöksenteossa, kun kokonaisvaltaista tietoturvaa pyritään suunnittelemaan. Varsinaista viitekehystä tai edes hyväksi todettujen käytäntöjen listaa esimerkkinä käytetyistä tutkimuksista ei kuitenkaan saada esitettyjen epävarmuustekijöiden valossa. Aiemmin kuitenkin todettiin kritisoitujen tutkimusten kohdalla, että kaikki niistä käyttivät hyödykseen asiantuntijoiden tuomia näkemyksiä hyvän tietoturvan rakenteesta. Esitettiin myös väite, että juuri asiantuntijat saattavat olla luotettavia lähteitä, koska heillä on käytännössä testattua tietotaitoa. Voidaan väittää, että käytännön testauksen tulokset erityisesti yhdistyessään pitkän ajan mittaan ovat luotettavimpia tutkimustuloksia. Ne ovat tulosta suoraan menetelmien soveltamisesta niiden varsinaisessa käyttötarkoituksessa, ja jos niitä on käytetty pitkään nousee todennäköisyys sille, että ne ovat joutuneet myös useamman kerran koetukselle. Näistä syistä myös tässä työssä pyritään luomaan katsaus tietoturvamenetelmiin, joita on altistettu käytännölle.

5.2 Suomalaisia referenssijärjestelmiä

Datahub ei ole Suomessa ensimmäinen tietojärjestelmä, jonka tekniseen rajapintaan liittymiselle on asetettu tietoturvavaatimuksia. Myös muihin käyttötarkoituksiin tarkoitetut järjestelmät, jotka sallivat tiedonvaihtoyhteyden rajapintoihinsa, kohtaavat saman tapaisia riskejä. Tarkastelemalla tällaisia ennakkotapauksia voidaan saada ohjaavia näkemyk-

siä tässä työssä suoritettavaan tietoturvavaatimusten muodostamiseen. Tämän vuoksi seuraavaksi tarkastellaan kolmea tällaista esimerkkiä: Kansallisen Terveysarkiston palveluita (Kanta tai Kanta-palvelut), Nordea Web Services -palvelua sekä Suomi.fi -palveluväylää. Kaikkia palvelujen tietoturvavaatimuksia ei tulla käymään läpi. Tietoturvavaatimuksista tarkastellaan pääasiassa tunnistautumistapoihin, lokitukseen ja seurantaan, palveluntarjoajalle luovutettaviin tietoihin sekä tietojen käsittelyyn liittyviä vaatimuksia. Myös joitakin tapauskohtaisia erityiskontrolleja nostetaan esiin näiden vaikuttaessa olevan arvokkaita vertailulle.

Referenssijärjestelmien tietoturvavaatimuksia asettavat tahot käyttävät eri termistöjä, joilla ne viittaavat itse järjestelmään sekä siihen liittyviin osapuoliin. Selkeyden vuoksi tässä työssä referenssijärjestelmien omissa tietoturvavaatimuksissa käytetyt termit on osaksi korvattu toisilla. Alla olevissa vertailuissa käytetään referenssijärjestelmään liittyvästä tahosta nimeä "liittyjäosapuoli" ja liitettävästä järjestelmästä "liittyjäosapuolen järjestelmä" tai "järjestelmä". Referenssijärjestelmästä käytetään lähtökohtaisesti sen omaa nimeä.

5.2.1 Kanta-palvelut

Kansallinen Terveysarkisto tai Kanta-palvelut on kokoelma tietojärjestelmäpalveluita Suomen kansalaisille sekä sosiaalihuollon, terveydenhuollon ja apteekkialan ammatinharjoittajille [66][67]. Ammatinharjoittajille keskeisimpiä näistä ovat keskitetty potilastiedon arkisto ja resepti-palvelu. Kanta-palvelut käsittävät myös muita palveluita ammatinharjoittajille, mutta näille ei aseteta erillisiä tietoturvavaatimuksia kuten potilastiedon arkistolle ja resepti-palvelulle. Kansalaisille Kanta-palvelut näkyvät lähinnä Omakanta-nimisenä palveluna, josta käyttäjä voi nähdä omat terveystietonsa ja reseptimääräyksensä sekä pyytää reseptiensä uusimista. Potilastiedon arkistoon ja resepti-palveluun ammatinharjoittajilta vaaditaan järjestelmä, joka ottaa yhteyden Kanta-palvelujen rajapintaan [68]. Omakanta taas on selainpohjainen palvelu eikä vaadi erillistä järjestelmää toimiakseen [69]. Tämän vuoksi sitä ei käsitellä tässä luvussa enempää.

Huomioitavaa osassa palveluista on se, että esimerkiksi resepti-palvelujen käyttö ja potilastietojen tallentaminen potilastiedon arkistoon ovat lakisääteisesti pakollisia laillistetuille ammattilaisille [70]. Kaikista suomalaisista, jotka ovat joskus tarvinneet terveydenhuollon palveluita, tallentuu lääkemääräys- ja potilastietoja Kanta-palveluihin. Kanta-palveluiden vastuulla on suojata näitä tietoja ja asettaa ne saataville palvelun muille asianmukaisille osapuolille. Toisin sanoen, Kanta-palvelut tallentavat suuria määriä hyvin arkaluontoista tietoa.

Kuten datahubiin liittyvät järjestelmät, myös Kanta-palveluihin kytkeytyvät järjestelmät käyvät läpi testausprosessin osana sertifiointia [71][72]. Liittyjäosapuolen järjestelmä liittyy Kanta-palveluihin Kanta-liityntäpisteeksi kutsutun tietoliikenteen pisteen kautta [68]. Liityntäpisteessä on Väestörekisterikeskuksen myöntämä palvelinvarmenne, jotta liittyjäosapuolen järjestelmä on tunnistettavissa liityntäpisteen ja Kanta-palvelujen välillä. Yhteys on salattu TLS-tekniikalla kuten datahubiin muodostettavat rajapinta-yhteydet [38]. Kanta-palvelujen rajapinnat noudattavat terveydenhuollon tietojärjestelmien integraatioiden kehittämiseen erikoistuvan HL7 Finland -yhdistyksen määritelmiä [73][74]. Ammatinharjoittajat ja organisaatiot käyttävät palveluita tarkoitukseen kehitettyjen tietojärjestelmien avulla, joiden kehitysprosessi on tarkkaan dokumentoitu ja säädelty [71][75]. Myös näiden järjestelmien käytölle on asetettu tarkkoja tietoturvavaatimuksia.

Tunnistautumiselle asetettavat vaatimukset
Ensisijainen tunnistautumisella valvottava vaihe Kanta-palvelujen käytössä on kirjautuminen liittyjäosapuolen järjestelmään eli siihen, jolla Kanta-palveluihin muodostetaan yhteys. Liittyjäosapuolen järjestelmän on sallittava yhteys Kantaan ainoastaan käyttäjän tunnistautuessa sosiaali- ja terveydenhuoltoalan varmennekortilla [75]. Järjestelmän annetaan sallia muulla tavoin kirjautuminen ainoastaan sellaisten toimintojen suorittamiseen, jossa käyttäjä pääsee tutkimaan vain liittyjäosapuolen omaan potilastietojärjestelmään tallennettuja tietoja. Jos tällainen muu kirjautumistapa vaatii salasanan käytön, salasanan on noudatettava Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) Sisäverkko-ohjeen mukaisia käytäntöjä [75][76][77].

Liittyjäosapuolen järjestelmässä ei saa pitää yleisluontoisia ylläpito- tai muita vastaavia oikeuksia ja toiminnallisuuksia eikä aktiivisia oletustunnuksia [75]. Kaikki järjestelmän käyttäjät tulee tunnistaa ja todentaa yksiselitteisesti. Esimerkiksi järjestelmän käyttölokiin on tallennuttava käyttäjän nimi, käyttäjätunnus, tunnistautumistapa, käyttäjätunnus sekä palveluyksikön tiedot järjestelmässä tapahtuneesta potilastietojen ja asiakirjojen käsittelystä [78]. Järjestelmän on pystyttävä tarkistamaan myös käyttäjän ammattioikeudet ja niiden mahdolliset rajoitukset Valviran ylläpitämästä palvelusta. Järjestelmän on kyettävä tarvittaessa rajaamaan käyttäjän toimintoja tämän noudetun tiedon perusteella.

Lokitus- ja seurantavaatimukset
Kanta-palvelujen tietoturvavaatimuksissa esiintyvät keskeisenä kaksi eri lokia: Liittyjäosapuolen järjestelmässä ylläpidettävät käyttöloki ja tekninen loki [75][78]. Käyttölokiin tallennetaan tietojen haun ja käytön osalta riittävän yksityiskohtaiset tiedot [75]. Tällaisia tietoja ovat muun muassa aiemmin mainitut liittyjäosapuolen käyttäjän tiedot, tapahtumaan liittyvät tiedot, tapahtuman tyyppi (tiedon haku, luku, kirjoitus, päivitys tai poisto), päivämäärä ja kellonaika, käyttävän järjestelmän tunniste sekä itsensä lokitapahtuman tunniste [78]. Käyttölokiin tulee tallentua myös joitakin erityistilanteita kuvaavat tiedot, kuten tieto ilman potilaan suostumusta suoritetusta toimenpiteestä sekä mahdolliset virheilmoitukset. Tekniseen lokiin on tallennettava Kanta-palvelun ja sen asiakkaiden välinen viestintä sekä liittyjäosapuolen järjestelmän tekniset virheet [75]. Erityishuomiona mainitaan, että lokia on pidettävä kaikissa niissä järjestelmissä, joiden kautta Kantaan välitetään potilastietoja. Lokeja tulee luonnollisesti myös pystyä seuraamaan joko järjestelmän sisällä tai ulkoisesti liitettävällä välineellä. Yleisemmin seurantaan liittyen mainitaan, että liittyjäosapuolen järjestelmän normaalin tietoliikenneprofiilin on oltava tiedossa ja epätavallinen liikenne on pystyttävä havaitsemaan.

Palveluntarjoajalle luovutettavat tiedot
Ennen järjestelmän käyttöönottoa liittyjäosapuolen on luovutettava Kelan Kanta-osoitehakemistoon seuraavat tiedot koskien liittyjäosapuolen Kanta-liityntäpistettä [68][79][80]:

- Liityntäpistettä käyttävän organisaation tai organisaatioyksikön OID-tunnus (Object Identifier -tunnus)
    - International Organization for Standardization Object Identifier (ISO OID) on yhdelle objektille kansainvälisesti ainutlaatuinen numerotunniste, joka on määritelty ISO:n ja International Electrotechnical Comission (IEC) -organisaation standardissa 9834-1:2012.

- Liityntäpisteen OID-tunnus.

- Järjestelmän tyyppi (esimerkiksi potilastietojärjestelmä, asiakastietojärjestelmä tai apteekkijärjestelmä.
- Sallitut Kanta-palvelut.
- Vastaanottopalvelujen verkko-osoitteet.
- Tietoliikenneosoitteet (IP-osoitteet, englannin sanoista Internet Protocol).

Kanta-osoitehakemistossa on myös oltava olemassa määritelty yhteys oman tai ulkoistetun liityntäpisteen sekä Kantaan liittyvän liittyjäosapuolen välillä [81]. Osoitehakemistosta on myös löydyttävä tarvittavat käyttöoikeudet jokaiselle Kanta-palvelua käyttävälle liityntäpisteen ja liittyjäosapuolen yhdistelmälle. Kummatkin näistä syntyvät hakemistoon liittyjäosapuolien täyttäessä Kantaa varten tarvittavan liittymishakemuksen. Kanta-osoitehakemistoon luovutettavien tietojen lisäksi liittyjäosapuolen järjestelmästä on pystyttävä kuvaamaan se, miten yleisiin hyökkäysmenetelmiin varaudutaan [75]. Kuvatun varautumisen on tapahduttava niin, että järjestelmässä käsiteltävien suojattavien tietojen luottamuksellisuus tai eheys ei vaarannu.

Tietojen käsittelyyn liittyvät vaatimukset
Tietojen käsittelyä koskevia tietoturvavaatimuksia sivuttiin jo aiemmin siltä osin, miten liittyjäosapuolen järjestelmän tulisi kontrolloida eri käyttäjien oikeuksia käsitellä erilaista tietoa. Kanta-palveluihin yhdistyvien järjestelmien ja niitä käyttävien organisaatioiden suorittamalle paikalliselle tiedon tallentamiselle on asetettu myös tietoturvavaatimuksia [75]. Potilastiedon arkistosta haettu tieto voidaan tallentaa paikallisesti liittyjäosapuolen järjestelmään siksi ajaksi, kun lakisääteinen määräaika sallii [82]. Potilaan tiedot on voitava aina tuhota tämän määräajan umpeutuessa.

Reseptikeskuksesta haettuja lääkemääräyksiin liittyviä asiakirjoja, kuten lääketoimituksia, ei saa tallentaa pysyvästi ollenkaan liittyjäosapuolen järjestelmään. Poikkeuksena ovat sellaiset tiedot, jotka ovat välttämättömiä lokeille asetettujen vaatimusten täyttämiseksi. Apteekeille on myös annettu lisäpoikkeuksena erilaiset toimialalla pidempää säilytystä vaativat tiedot. Muissa tapauksissa apteekit eivät saa tallentaa järjestelmäänsä reseptikeskuksesta hakemiansa tietoja kuin siksi aikaa, mitä toimituksen käsittely tai muu lainmukainen tarkoitus vaatii. Kaikkien tahojen on hävitettävä reseptikeskuksesta väliaikaisesti haettu tieto kokonaan heti kun niitä ei enää tarvita.

Yhteenveto ja johtopäätökset
Kanta-palveluihin liittyvissä tietoturvamääräyksissä näkyy suojattavan tiedon salainen luonne. Kanta-palveluiden suojattava tieto on arkaluontoista, joskus yksilön vahingoittamiseen soveltuvaa tietoa, kuten tietoa sairauksista ja hoitotarpeista. Sen vääriin käsiin joutuminen tai sen oikeudeton muuttaminen voidaan nähdä vakavampana, kuin saman tapahtuminen datahubissa liikkuvalle tiedolle. Tämä näkyy selkeästi tiukassa tietojen käsittelyn kontrollissa [75]. Ensinnäkin Kannasta saatavaa tietoa käsittelevän henkilön on täytynyt suorittaa ammattiin valmistava koulutus toisin kuin datahubin kohdalla. Toiseksi Kantaan liittyvien järjestelmien suunnittelu ja käyttö ovat hyvin tarkkaan kontrolloituja. Suuri osa tietoturvavaatimuksista painottuu nimenomaan Kantaan liittyvän osapuolen järjestelmän käyttöön ja paikallisesti järjestettäviin teknisiin käytäntöihin kuten tarkkaan kuvattujen lokien ylläpitämiseen ja tunnistautumisteknologioihin [75][78].

Teknisiin käytäntöihin puuttuminen liikaa on datahubin kannalta ongelmallista. Esimerkiksi laitehankinnat tuottavat aina resurssitarpeita, ja datahub-projektin kohdalla tällaisten asettamista markkinaosapuolille pyritään minimoimaan. Lisäksi Fingrid Datahub on sitoutunut varjelemaan puolueetonta markkinakilpailua, ja liiallisten muutosten vaatiminen kolmansien osapuolien kehittämille järjestelmille voi koitua hyvin kalliiksi näitä käyttäville osapuolille. Jotkin kytkeytyville järjestelmille asetettavista vaatimuksista, kuten laajempi ja tiukempi käyttäjän oikeuksien hallinnointi eri toiminnoissa saman järjestelmän sisällä, on myös datahubin kannalta tarpeetonta. Toisaalta Kanta-palveluiden tietoturvassa korostetaan tarkkaa seurantaa ja lokitusta, jotka saattavat olla jo hyödynnettyinä niissä järjestelmissä, jotka tulevat kytkeytymään datahubiin. Kuten aiemmassa luvussa todettiin, lokituksen ja seurannan tärkeyden huomiointi on tärkeää otettaessa huomioon vaikeus havaita jo valmiiksi järjestelmässä olevia hyökkääjiä, jotka saattavat odottaa operaationsa varsinaista alkua [44][49]. Järjestelmistä kerätty informaatio auttaa aina myös kaikkia muita tietoturvatoimenpiteitä, joihin yhtiö on investoinut, sillä se auttaa tietoturvasta vastuussa olevia toimijoita tekemään parempia päätöksiä ja löytämään vaihtoehtoja haitallisen toiminnan estämiseksi.

5.2.2 Nordea Web Services

Nordea Web Services on Nordea pankin tiedonvaihtoprotokolla, jolla pankki tarjoaa yrityksille mahdollisuuden lähettää ja vastaanottaa tiedostoja [83]. Yhteys on tarkoitettu niin sanottujen kassanhallintatiedostojen vaihtoon, jotka esiintyvät eri tiedostotyyppeinä [83]. Kassanhallinnalla tarkoitetaan yleisesti yritysten tai yksilöiden kassavirtojen keräämis- ja hallintaprosesseja [84]. Nordean omat kassanhallintapalvelut ovat kansainvälisiä yrityksille suunnattuja palveluita, joissa Web Services -protokolla on vain yksi elementti erilaisten konsultaatio- ja tukipalveluiden joukossa [85]. Toisin sanoen, protokollan kautta välitetään jatkuvasti yritysten talouteen liittyvää tietoa, jonka voidaan perustellusti olettaa olevan luottamuksellista. Jos protokollan salaus vaarantuisi, Nordeaa kohtaisi vakava maineen vahingoittumisen riski asiakkaiden pystyessä oikeutetusti kyseenalaistamaan pankin kyvyn turvata luotettavasti tälle luovutettu tieto. Voidaan siis turvallisesti olettaa, että pankille on tärkeää suojata Web Services erittäin hyvin.

Protokolla käyttää TCP/IP muotoista SSL-salattua yhteyttä [83]. Käyttäjät tunnistetaan yhteyden muodostuksessa pankin luovuttamalla Public Key Infrastructure (PKI) -varmenteella, joka on joko yritys- tai käyttäjäkohtainen riippuen asiakkaan toivomuksesta. PKI on digitaaliseen allekirjoitukseen pohjautuva varmenneteknologia osapuolten välisessä tietoliikenneyhteydessä [86]. Palvelua käyttävä asiakas, tai liittyjäosapuoli, luo yhteyden pankkiin jollakin kolmannen osapuolen tarjoamalla protokollaa tukevalla pankkiyhteysohjelmistolla [83]. Liittyjäosapuoli sitoutuu noudattamaan sekä Nordean yrityksille tarkoitettujen elektronisten palvelujen yleisiä ehtoja sekä Web Services tiedonsiirron käytölle erikseen asetettuja ehtoja [83][87][88]. Web Services -protokollan teknisempi Web Services Security and Communication Description -dokumentaatio esittää myös joitakin ohjeistuksia palvelun käytöstä käytännössä [89].

Tunnistautumiselle asetettavat vaatimukset

Nordea ei aseta varsinaisia vaatimuksia yhteyden muodostukseen käytettävän sovelluksen kohdalle, mutta se vaatii viestiliikenteessä käytettävän itse luovuttamansa PKI-varmenteen tarkkaa valvontaa. Tunnistautuminen PKI-teknologian avulla perustuu siihen, että varmenteen omaava osapuoli allekirjoittaa digitaalisesti lähettämänsä sanomat kryptografisella yksityisellä avaimella, joka on ainoastaan sen hallussa [86]. Vastaanottavat tahot taas omaavat lähettävän tahon julkisen avaimen, jolla sanomia ei voida allekirjoittaa mutta joka voi todentaa sanoman lähettävän tahon yksityisellä avaimella allekirjoitetuksi.

Pankin luovuttamaan PKI-varmenteeseen liitetään aina liittyjäosapuolen järjestelmän ylläpitäjän henkilökohtainen käyttäjätunnus, vaikka muut yrityksen työntekijät käyttäisivät varmennetta itse [83]. Pankin luovuttama PKI-varmenne täytyy suojata sen käyttäjän valitsemalla tunnusluvulla, eikä varmennetta saa olla mahdollista käyttää ilman sitä. Poikkeuksena tietoturvavaatimukset sallivat kuitenkin sellaiset tilanteet, jossa liittyjäosapuolen järjestelmän voidaan katsoa kontrolloivan käyttäjän käyttöoikeuksia jollain muulla tavoin. Esimerkkinä annetaan automaattinen yhteydenmuodostus, jossa järjestelmä käyttää siihen tallennettua PKI-varmenteen yksityistä avainta. Tällaisissa tilanteissa kaikki avaimella tehdyt transaktiot on kuitenkin tallennettava järjestelmän paikallisiin lokeihin. On huomioitavaa, että tämä on ainoa Nordean asettama lokitukseen liittyvä vaatimus liittyjäosapuolelle.

Nordea painottaa tietoturvavaatimuksissaan ja palvelujensa ehdoissa tunnistautumistietojen tarkkaa valvontaa [83][88]. Tunnistautumistietoja ei saa luovuttaa edes osittain muille kuin käyttöön oikeutetuille, eikä avattua palveluyhteyttä saa luovuttaa oikeudettomalle taholle. Liittyjäosapuoli voi valtuuttaa myös kolmannen tahon lähettämään tiedostonsa itsensä puolesta, mutta tässä tapauksessa kyseisellä kolmannella taholla on oltava oma PKI-varmenteensa [89]. Liittyjäosapuolen on pidettävä huolta, että varmenteet ja niiden yksityiset avaimet pysyvät vain niiden asianmukaisten omistajien hallinnassa [88]. Liittyjäosapuoli ei saa säilyttää tunnistautumistietoja kuten tunnuslukua ja varmenteen omaavaa laitetta samassa paikassa. Jos liittyjäosapuolen järjestelmään on tallennettu varmenteen yksityinen avain, sitä tietokonetta, jossa järjestelmä sijaitsee, on suojeltava asianmukaisesti [83]. Liittyjäosapuolen on hallinnoitava luetteloa siitä, ketkä henkilöt hallitsevat ja käyttävät sen tunnistautumistietoja ja huolehtia, että käyttöoikeutensa menettänyt henkilö (esimerkiksi työsuhteen päättyessä) luopuu asiakohtaisista tunnistautumisvälineistä. Järjestelmän ylläpitäjän vaihtuessa on aikaisemman ylläpitäjän hallinnoima varmenne vaihdettava. Varmenne on lisäksi uusittava kahden vuoden välein.

Jos liittyjäosapuolella on syytä olettaa varmenteen omaavan laitteen tai sen tunnusluvun kadonneen tai joutuneen oikeudettoman osapuolen haltuun tai tietoon, on osapuolella velvollisuus ilmoittaa pankille välittömästi [88]. PKI-varmenteen omistaja on vastuussa kaikista Nordealle lähetetyistä sanomista ja niistä mahdollisesti koituvista vahingoista [83][88]. Tämä varmenteen omistajan vastuu jatkuu siihen asti, kunnes pankki saa tiedon varmenteen joutumisesta sivullisen haltuun tai tiedon sellaisen laitteen katoamisesta, johon varmenne on tallennettu. Lisäksi vastuu jatkuu niin pitkään, että pankilla on ollut kohtuullisesti aikaa estää palvelun käyttö. Merkittävin kohta tässä tietoturvavaatimuksessa koskee tilanteen jälkiselvitystä: Jos käy ilmi, että liittyjäosapuoli on myötävaikuttanut menettelyillään tunnistautumistietojen vaarantumiseen, osapuoli on vastuussa kaikista vahingoista. Täten Nordea sitouttaa palveluaan käyttävän osapuolen huolehtimaan hyvin tarkasti omasta tietoturvakäyttäytymisestään koskien tunnistautumistietojen hallintaa.

Lokitus- ja seurantavaatimukset

Nordean tietoturvavaatimuksissa ei esiinny juuri ollenkaan liittyjäosapuolen järjestelmän toiminnan seurantaan tai lokitukseen liittyviä vaatimuksia [83][88]. Aiemmassa osiossa mainittiin PKI-varmenteen ja tunnusluvun suojaamiseen liittyvät vaatimukset. Nämä vaatimukset on jätetty sen verran avoimiksi, että liittyjäosapuolen voidaan olettaa suorittavan parhaiten näkemänsä tekniset toimenpiteet vaatimusten täyttämiseksi. Tämän lisäksi aiemmassa osiossa mainittiin vaatimus tallentaa liittyjäosapuolen järjestelmän lokiin toiminnot, jotka on suoritettu ilman tunnuslukua yksityisavaimen tallennusta hyödyntäen. Nordea ilmoittaa itse ylläpitävänsä tarkempaa lokia erilaisista toimeksiannoista ja

tahdonilmaisuista. Pankki kuitenkin vaatii liittyjäosapuolia ilmoittamaan aina tapauksista, jossa sen on syytä epäillä pankin keräämän tiedon oikeellisuutta. Nordea ilmoittaa, ettei itse tarkasta tallennettujen tietojen oikeellisuutta.

Palveluntarjoajalle luovutettavat tiedot
Tehdessään Web Services -palvelusopimuksen pankin kanssa liittyjäosapuolen on ilmoitettava yrityksensä tiedot, osapuolen järjestelmän ylläpitäjän tiedot ja tarvittaessa muiden yrityksessä toimivien käyttäjien tiedot [83]. Luovutettavia tietoja ei ole tarkemmin määritelty Nordean File Transfer Service Description -dokumentaatiossa, jossa vaatimus on kuvattu. Liittyjäosapuolen järjestelmän ylläpitäjä luovuttaa myös hankittavaa PKI-sertifikaattia varten seuraavat tiedot pankille:

- Liittyjäosapuolen yrityksen nimi (jos PKI-sertifikaatti on yrityskohtainen) tai käyttäjän nimi (jos PKI-sertifikaatti on käyttäjäkohtainen).
- Käyttäjätunnus.
- Maakoodi (esimerkiksi FI Suomelle, englannin sanoista Finland).
- Pankin ylläpitäjälle lähettämä aktivaatiokoodi.

Järjestelmän ylläpitäjän vaihtuessa pankille on ilmoitettava uusi ylläpitäjä sekä entisen ylläpitäjän tunnus, joka on yhdistetty vanhaan varmenteeseen.

Tietojen käsittelyyn liittyvät vaatimukset
Nordea ei erottele tarkemmin tietojen käsittelyyn liittyviä ohjeita tietoturvavaatimuksissaan. Pankin elektronisten palveluiden yleisissä ehdoissa liittyjäosapuolia kielletään ilman tekijänoikeuden omistajan kirjallista suostumusta julkaisemasta, toisintamasta tai jakamasta palvelujen sisältämää informaatiota, ellei palvelukohtaisissa ehdoissa olla toisin sovittu [88].

Yhteenveto ja johtopäätökset
Nordean palvelulleen asettamat tietoturvavaatimukset painottuvat raskaasti liittyjäosapuolen ohjeistamiseen siitä, miten sen tulee järjestää oma tietoturvansa käyttäessään Web Services -palvelua. Suurin osa tietoturvavaatimuksista keskittyy määrittelemään palvelussa tunnistautumiseen käytettävien välineiden suojelua. Nordea ei auditoi liittyjäosapuolta tältä osin aktiivisesti eikä rajoita sitä voimakkaasti siltä osin, millä kolmannen osapuolen palveluilla se saa muodostaa yhteyden palveluihinsa. Tässä lähestymistavassa voidaan tunnistaa kaksi vahvuutta. Ensinnäkään ei Nordean eikä sen liittyjäosapuolen tarvitse sijoittaa erityisiä lisäkuluja palvelun käyttöönottoa varten. Kulujen minimointi on todennäköisesti ainakin osittain välttämätöntä, kun kyseessä on markkinoilla oleva tuote lakivelvoitteisen järjestelmän sijaan. Toisaalta määrittelemällä tarkasti sen, minkä Nordea näkee hyvänä tietoturvakäyttäytymisenä, pankki asettaa liittyjäosapuolelle velvoitteen olla tarkka omasta tietoturvastaan ilman aktiivista valvontaa. Tietoturvaan käytettävien kustannuksien lisäksi pankki vähentää tällä tavoin omia riskejään käyttäen ennalta resursseja sen alueen määrittämiseksi ja sopimiseksi, jossa sitä ei voida pitää syypäänä tietoturvamurtoon.

Toisaalta edellä mainittu antaa joitakin viitteitä myös palvelun yritystä kohtaan kohdistamista riskeistä. On todennäköistä, että pankki ei hahmota liittyjäosapuolten kohdistavan

ainakaan todennäköisiä uhkia omiin järjestelmiinsä käyttäessään palvelua. Jos mahdollisen liittyjäosapuoleen kohdistuvan tietoturvahyökkäyksen voitaisiin kuvitella uhkaavan pahasti Nordean omaa omaisuutta olisi syytä kuvitella, että Nordea käyttäisi enemmän resursseja ehkäistäkseen näitä. Sama pätee tilanteeseen, jossa Nordean voisi kuvitella hahmottavan yhden liittyjäosapuolen tietomurron uhkaavan muita osapuolia palvelunsa kautta, kyseenalaistaen oman palvelunsa turvallisuuden. Toisaalta on selvää, että toisin kuin datahubin kohdalla ei Nordean Web Services -palvelun käytölle ole lakisääteisiä velvoitteita, eikä yksi osapuoli ole riippuvainen toisen järjestelmään toimittamista tiedoista. Datahubissa tällaisia tilanteita on esimerkiksi myyjien ja jakeluverkonhaltijoiden kohdalla. Liian pitkälle meneviä oletuksia tulee kuitenkin välttää arvioitaessa yritystä sen päältäpäin näyttäytyvän valmistautumisen tilan perusteella.

Jos Nordea on järjestänyt tietoturvansa siitä näkökulmasta, että tietoturvamurrot liittyjäosapuoliin eivät kohdista vakavia riskejä yritystä itseään kohtaan, on tilanne erilainen kuin datahubilla. Datahubin sisäisissä riskiarvioissa on nähty, että tietyissä tapauksissa järjestelmään liittyviin tahoihin kohdistuvat hyökkäykset saattavat heijastua muihin osapuoliin sen verran vakavasti, että pelkät jälkikäteen langetettavat sanktiot eivät ole riittäviä [90]. Toisaalta sanktiot ovat hyvin yleinen menettelytapa ja joissakin tilanteissa jopa välttämättömiä, jotta sopimuksen rikkojat voitaisiin saada oikeudenmukaiseen korvausvastuuseen. Datahubin tietoturvavaatimuksissa voidaan ottaa huomioon sanktion uhalla vaadittava perusteellinen tietoturvakäyttäytyminen palveluun liittyviltä käyttäjiltä. Tämän lisäksi on kuitenkin pyrittävä paljon perusteellisempiin tietoturvahyökkäysten ennaltaehkäisyihin, kuin mitä Nordea soveltaa Nordea Web Services -palvelussaan.

5.2.3 Suomi.fi-palveluväylä

Suomi.fi-palveluväylä (tästä eteenpäin “Palveluväylä”) on Väestörekisterikeskuksen organisaatioille tarjoama standardoitu tiedonsiirtokanava [91]. Palveluväylää hyödyntäen eri osapuolet voivat muodostaa turvatun tiedonvaihtoväylän välilleen tai tarjota omia palveluitaan internetissä. Tiedonvaihdon toisessa päässä on vähintään yksi jonkin osapuolen tarjoama sähköinen asiointipalvelu, joka tuottaa ja/tai käyttää Palveluväylän kautta liikkuvaa tietoa [92].

Palveluväylä sallii liittyjäosapuolten tunnistamisen sekä yhteyden salaamisen Väestörekisterikeskuksen vastuulla [92]. Osapuolten tunnistus tapahtuu Suomi.fi:n varmennepalvelun tuottamilla varmenteilla. Palveluväylä käyttää tiedonsiirtoprotokollanaan X-Road -teknologiaa, joka vuorostaan hyödyntää Hypertext Transfer Protocol (HTTP) -protokollan yli lähetettäviä SOAP-sanomia [93]. Liittyjäosapuolten on myös mahdollista hyödyntää Representational State Transfer (REST) -palveluja [94]. Palveluväylän käyttöönottoon tarvitaan Väestörekisterin tarjoamalle liityntäpalvelimeksi kutsutulle palvelimelle asennettava palveluväyläohjelmisto [95]. Liityntäpalvelin itsessään on X-Road-ratkaisussa keskeinen komponentti, jonka kautta liittyjäosapuolen järjestelmän liittäminen Palveluväylään tapahtuu. Kuten datahubin kohdalla myös Palveluväylässä on liityttävä ensin testiympäristöön omalla järjestelmällään ennen tuotantoympäristöön hyväksyttyä siirtymistä [72].

Tunnistautumiselle asetettavat vaatimukset

Väestörekisterikeskuksen Palveluväylälle asettamissa tietoturvavaatimuksissa tunnistautumiseen liittyvät kohdat koskevat lähinnä liittyjäosapuolen järjestelmän liittämistä palveluväylään. Ne ovat siis käytännössä passiivisesti hallittavia vaatimuksia aktiivisten, kuten käyttäjätunnukselle ja salasanalle asetettavien ehtojen sijaan. Vaatimuksissa maini-

taan, että liittyjäosapuolen järjestelmä tulee liittää Palveluväylään erityisen alijärjestelmän kautta [96]. Tätä perustellaan muun muassa käyttöoikeuksien hienojakoisemman määrittelyn mahdollistamisella. Alijärjestelmän tunnisteeseen sisältyy sen omistavan organisaation tunnus, ja tietojärjestelmän tunnisteeseen vuorostaan sisältyvät nämä tunnukset.

Kuten aiemmin on mainittu, Palveluväylään liittymisen keskiössä on Väestörekisterikeskuksen omistama, liittyjäosapuolelle tarjottava liityntäpalvelin, johon alijärjestelmä lisätään [92][97]. Alijärjestelmän lisäksi liityntäpalvelimelle on asennettava Väestörekisterikeskuksen tarjoama palveluväyläohjelmisto [95]. Jokaisella Palveluväylään liittyvällä järjestelmällä on oltava käytössään liityntäpalvelin, mutta liityntäpalvelin itse voi olla osapuolikohtainen tai usean liittyjäosapuolen yhteinen [92]. Sen lisäksi, että liityntäpalvelin sisältää liittyjäosapuolen järjestelmän Palveluväylään liittävän alijärjestelmän, liityntäpalvelin vastaa myös "mm. palvelukutsujen välittämisestä järjestelmien välillä, palvelukutsujen varmennekättelystä, tietoliikenteen ja sanomien salauksesta, lokituksesta sekä käyttöoikeuksien hallinnasta". Edellä mainittu liityntäpalvelinten tietoliikenteen ja sanomien salaus tapahtuu Väestörekisterikeskuksen varmennepalvelun tuottamalla varmenteella, jota liittyjäosapuolen on haettava Palveluväylään liittymistä varten.

Lokitus- ja seurantavaatimukset
Väestörekisterikeskuksen tarjoama liityntäpalvelin huolehtii itse Palveluväylän käytöltä vaadittavasta lokituksesta [98]. Liityntäpalvelimen lokeihin tallentuu ainakin seuraavien, keskeisimmiksi kuvattujen palvelujen toiminnot [92][98]:

- Xroad-confclient: Global conf -konfiguraatiotiedostojen hausta keskuspalvelimelta (Väestörekisterikeskuksen omistamat ja ylläpitämät palvelimet, jotka hoitavat muun muassa yhteistä konfiguraatiohallintaa ja varmennepalveluita Palveluväylässä) vastaava asiakassovellus.

- Xroad-jetty: Käyttöliittymän sovelluspalvelin.

- Xroad-proxy: Liityntäpalvelinten välisestä sanomaliikenteestä vastaava komponentti.

- Xroad-signer: Avainten hallinnasta ja mm. sanomien allekirjoituksesta sekä allekirjoitusten verifioinnista vastaava komponentti.

- Nginx: WWW-palvelin.

Vaikka liityntäpalvelin hoitaakin lokituksen itse, tietoturvavaatimuksissa kuitenkin vaaditaan liittyjäosapuolta valvomaan kyseisiä palveluita. Sen lisäksi liittyjäosapuolen velvollisuuksiin kuuluvat edellä mainittujen lokien säilyttäminen ja arkistointi [92][96]. Tietojen säilytysaika riippuu lainsäädännöstä tai edeltä määrittelemättömistä muista vaatimuksista [92]. Vaatimuksissa huomautetaan, että myös kolmannet tahot joiden kanssa liittyjäosapuolella on tiedonvaihtoon liittyvä sopimus saattavat edellyttää lokeihin tallennettavia tai muuten ylöskirjattavia lisätietoja. Tapahtuma- ja lokitiedoista on pystyttävä selvittämään taho, joka on käsitellyt kyseessä olleita tietoja. Käyttöehtojen luvussa 21, "Seuranta ja valvonta", vaaditaan lisäksi Palveluväylää käyttävän henkilöstön riittävää tietoturvakoulutusta liittyjäosapuolelta.

Lokituksen järjestämisen lisäksi Väestörekisterikeskus vaatii itselleen laajoja valvontapalveluita Palveluväylän käytön yhteydessä [92]. Ensinnäkin Väestörekisterikeskus ilmoittaa, että se tai sen osoittama palveluväyläoperaattori saattaa suorittaa porttiskannauksia liityntäpalvelimeen sen ympäristön tietoturvan todentamiseksi. Toiseksi Väestörekisterikeskus pitää itsellään oikeuden edellyttää liittyjäosapuolelta etävalvontaa liityntäpalvelimiin omasta tai palveluväyläoperaattorin toimesta. Väestörekisterikeskuksella pitää itsellään oikeuden myös julkaista liittyjäorganisaatiolle luovutettua liityntäpalvelinta koskevia valvontatietoja sekä näiden perusteella tietoa liityntäpalvelimen häiriöttömyyden tilasta.

Palveluntarjoajalle luovutettavat tiedot
Väestörekisterikeskukselle on Palveluväylään liityttäessä ilmoitettava ainakin seuraavat tiedot [92][94]:

- Liittyjäosapuolen organisaatio.

- Yhteyshenkilöt.
    - Liittyjäosapuolen on nimettävä tekninen yhteyshenkilö ja varayhteyshenkilö, sekä hallinnollinen yhteyshenkilö ja varayhteyshenkilö.
    - Liittyjäosapuolen on myös nimettävä tietosuoja ja -turvavastaava, jos Väestörekisterikeskus näin edellyttää.

- Palveluväylän käyttäjistä henkilötiedot sekä käyttöehdoissa mainitut mutta tarkemmin määrittelemättömät "muut tiedot".

- Liitettävä(t) järjestelmä(t).

Liityntäpalvelinta koskien on luovutettava seuraavat tiedot:

- Liityntäpalvelimen ohjelmistoversion tiedot

- Liityntäpalvelimen käyttöjärjestelmään asennetut paketit

- Liityntäpalvelimella käytössä olevat palvelut

Tietojen käsittelyyn liittyvät vaatimukset
Palveluväylään liittyvää tietojen käsittelyä koskevissa vaatimuksissa painottuvat Palveluväylän luonne järjestelmänä, joka yhdistää toisiinsa mahdollisesti luottamuksellisia tietoja keskenään vaihtavia osapuolia. Liittyjäosapuolella ei ole oikeutta luovuttaa eteenpäin Palveluväylän kautta saatua materiaalia, joka ei ole julkista ilman oikeudenomistajan kirjallista suostumusta [92]. Kaikki Palveluväylän käytön yhteydessä paljastuva Väestörekisterikeskuksen, muiden liittyjäosapuolien tai näiden mahdollisten alihankkijoiden liiketoimintaa tai teknisiä ratkaisuja koskeva aineisto on salassa pidettävää. Palveluväylän avulla keskenään tietoja vaihtavien osapuolten sekä Väestörekisterikeskuksen on merkittävä asiaankuuluvassa yhteydenpidossaan ne asiakirjat, asiakirjojen kohdat ja mahdolliset alihankkijoiden aineistot, jotka ovat salassa pidettäviä. Vastuu mahdolliseen salassapitoon mainitaan jatkuvan myös Palveluväylän käytön loputtua. Liittyjäosapuolia velvoitetaan selvittämään henkilöstölleen ja alihankkijoilleen, mikä tietoaineisto on luottamuksellista ja miten sen salassapito ja luottamuksellisuus on järjestettävä.

Yhteenveto ja johtopäätökset
Kuten Kanta-palveluiden kohdalla, myös Palveluväylään yhdistettäessä palvelua hallinnoiva taho, tässä tapauksessa Väestörekisterikeskus, asettaa tiukkoja ehtoja liittyjäosapuolten järjestelmille. Toisin kuin Kanta-palveluiden kohdalla, Palveluväylään luodaan kuitenkin yhteys Väestörekisterikeskuksen luovuttamilla ohjelmistoilla ja komponenteilla. Vaatimusten rajaaminen yhteyden ottavaan komponenttiin mahdollistaa liittyjäosapuolten harjoittaa ohjelmistonkehitykseen, digitaalisten palveluiden tarjontaan tai muuhun samankaltaiseen käyttöön liittyvää toimintaansa vapaammin. Väestörekisterikeskus tosin vaatii itselleen hyvin laajamittaisia oikeuksia koskien sen luovuttamia ja liittyjäosapuolen käyttämiä liityntäpalvelimia. Edellisten valvontaan liittyvien toimenpiteiden lisäksi Väestörekisterikeskus pitää itsellään oikeuden myös esimerkiksi vaatia liittyjäosapuolta asentamaan tarpeelliseksi näkemiään päivityksiä liityntäpalvelimilleen [92]. Väestörekisterikeskus vaatii myös oikeuden asettaa tarvittaessa liittyjäosapuolelle ja sen Palveluväylään kytketylle järjestelmälle erityisiä tietoturvavaatimuksia.

Väestörekisterikeskus hahmottaa selkeästi Palveluväylän toiminnan luonteen mahdollistavan tietoturvauhkien leviämisen yhdestä osapuolesta muihin. Tämä ilmenee valvontaoikeuksien vaatimisen lisäksi muun muassa tarkkaan määriteltyjen tietojen käsittelyä koskevien tietoturvavaatimusten kohdalla. Näissä vaatimuksissa korostuvat esimerkiksi Palveluväylän yhdistävien Väestörekisterikeskuksen ulkopuolisten osapuolten keskinäisten sopimusten kunnioittaminen. Palveluväylän voidaan siis nähdä sisältävän osittain samanlaisia haavoittuvuuksia kuin datahub koskien tietoturvauhan leviämistä yhdestä osapuolesta useampaan. Ne tavat, joilla tällaisilta haavoittuvuuksilta koetetaan suojautua Palveluväylän puolella ovat kuitenkin hieman ongelmallisia datahubin kannalta. Palveluväylään liittyminen ei ole lakisääteinen pakote, joten liittyjäosapuolet voivat arvioida tarpeensa ja resurssinsa ennen suostumistaan muun muassa laajoihin valvontatoimenpiteisiin. Datahubin kohdalla ainakin yhtä laajojen toimenpiteiden soveltaminen Suomen kaikkiin sähkön vähittäismarkkinoiden osapuoliin voisi haitata markkinoita huomattavasti. Datahub ei myöskään voi vaatia itselleen oikeuksia valvoa markkinaosapuolten omia järjestelmiä kuten VRK tekee.

Palveluväylää voidaan pitää hyvänä esimerkkinä siitä, miten pitkälle suomalaisissa sähköisissä palveluissa tietoturvavaatimuksia on viety liittyjäosapuolen valvonnan osalta. Joitakin ideoita esimerkiksi siitä, mihin ja miten valvontaa on kohdistettu, voidaan mahdollisesti hyödyntää datahubin tietoturvavaatimuksissakin. Lisäksi liittyjäosapuolista liitynnän yhteydessä rekisteröitävät tiedot voivat olla asioita, jotka on määriteltävä tarkkaan mahdollisten uhkien tunnistamiseksi. Kun kaikista liittyjäosapuolista on tarjolla tarpeeksi tarkat tiedot voi mahdollisten tietoturvamurtojen tai -hyökkäysten jälkiselvitys helpottua, kun tiedot tekevät mahdolliseksi osapuolten tarkemman kartoittamisen. Kuitenkin kaikissa tapauksissa, jossa Palveluväylästä otetaan mahdollisesti mallia datahubin tietoturvavaatimuksiin, on tärkeätä punnita tarkkaan erot kaupallisen palvelun ja lakisääteisen palvelun asettamista tietoturvavaatimuksista.

5.2.4 Yhteenveto ja vertailu

Edellä tarkasteltujen referenssijärjestelmien vertailu nostaa erityisesti esille tämän luvun alussa mainitut tapauskohtaiset vaatimukset. Referenssijärjestelmien tietoturvavaatimukset ovat hyvin erilaisia toisistaan. Osittain erojen voidaan nähdä suoraan johtuvan referenssijärjestelmän luonteesta. Esimerkkinä tästä ovat Kanta-palveluihin yhdistettävien järjestelmien käyttöoikeuksien valvontaan liittyvät vaatimukset, jotka ovat olennaisia käsiteltävän tiedon luonteen vuoksi [78]. Toisaalta joitakin yleisesti hyväksi todettuja käytäntöjä voidaan myös tunnistaa. Tällaisia ovat esimerkiksi erilaiset seurantaan liittyvät

toimenpiteet sekä osapuolelle luovutettavat tiedot. Tosin on huomioitava, että samoja kategorioitakin käsittelevät kontrollit vaihtelevat voimakkuudeltaan eri järjestelmien välillä, seikka joka myös tuo esille tietoturvavaatimusten tarpeiden tapauskohtaisuutta.

Referenssijärjestelmien tietoturvavaatimusten voimakkaan tapauskohtaisuuden vuoksi ne eivät voi tarjota suoria esimerkkejä datahubiin liittyviä osapuolia määriteltäville tietoturvavaatimuksille. Niitä voidaan kuitenkin monessa suhteessa käyttää viitteenä siitä, millaisia järjestelyjä on jo toteutettu suomalaisilla markkinoilla. Tässä työssä ne ovat hyödyksi, kun datahubiin liittyville osapuolille määriteltäviä tietoturvavaatimuksia kootaan, antaessa viitteitä ennakkotapauksina muuta kirjallisuutta tulkitessa. Taulukkoon 3 on koottu tiivistelmä kaikista edellä tarkastelluista referenssijärjestelmistä ja arvioiduista kontrolleista. Taulukko on yksinkertaistettu niin, että siinä tuodaan esiin edellä tehdyssä tarkastelussa keskeisimmäksi esiin nousseet asiat.

Taulukko 3. Referenssijärjestelmien vertailu [66][68][82][83][87][88][92][91][97].

Referenssi-järjestelmä	Kanta-palvelut	Nordea Web Services	Suomi.fi-palveluväylä
Käyttötarkoitus	Sosiaali- ja terveydenhuollon sekä apteekkien tietojärjestelmäpalvelut	Pankin tarjoama tiedonvaihtoprotokolla yritysasiakkaiden kassanhallintapalveluille	Väestörekisterikeskuksen tiedonsiirtokanava sähköisten palveluiden käytölle ja tarjonnalle
Liittyjäosapuoli	Asianmukaista alaa edustava organisaatio	Nordean yritysasiakkaat	Palvelua hyödyntävät tietojärjestelmien tuottajat tai käyttäjät
Ensisijainen tunnistautumisen vaativa vaihe	Liittyjäosapuolen järjestelmään kirjautuminen	Yhteyden muodostus pankkiin	Liittyjäosapuolen järjestelmän liittäminen palveluväylään
Pääasiallinen tunnistautumistapa	Terveydenhuollon varmennekortti	Pankin luovuttama PKI-sertifikaatti	Sen alijärjestelmän tunniste, joka liittää liittyjäosapuolen järjestelmän Palveluväylään
Lokitus ja seuranta	Oltava käyttöloki, johon tallennetaan tietojen haun ja käytön osalta yksityiskohtaiset tiedot	Liittyjäosapuolen järjestelmän on lokitettava sellaiset transaktiot, jossa toiminnot suoritetaan järjestelmään tallennetulla PKI-sertifikaatilla	VRK:n omat palvelut keräävät lokitietoja, mutta asiakkaalla on vastuu lokitietojen valvontaan ja säilyttämiseen
	Oltava tekninen loki, joka tallentaa Kanta-palveluiden ja sen asiakkaiden välisen viestinnän sekä järjestelmän tekniset virheet		Lokitiedoista selvittävä taho, joka on käsitellyt liikkunutta tietoa
	Organisaation järjestelmän normaali tietoliikenneprofiili tunnettava ja epätavallinen liikenne pystyttävä havaitsemaan		
Luovutettavat tiedot	Liityntäpistettä käyttävän organisaation OID-tunnus	Liittyjäosapuolen yrityksen tiedot	Liittyjäorganisaatio
	Liityntäpisteen OID-tunnus	Liittyjäosapuolen järjestelmän ylläpitäjän tiedot	Liittyjäosapuolen tekninen ja hallinnollinen yhteyshenkilö sekä varahenkilöt
	Järjestelmän tyyppi	Tarvittaessa muut liittyjäosapuolen henkilöt, jotka käyttävät Web Servicesiä	Liittyjäosapuolen tietosuoja- ja turvavastaava
	Sallitut Kanta-palvelut	Ylläpitäjä ilmoittaa sertifikaatin latausta varten seuraavat tiedot:	Käyttäjistä henkilötiedot

	Vastaanottopalvelujen verkko-osoitteet IP-osoitteet	• Yrityksen nimi • Käyttäjätunnus • Maakoodi (esim. FI Suomelle) • Pankin ylläpitäjälle lähettämä aktivaatiokoodi	Liitettävä(t) tietojärjestelmä(t) Liityntäpalvelinta koskien: • Liityntäpalvelimen ohjelmistoversion tiedot • Liityntäpalvelimien käyttöjärjestelmään asennetut paketit • Liityntäpalvelimella käytössä olevat palvelut
Tietojen käsittely	Potilastiedon arkistosta haetut tiedot voidaan tallentaa liittyjäosapuolen järjestelmään vain siksi ajaksi, lakisääteinen määräaika sallii.	Asiakas ei saa ilman tekijänoikeuden omistajan kirjallista suostumusta julkaista, toisintaa tai jakaa edelleen palvelujen sisältämää tietoa ellei palvelukohtaisissa ehdoissa olla sovittu toisin	Liittyjäosapuolella ei oikeutta luovuttaa eteenpäin Palveluväylän kautta saatua tietoa ilman sen omistajan kirjallista suostumusta
	Reseptikeskuksesta haettuja lääkemääräyksiin liittyviä asiakirjoja voidaan tallentaa osapuolen järjestelmään vain siksi ajaksi, kun toimialan vaatimukset määräävät.		

5.3 Asiantuntijaorganisaatioiden kehittämät työkalut

Akateeminen kirjallisuus ja referenssijärjestelmät eivät ole ainoita esimerkkejä, joista etsiä hyviä tapoja tietoturvan määrittämiseksi. Erilaiset kansalliset ja kansainväliset asiantuntijaorganisaatiot omaavat laajasti tätä aluetta käsittelevää materiaalia. Suurena erona näiden organisaatioiden toimintaan verrattuna akateemiseen tutkimukseen on se, että ne pyrkivät tuomaan materiaalia tietoturvan kehittämiseksi tai arvioimiseksi suoraan käytäntöön tutkimuksen sijaan [54][55][56][57]. Ne pyrkivät vastaamaan suoraan organisaatioiden tarpeeseen varmistua omasta tietoturvastaan mahdollisimman tehokkaasti. Monet näistä tuotoksista ovat työkaluja tai sertifikaatteja, joita useat asiantuntijat ovat suunnitelleet yhteistyössä toistensa ja joskus myös valtion tai teollisuuden kanssa.

Tässä luvussa tullaan tarkastelemaan kolmen eri asiantuntijaorganisaation aiheeseen oleelliseksi nähtyjä tuotoksia: Yhdysvaltalaisen National Institute of Standards and Technology (NIST) -instituutin viimeisintä versiota kriittisen infrastruktuurin tietoturvan kehittämiseen tarkoitetusta viitekehyksestä, Kansallista turvallisuusauditointikriteeristöä (Katakri), sekä kahta ISO/IEC 27000 -sarjaan kuuluvaa tietoturvaa käsittelevää standardia [54][55][56]. Työkalut on valittu asiantuntijahaastattelujen suositusten kautta siten, että kaikki niistä olisivat vähintään Suomessa hyväksi todettuja ja käytettyjä tietoturvan määrittämiseen soveltuvia työkaluja. Työkaluja tullaan tarkastelemaan pääasiallisesti sen osalta, miten ne soveltuvat tämän työn tavoitteeseen määritellä tietoturvavaatimuksia datahubiin liittyville osapuolille.

5.3.1 NIST:n viitekehys kriittisten infrastruktuurien kyberturvallisuuden kehittämiseen

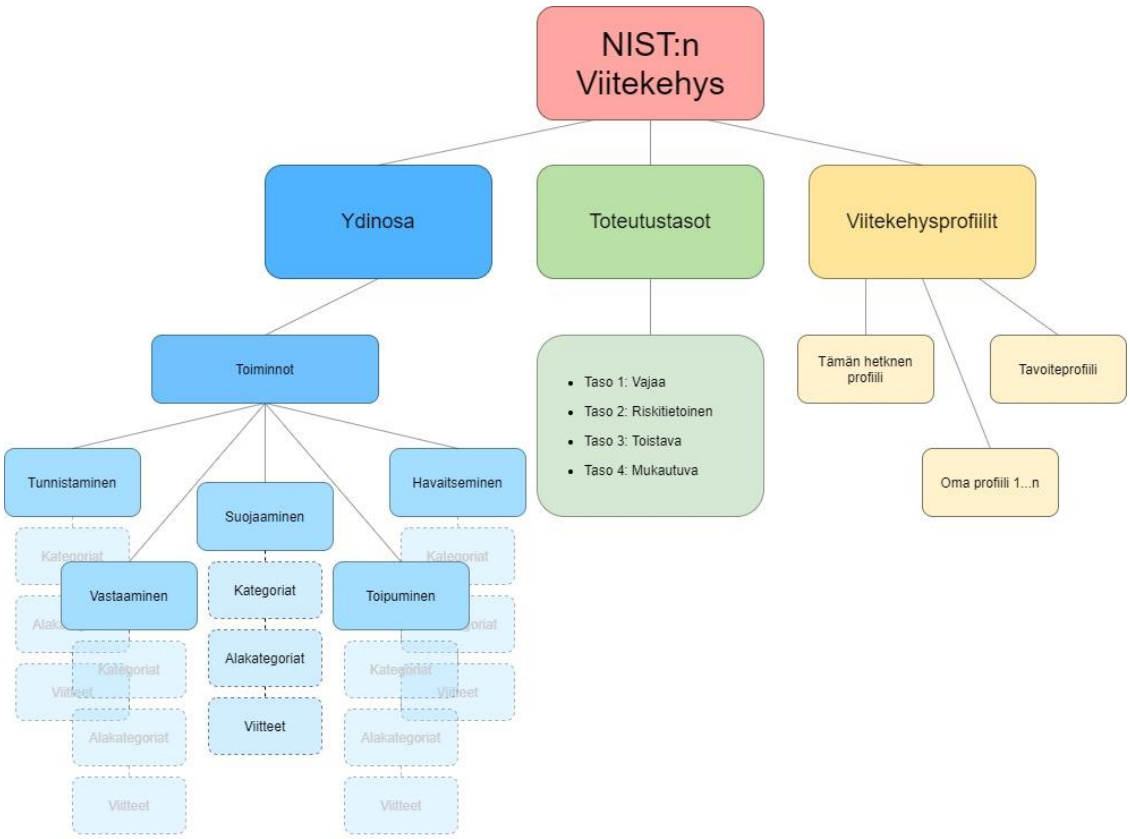
Yhdysvaltalainen NIST on vuonna 1901 perustettu instituutti, joka on nykyään osa Yhdysvaltain kauppaministeriötä [99]. Sen tehtävä on yhdysvaltalaisen innovaation ja teollisuuden kilpailukyvyn tukeminen. NIST toteuttaa tätä edistämällä mittaustieteitä, standardeja ja teknologiaa jotka tehostavat muun muassa taloudellista turvaa. Yhdysvaltojen kongressin vuoden 2014 joulukuussa määräämä asetus kyberturvallisuuden kehittämisestä (CEA, englannin sanoista Cybersecurity Enhancement Act) määräsi instituutin muuttamaan rooliaan koskien kriittisten infrastruktuurien kyberturvallisuuden tukemista [54][100]. Tätä tavoitetta varten NIST määrättiin luomaan viitekehys, jota voidaan hyödyntää asianmukaisten tahojen tietoturvariskien tunnistamisessa, arvioimisessa ja hallinnassa [54]. Asetuksen pohjalta NIST:n jo aiemmin julkaiseman "Framework for Improving Critical Infrastructure Cybersecurity" ensimmäinen versio päivitettiin vuoden 2018 huhtikuussa versioon 1.1 vastaanotetun palautteen pohjalta vastaamaan paremmin asetettuja tarpeita.

NIST:n kehittämän viitekehyksen hyötyä tämän työn tavoitteisiin voidaan perustella useilla argumenteilla. Ensinnäkin viitekehystä käytetään laajasti Yhdysvalloissa niin julkisella kuin yksityisellä sektorilla tietoturvatavoitteiden saavuttamiseksi [101]. Myös kansalliset tietoturvariskien hallintaan erikoistuvat tahot Yhdysvaltojen ulkopuolella, kuten Israelin kansallinen kyberdirektoraatti sekä Suomen Liikenne- ja viestintäviraston hallinnoima Kyberturvallisuuskeskus, pitävät NIST:n viitekehystä hyvänä työkaluna tietoturvan kehittämiseen [102][103]. Instituutti itsessään on myös toiminut tietoturvariskienhallinnan tehtävissä yhteistyössä muun muassa Yhdysvaltain armeijan kanssa, jota voidaan pitää luotettavasta tietotaidosta kriittisesti riippuvana tahona riskienhallintaan liittyvissä projekteissa [104]. Viitekehystä päivitetään teollisuudelta tulevan palautteen perusteella instituutin tehdessä yhteistyössä sekä Yhdysvaltojen yksityisen, että julkisen sektorin kanssa [54]. Toisin siis kuin useiden akateemisten tutkijoiden kehittämiä tietoturvakriteeristöjä, NIST:n asiantuntemusta ja sen viitekehystä on todistetusti hyödynnetty

käytännön riskinhallinnassa. Viitekehystä on myös kehitetty käytännön kokemuksesta esiin tulleeseen palautteeseen pohjautuen abstraktimpien ja tuntemattomampien akateemisten menetelmien sijaan. Lopuksi, vaikka viitekehys on kehitetty ensisijaisesti kriittisten infrastruktuurien omistajien tarkoituksiin (joihin muun muassa jakeluverkonhaltijat kuuluvat määritelmällisesti [20]), se on silti suunniteltu vastaamaan myös muunlaisten teollisuuden toimijoiden tarpeita näiden koosta riippumatta [54].

NIST:n viitekehys on pääasiassa tarkoitettu organisaatioiden itselähtöisen päätöksenteon tukemiseen tietoturvan tason arvioimiseen ja kehittämiseen liittyvissä asioissa [54]. Tätä ei nähdä kuitenkaan ongelmana tämän työn tavoitteiden kannalta. Ensinnäkin viitekehyksen modulaarinen rakenne sallii sen hyödyntämisen käyttämällä siitä vain tapauskohtaisesti tärkeäksi nähtyjä osia. Toiseksi viitekehyksen esimerkkejä hyvistä tietoturvakäytännöistä voidaan soveltaa tietoturvavaatimusten määrittelyyn datahubiin liittymistä varten, vaikka ne olisivatkin alun perin esitetty organisaatioiden itsearviointia varten.

Viitekehys koostuu kolmesta ylätason osasta, jotka jakautuvat edelleen alakategorioihin [54]. Alakategoriat eroavat sen mukaisesti, millaiseen käyttöön niiden ylätaso on suunniteltu. Seuraavassa osiossa tämä rakenne esitellään tarkemmin. Jokaisen ylätason ja sen alakategorioiden kohdalla tarkastellaan sitä, miten kohtia voidaan hyödyntää tämän työn tavoitteissa. Kuvassa 2 on hahmotelma viitekehyksen rakenteesta.



Kuva 2. NIST:n viitekehyksen rakenne [54].

Viitekehyksen ydinosa
Ydinosa on kokoelma tietoturvakäytäntöjä asiaankuuluvineen viitteineen, joiden NIST näkee olevan yhteisiä kaikilla kriittisten infrastruktuurien alueilla [54]. Ydinosa jaetaan edelleen viiteen rinnakkaiseen ja jatkuvaan tietoturvariskeihin liittyvään toimintoon. Nämä toiminnot ovat tunnistaminen, suojaaminen, havaitseminen, vastaaminen ja toipuminen. Toiminnot on luotu auttamaan organisaatioita näiden riskienhallinnassa tarjoamalla työkaluja hahmottamaan itseensä kohdistuvia uhkia sekä antamalla esimerkkejä hyväksi todetuista käytännöistä lähestyä tunnistettuja riskejä. Jokainen toiminto jaetaan edelleen kategorioihin ja alakategorioihin, jotka ryhmittelevät toimintoon kuuluvia menettelytapoja yksityiskohtaisemmin. Alakategorioita voidaan pitää yksityiskohtaisina kontrolleina. Jokaiseen näistä kontrolleista on lisäksi liitetty viitteet, jotka toimivat esimerkkeinä kontrollien toteutumisesta muissa lähdeaineistoissa.

Datahubiin liittyvien osapuolten tietoturvaa määrittäessä edellä mainittua ydinosaa, erityisesti sen alakategorioita, voidaan käyttää hyväksi tietoturvavaatimusten laatimisessa. Monet alakategorioista ovat kuitenkin hyvin spesifejä ja määritelty itsetarkastelevasta näkökulmasta, joten ne eivät voi suoraan toimia tietoturvavaatimuksina. Alakategoriat tarjoavat kuitenkin ohjaavia esimerkkejä, joiden pohjalta varsinaisia tietoturvavaatimuksia on mahdollista koota.

Viitekehyksen toteutustasot
Toteutustasot tarjoavat kontekstin luokitella organisaatioita sen mukaan, miten ne ymmärtävät ja lähestyvät kohtaamiaan tietoturvariskejä [54]. Määritellyt toteutustasot ovat Vajaa, Riskitietoinen, Toistava ja Mukautuva ensimmäisen edustaessa heikointa tasoa ja viimeisimmän parhainta. NIST toteaa, ettei toteutustasoja pitäisi kohdella kypsyystasoina tietoturvakäytäntöihin liittyen vaan kehittämisen päätöksentekoa ohjaavana työkaluna. Toteutustasot ovat varsin yksityiskohtaisesti kuvattuja, useita kriteerejä sisältäviä tavoitteita. NIST painottaakin, ettei organisaatiokohtaisissa tietoturvatavoitteissa onnistumista tulisi arvioida täysin niihin perustuen, vaan pikemmin seuraavaksi esiteltävien viitekehysprofiilien kautta.

Toteutustasoja on hyvin vaikea käyttää arvioimaan organisaatioita näiden ulkopuolelta, sillä joidenkin kriteerien arviointi saattaa vaatia hyvin tarkkaa organisaation tuntemusta mukaan lukien liikesalaisuuksien ymmärrystä. Näin ollen esimerkiksi tietyn tason vaatiminen datahubiin liittyvältä markkinaosapuolelta olisi hyvin vaikeaa, sillä kustannustehokkaita tapoja todentaa osapuolen täyttämät kriteerit tässä kontekstissa ei ole. Toteutustasoja voidaan kuitenkin hyödyntää kannustaessa osapuolia tietoturvansa itsearviointiin.

Viitekehysprofiilit
Viitekehysprofiilit ovat spesifimpiä hahmotelmia organisaation tietoturvan nykyisestä ja tavoiteellisesta tasosta kuin toteutustasot [54]. Profiileista ei ole koottu tarkkoja täytettäviä kriteereitä. NIST määrittelee viitekehysprofiilit "organisaation toimintojen, kategorioiden ja alakategorioiden kohdennuksiksi organisaation liiketoimintavaatimusten, riskitoleranssin ja resurssien kanssa". Ne ovat siis päätöksentekoa ohjaavia hahmotelmia organisaation tietoturvan tilasta sekä sen oma- ja yksityiskohtaisista tarpeista.

NIST toteaa organisaatioiden saattavan hyötyä useammankin profiilin luonnista, mutta antaa esimerkkejä vain "tämänhetkisen profiilin" ja "tavoiteprofiilin" luonnista. NIST:n mukaan organisaatiot luovat ensimmäisen analysoidessaan mitä toimintojen kategorioiden ja alakategorioiden lopputulemia sen tietoturva tällä hetkellä saavuttaa täysin tai vaillinaisesti. Tavoiteprofiili luodaan suorittamalla riskiarvio, jonka pohjalta katsotaan mitä

toimintojen kategorioita ja alakategorioita tulisi lähestyä ja millä tavoin haluttujen päämäärien saavuttamiseksi. Organisaatioita kehotetaan myös tarpeen ilmetessä suunnittelemaan omia kategorioitaan ja alakategorioitaan omakohtaisten riskien ilmetessä. NIST kehottaa suunnittelemaan tavoiteprofiilin vastaamaan jonkin tavoitetason kriteereitä.

Myös viitekehysprofiilit ovat selkeästi työkaluja, joita organisaation ulkopuolisen tahon on mahdotonta laatia ilman täsmällistä ja korkeaa luottamusta vaativaa selvitystä. Näin ollen myöskään viitekehysprofiileja ei voida käyttää datahubin tietoturvavaatimusten määrittelyssä.

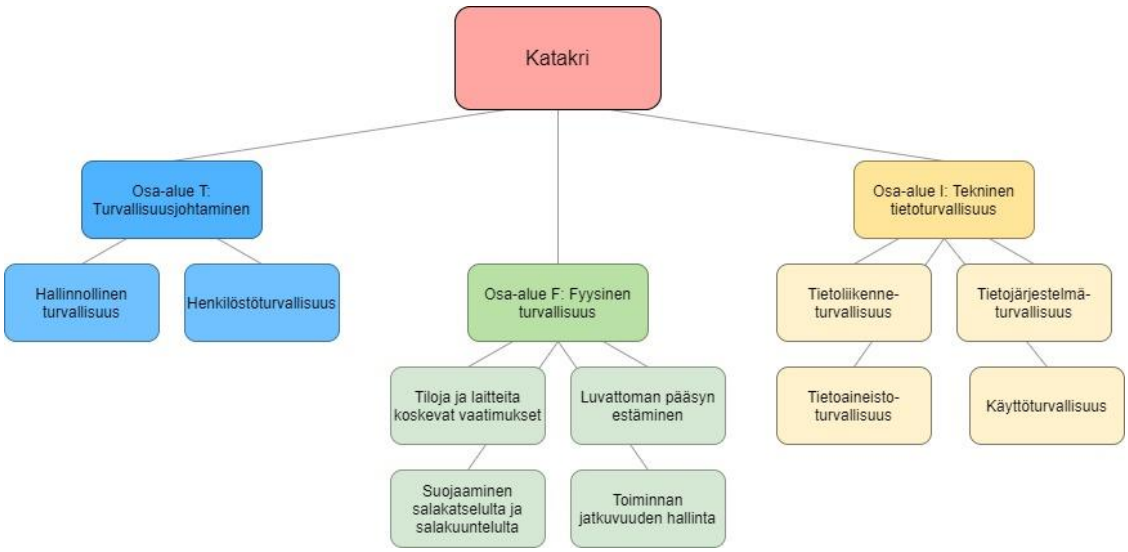
5.3.2 Katakri

Katakri on suomalainen viranomaisten käyttöön suunniteltu tietoturvallisuuden auditointityökalu [55][90][103][105]. Se perustuu vuonna 2009 julkaistuun samannimiseen kriteeristöön, jonka puolustusministeriö loi osana Suomen hallituksen sisäisen turvallisuuden ohjelmaa. Vuonna 2011 Katakristä julkaistiin päivitetty versio sisäministeriön suunnittelemana, jonka jälkeen se määrättiin jatkohallinnoitavaksi ulkoministeriön alaiselle Kansalliselle turvallisuusviranomaiselle (NSA, englannin sanoista National Security Authority). NSA julkaisi vuonna 2015 täysin uudistetun auditointityökalun, tässä työssä käsiteltävän Katakrin, joka peri edeltäjänsä nimen termin vakiintumisen vuoksi viranomaisten keskuudessa.

Katakri antaa yläkategorioihin luokiteltuja vaatimuksia, joihin vedoten auditoijan tulisi arvioida "kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa" [55]. Vaatimukset perustuvat valtioneuvoston asetukseen tietoturvallisuudesta, sekä Suomea sitoviin EU:n neuvoston turvallisuussääntöihin [106][107]. Osa ohjeistuksista on avoimia ja monitulkintaisia (esimerkiksi kohta T03: "Organisaatiolla on käytössään riittävä asiantuntemus tietoturvallisuuden varmistamiseksi." [55, s. 7]). Toiset ohjeistuksista tarjoavat spesifimpiä kriteerejä (esimerkiksi kohta T04, toteutusesimerkki 3: "Suojattaville kohteille on nimetty omistaja/vastuuhenkilö" [55, s. 8]). Joka tapauksessa materiaalin laajuudestaan huolimatta Katakrin tekijät nostavat esille sen olevan enimmäkseen suuntaa-antava työkalu, jota tulisi soveltaa tilannekohtaisen, tarkan riskianalyysin tukena [55]. Kuten NIST:n viitekehyksen toimintojen alakategorioita, Katakrin suuntaa-antavia ohjeistuksia voidaan kuitenkin käyttää pohjana eri tietoturvavaatimusten laatimiselle niin kauan, kun niitä kyetään soveltamaan tapauskohtaisesti.

Useat Viestintäviraston hyväksymät tietoturvallisuuden arviointilaitokset käyttävät Katakria yhtenä keskeisenä auditointityökalunaan [108]. Koska työkalu pohjautuu useampaan päivitykseen, voidaan sen vaatimusten myös olettaa pohjautuvan käytännön kokemuksen kautta esiin tulleisiin haasteisiin antaen sille meriittiä testattuna työkaluna [55]. On myös huomionarvoista, että sen vaatimukset on johdettu voimassa olevista kansallisista ja kansainvälisistä lakiasetuksista [55][106][107]. Tätä työtä varten haastatellut asiantuntijat mieltävät sen kuitenkin kokonaisuudessaan niin laajaksi kokoelmaksi ohjeistuksia, ettei ole realistista olettaa niiden kaikkien toteutuvan datahubiin liittyvien markkinaosapuolten kohdalla [90][103][105]. Ensinnäkin Fingrid Datahubilla ei ole tarvetta ottaa kantaa kaikkiin Katakrin asettamiin tietoturvavaatimuksiin, kuten useisiin fyysisin turvallisuusvaatimuksiin. Toiseksi, useat vaatimuksista ovat niin yksityiskohtaisia, että niitä ei ole tarkoituksenmukaista vaatia sellaisenaan laajalta joukolta erilaisia toimijoita. Työtä varten haastateltujen tietoturva-asiantuntijoiden mukaan Katakri kuitenkin tarjoaa huomionarvoista materiaalia datahubin tietoturvavaatimuksia varten. Seuraavissa alakohdissa kuva-

taan Katakrin kolmen osa-alueen rakenne pääosin sekä niiden rooli sovellettaessa Katakritä tämän työn tavoitteita varten. Kuvassa 3 on esitetty hahmotelma Katakrin rakenteesta.



Kuva 3. Katakrin rakenne [55].

Osa-alue T: Turvallisuusjohtaminen

Katakrin turvallisuusjohtamisen osa-alue käsittelee sellaisia käytäntöjä, joilla tietoturvallisuutta harjoitetaan organisaation hallinnollisin keinoin [55]. Osa-alueen vaatimukset on jaettu kahteen kategoriaan: hallinnolliseen ja henkilöstöturvallisuuteen. Kategorioiden vaatimukset käsittävät niin johtamisen, roolien jaon, koulutuksen kuin muut henkilökuntaa ohjaavat linjaukset. Katakrin tekijät painottavat, että osa-alueen menettelyjen täytäntöönpanon on pohjauduttava riskiarvioon, jossa riskialttiit alueet ja tiedot tunnistetaan tarkasti. Tätä tulisi seurata kohdentaminen, jolla osa menettelyistä voidaan rajata esimerkiksi koskemaan tietojenkäsittely-ympäristöä hallinnoiva organisaation osa. Tämän työn kannalta nähdään, että menetelmien kohdentaminen tapahtuu datahubin käyttöä hallinnoiviin osiin liittyjäorganisaatioissa silloin kuin tarkka kohdentaminen on mielekästä ja riittävää.

Osa-alue F: Fyysinen turvallisuus

Osa-alue F kuvaa niitä menetelmiä, joilla kohdeorganisaatio turvaa fyysisesti salassa pidettävää tietoaineistoaan [55]. Tämä käsittää myös sellaisten tilojen ja laitteiden suojaamisen, joissa kyseenolevaa tietoa käsitellään tai säilötään. Osa-alue jaetaan tiloja ja laitteita koskeviin vaatimuksiin, luvattoman pääsyn estämiseen, suojaamiseen salakatselulta ja salakuuntelulta sekä toiminnan jatkuvuuden hallintaan. Esitettyjä vaatimuksia ovat esimerkiksi monitasoisen suojaamisen periaatteiden käyttö, missä tilat esimerkiksi muodostavat keskenään sisäkkäisiä vyöhykkeitä sisempien vyöhykkeiden ollessa kriittisempiä ja paremmin turvattuja. Vaatimuksissa käsitellään myös erilaista fyysistä turvavälineistöä, kuten turvakaappeja, kameravalvontajärjestelmiä ja murtohälytysjärjestelmiä. Kuten edellä mainittiin, Fingrid Datahubilla ei ole tarvetta puuttua muun muassa tämän kaltaisiin hallintakeinoihin [90][109]. Puuttuminen liian yksityiskohtaisella tasolla osapuolten toimintaan ei ole käytännöllistä edellä mainitun osapuolten erilaisuuden vuoksi. Markkinaosapuolet saattavat erota erityisesti fyysisiltä kontrolleiltaan hyvin eri tavoin, vaikka hallintakeinoja voitaisiin pitää niiden asemaan nähden tietoturvallisina. Tämän vuoksi Katakrin osa-alue F tullaan sivuuttamaan täysin tässä työssä.

Osa-alue I: Tekninen tietoturvallisuus
Teknisen tietoturvallisuuden osa-alue käsittelee niitä turvallisuuskäytäntöjä, jotka liittyvät tiedon suojaamiseen digitaalisissa käyttöympäristöissä [55]. Se jakautuu edelleen neljään alakategoriaan, tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuteen. Tämä kattaa suuren joukon salaamisen ja suojauksen teknisiin ratkaisuihin liittyviä vaatimuksia, mutta myös jonkun verran tietotallenteiden fyysistä käsittelyä. Esimerkkejä viimeisestä ovat muun muassa tallennetun tiedon fyysinen kuljettaminen esimerkiksi kirjekuoria käyttäen sekä hävitettävien tallennuslaitteiden ja paperiaineistojen maksimisilppukoon määrittäminen. Osa-alue asettaa myös rajoja esimerkiksi ohjelmistotoimittajien kanssa toimimiselle.

Erityisesti teknisen tietoturvallisuuden osa-alue sisältää kirjavan joukon erilaisia vaatimuksia, joihin on suhtauduttava tapauskohtaisesti [55]. Aiemmassa osiossa toistettiin jo Fingrid Datahubin riskiarvion kanta fyysisiin kontrollikeinoihin puuttumisiin [90][109]. Monet vaatimuksista saattavat vaatia kohdeorganisaatioilta myös lisäinvestointeja joiden edellyttämistä pyritään välttämään. Esimerkiksi kohta I04: "Tietojenkäsittely-ympäristön suojattu yhteenliittäminen - Hallintayhteydet" asettaa vaatimukseksi seuraavan: "Hallintayhteydet on rajattu suojaustasoittain, ellei käytössä ole viranomaisen ko. suojaustasoille hyväksymää yhdyskäytäväratkaisua" [55, sivu 35]. On hyvin mahdollista, että monet osapuolet eivät toteuta tällaisia käytäntöjä, mutta samaan aikaan omaavat riittävän tietoturvan datahubin kannalta. Osa-alue kuitenkin sisältää viitteitä joistakin teknisistä ratkaisuista, jotka nähdään datahubin kannalta jossain määrin välttämättömiksi. Näin ollen tätä aluetta tullaan soveltamaan tietoturvavaatimuksissa turvallisuusjohtamisen osa-alueen lisäksi. Useata vaatimusta on kuitenkin sovellettava tapauskohtaisesti.

5.3.3 ISO/IEC 27000 -sarjan standardit

ISO/IEC 27000 -sarja on ISO ja IEC -järjestöjen kokoama kansainvälinen standardiperhe [56][57][110]. Kummatkin järjestöt harjoittavat maailmanlaajuista standardointitoimintaa yhdessä useiden kansallisten jäsenjärjestöjensä kanssa. Tämän työn teon aikana ISO:lla on jäsenenä 164 kansallista standardointijärjestöä. IEC:llä vastaava luku on 88. Osa näistä jäsenistä kuuluu kumpaankin järjestöön. Standardit 27000 -sarjassa kokoavat yhteen edellä mainittujen järjestöjen parhaaksi näkemät käytännöt tietoturvallisuuden hallinnasta, riskeistä ja kontrolleista. Sarjaan kuuluu useita eri standardeja, jotka käsittelevät tietoturvallisuuden eri osa-alueita. Standardit eivät ole julkisesti saatavilla vaan maksullisia. Tässä työssä on käytetty Fingridin omistamia standardeja ISO/IEC 27001:2017 ja ISO/IEC 27002:2017 [56][57]. Ensimmäinen standardeista käsittelee tietoturvallisuuden hallintajärjestelmiä, seuraava taas tietoturvakontrollien käytäntöjä. Kummatkin standardeista ovat Euroopan standardointikomitea CEN:n (Comité Européen de Normalisation) virallisesti hyväksymiä eurooppalaisia standardeja.

Standardeissa olevien tietoturvakäytäntöjen puolesta puhuu kansainvälisten tahojen määrä, joka niitä on auttanut suunnittelemaan [56][57]. Lisäksi standardeista on useita versioita, jotka viestivät kokemuksen kautta tehdyistä parannuksista. Kuten aiemmin esitettiin, edellä mainittuja standardeja on siis hyödynnetty käytännössä ja paranneltu saadun kokemuksen mukaan toisin kuin aiemmin mainittujen akateemisten tutkijoiden suunnittelemia viitekehyksiä. Tutkimalla muuta viitekirjallisuutta voidaan myös nähdä, että standardit tunnistetaan hyviksi käytännöiksi myös ISO:sta ja IEC:stä riippumattomista organisaatioista. Esimerkiksi NIST:n viitekehys sekä Katakri kummatkin viittaavat useisiin kohtiin edellä mainittujen standardien vanhempiin versioihin kuvatessaan omia hyväksi todettuja käytäntöjään tai vaatimuksiaan [54][55].

Tässä työssä standardeja itseään analysoitiin tämän työn haastatteluissa siitä näkökulmasta voisiko niiden täyttäminen olla tarpeeksi tyydyttävä tietoturvan taso datahubiin liittyville markkinaosapuolille [90][103]. Lopputuloksena kuitenkin nähtiin, että standardien velvoittaminen liittyviltä osapuolilta olisi liian raskas sijoitus joillekin markkinoiden osapuolista. Standardit kuitenkin tarjoavat hyviä viitteitä tilannespesifien tietoturvakäytäntöjen suunnittelussa [105]. Täten kuten NIST:n viitekehyksen ja Katakrin kohdalla, ISO/IEC 27001:2017 ja ISO/IEC 27002:2017 -standardeissa hyväksi todettuja käytäntöjä tullaan käyttämään viitteenä työn lopputuloksena määriteltävissä tietoturvavaatimuksissa.

Toisin kuin NIST:n viitekehys ja Katakri, standardit eivät omaa selkeää helposti kuvattavaa rakennetta [57][110]. Sen sijaan niiden ohjeistukset on jaoteltu useampien eri otsikoiden alle. Ohjeistukset muodostavat varsin yksityiskohtaisia odotuksia organisaatioille, joita näiden tulisi täyttää. Toisin kuin esimerkiksi Katakrin kohdalla ohjeistuksia ei ole asetettu muutamaan tarkkaan kategoriaan, vaan parhaimmillaankin useaan määrään yksityiskohtaisten erojen mukaan jaoteltuja luokkia. Näin ollen toisin kuin edellä mainittujen työkalujen kohdalla, näiden standardien rakennetta ei koeta hyödylliseksi kuvata tarkemmin.

5.3.4 Yhteenveto asiantuntijaorganisaatioiden työkaluista

Jokaisen edellä tarkastellun työkalun kohdalla nähdään monia vahvuuksia, jotka tukevat niiden käyttöä määriteltäessä datahubiin liittymiseen velvoitettavia tietoturvavaatimuksia. Kaikkien kohdalla vahvuuksia ovat muun muassa niiden käytettävyys Suomessa ja kansainvälisesti. Käytettävyyttä pidetään vahvuutena aiemmin esitettyjen perusteluiden vuoksi, jotka koskivat käytännön kokemuksen tuomaa luotettavuutta. Jos jotkin käytännöt ovat olleet käytössä pitkään ja laajalti, voidaan niiden vahvasti olettaa olevan myös toimivia. Tätä tukevat myös eri tietoturva-alan asiantuntijoiden näkemykset tarkastelluista työkaluista [90][103][105]. Lisäksi edellä esitetyt työkalut altistetaan päivitettävyydelle saadun palautteen perusteella, joka ohjaa niiden kehitystä tietoturva-alan kehittyessä.

Näiden vahvuuksien valossa jokaista tarkasteltua työkalua tullaan hyödyntämään tämän työn lopputuloksen muodostamisessa. Kaikkia osia työkaluista ei kuitenkaan voida hyödyntää, kuten edellä olevissa tarkasteluissa mainittiin. On myös huomioitava, että työkalujen antamat kontrollit ovat suureksi osaksi yleisesti hyväksi koettuja käytäntöjä. Kuten tämän luvun alussa todettiin, nämä muodostavat tärkeän osan tietoturvaa. Joka tapauksessa osaa tietoturvavaatimuksista on sovellettava, jotta ne vastaisivat täsmällisesti nimenomaan datahubin tarpeita. Näin ollen työkaluissa esitettyjä kontrolleja ja menettelytapoja tullaan soveltamaan tarpeen mukaan. Sellaisissa tilanteissa, joissa niitä on sovellettu, on lähteisiin viitattu asianmukaisesti.

6 Datahubiin liittymiseen vaadittava tietoturva

Tässä luvussa esitellään työn lopputuloksena luotu viitekehys, jolla voidaan lähestyä datahubiin liittyville osapuolille määrättäviä tietoturvavaatimuksia. Viitekehys koostuu omista esimerkkivaatimuksistaan, jotka on jaettu neljään eri kategoriaan: suunnitteluun, teknisiin kontrolleihin, reagointiin ja henkilöstöön. Jokaisen kategorian vaatimus on muodostettu perusteluineen, lähteineen sekä täsmennyksineen. Täsmennysten tehtävänä on toimia vaatimuksen soveltamista yksityiskohtaisemmin ajavina osavaatimuksina, jotka Fingrid Datahubin palvelusopimuksen laativa ryhmä voi huomioida, muokata tai sivuuttaa oman näkemyksensä mukaan. Viitekehys on muodostettu seuraavaksi esitettävien perusteiden mukaan.

Luvussa 2 ja 3 keskusteltiin datahubiin liittyvien osapuolten erovaisuuksista niin liiketoiminnan kuin resurssikapasiteettien kannalta. Toisaalta luvussa neljä nostettiin esille tietoturvauhkien vakavuus ja todettiin, kuinka arvaamattomia mahdollisten hyökkääjien kohteet, motiivit ja menettelytavat voivat olla. Datahubiin liittyville osapuolille asetettaville tietoturvavaatimuksille on selkeä tarve. Kuitenkin sähkön vähittäismarkkinoiden osapuolten erilaiset mahdollisuudet tietoturvan toteuttamiseen ovat olleet kantava teema muun muassa kaikissa tämän työn aikana suoritetuissa asiantuntijahaastatteluissa [38][65][90][101][111][112]. Haastatteluiden ja analyysien lopputuloksena nähdään, että osapuolet eivät ainoastaan omaa erilaisia resursseja tietoturvan toteuttamiseen, vaan joissakin tilanteissa ne myös tuntevat omat haavoittuvuutensa ja mahdollisuutensa suojautua paremmin kuin Fingrid Datahub.

Näin ollen tässä luvussa esitettävä viitekehys painottaa teknologianeutraaleja ylätason tavoitteita, joiden tarkempi toteuttaminen on osapuolen omissa käsissä. Viitekehyksen muodostavat vaatimukset on pyritty asettamaan niin, että osapuolille tulee selkeäksi kontrollien tavoitteet pikemminkin kuin miten päästä niihin. Tällä menettelyllä pyritään siihen, että osapuolet kykenevät toteuttamaan itse omiin toimintoihinsa ja resursseihinsa parhaiten sopivat käytännöt sen sijaan, että Fingrid Datahub olettaisi tietävänsä ne.

6.1 Metodi viitekehyksen muodostamisen takana

Viitekehyksen muodostamat vaatimukset on muodostettu seuraavasti. Ensimmäiseksi luvussa kuusi esitetystä lähdekirjallisuudesta on koetettu valita oikeanlaiset kontrollit datahubiin liittyviä markkinaosapuolia varten. Tätä varten on sovellettu myös erilaisia asiantuntijahaastatteluja. Kontrollien valinnoissa on pyritty vastaamaan datahubin tarpeita Fingrid Datahubin projektidokumentaation sekä osittain edellä mainittujen asiantuntijahaastattelujen mukaan. Datahubin järjestelmäkohtaisia tietoturvavaatimuksia suunniteltaessa on painotettu niiden asiantuntijoiden mielipiteitä, jotka ovat tutustuneet enemmän projektin tarpeisiin ja järjestelmän toimintatapaan. Ensimmäisen vedoksen jälkeen viitekehys on jälleen luovutettu arvioitavaksi viimeksi mainituille, datahubin paremmin tunteville asiantuntijaryhmille. Tämän jälkeen viitekehystä on muokattu asiantuntijaryhmiltä saadun palautteen pohjalta. Lopuksi tätä tarkastelun ja palautteen sykliä on jatkettu niin kauan, että on löydetty asianmukainen konsensus viitekehyksen rakenteesta. Näin on pyritty takaamaan luvussa 5 mainittujen yleisesti hyvien tietoturvakäytäntöjen sekä kohdejärjestelmän erityispiirteiden vaatimien toimenpiteiden riittävä sisällyttäminen malliin.

6.2 Viitekehys ja sen käyttö kokonaisuutena

Vaatimukset, joista viitekehys koostuu, määrittävät kokonaisuuden, jonka on tarkoitus toimia jatkuvana osapuolia ja datahubia suojelevana lähestymistapana. Kokonaisuus voidaan kuvata ylätasolla seuraavanlaisena prosessina:

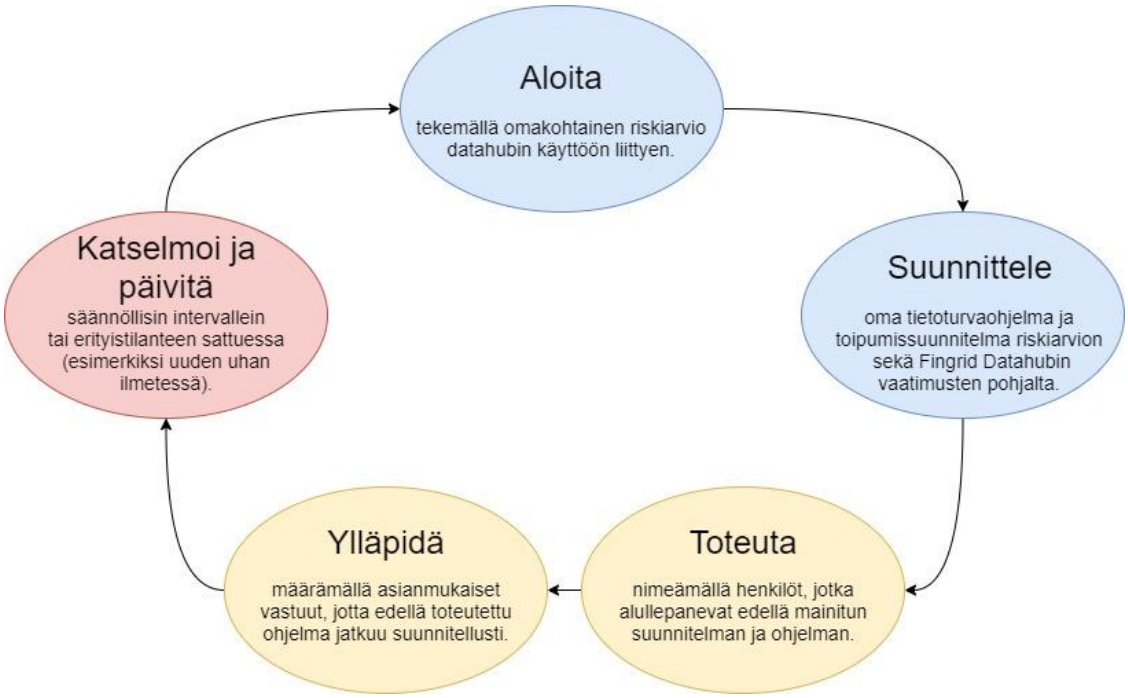
- Liittyjäosapuoli suorittaa omakohtaisen riskiarvionsa olettaen tilanteen, että se on ottanut jo datahub-järjestelmän käyttöön.

- Riskiarviossa esiin nousseiden riskien pohjalta on luotava omakohtainen tietoturvaohjelma sekä toipumissuunnitelma sitä varten, että liittyjäosapuolen datahub-yhteys joudutaan sulkemaan. Tietoturvaohjelman on otettava huomioon kaikki viitekehyksessä erikseen mainitut kontrollit osapuolen omien riskinhallintaprosessien lisäksi.

- Liittyjäosapuolen johto ymmärtää ja hyväksyy edellä määritellyn riskiarvion, tietoturvasuunnitelman ja toipumissuunnitelman. Osapuolen johto nimeää asianmukaisen henkilöstön toteuttamaan ja ylläpitämään hyväksyttyä tietoturvasuunnitelmaa viitekehyksen vaatimusten mukaisesti.

- Joko ennalta määritetyn aikajakson umpeutuessa tai sellaisen tilanteen sattuessa, jossa riskiarvion nykytilaa voidaan pitää vanhentuneena (esimerkiksi odottamattoman tietoturvaloukkauksen sattuessa), riskiarvio tarkistetaan ja tarvittaessa päivitetään. Jos riskiarvio päivitetään, edellä kuvattu prosessi alkaa alusta tietoturvasuunnitelman ja toipumissuunnitelman päivityksellä.

Yllä kuvattu prosessi on hahmoteltu Kuvassa 4.



Kuva 4. Viitekehyksen tarkoituksenmukainen käyttö.

6.3 Viitekehyksen muodostamat tietoturvavaatimukset

Taulukossa 4 on esitetty lista kaikista vaatimuksista ylätasolla. Tämän jälkeen jokainen vaatimus esitellään yksityiskohtaisemmin Taulukoissa 5-18.

Taulukko 4. Datahubin osapuolille asetettavat vaatimukset.

Suunnittelu
Vaatimus 1: Markkinaosapuolen on toteutettava sisäinen riskiarvio roolistaan datahubin käyttäjänä sekä datahubiin liittyvästä tietoturvastaan.
Vaatimus 2: Riskiarvion pohjalta on luotava tietoturvaohjelma.
Vaatimus 3: Riskiarvion pohjalta on luotava erikseen erityinen toipumissuunnitelma sille tilanteelle, että osapuoli joudutaan kytkemään irti datahubista.
Tekniset kontrollit
Vaatimus 4: Ne järjestelmät, jotka luovat datahubiin tietosisältöä tai hakevat tietoa datahubista, sekä kaikki yhteydet niihin ja niistä pois päin, on suojattava.
Vaatimus 5: Kaikki tieto, joka tulee muodostamaan datahubiin välitettävän tietosisällön, on suojattava asianmukaisin keinoin.
Vaatimus 6: Kaikki datahubista vastaanotettu tieto on suojattava asianmukaisin keinoin.
Vaatimus 7: Markkinaosapuoli ei saa missään tapauksessa luovuttaa datahubiin tunnistautumiseen käytettävää sertifikaattiaan toisen organisaation järjestelmiin.
Reagointi
Vaatimus 8: Sellaisen tietoturvahaavoittuvuuden ilmetessä, joka liittyy datahubin käyttöön, markkinaosapuolen on viipymättä raportoitava datahubille.
Vaatimus 9: Tietoturvaloukkauksen ilmetessä markkinaosapuolen on viipymättä raportoitava datahubille.
Vaatimus 10: Markkinaosapuoli hyväksyy sen, että Fingrid Datahubin valtuutettu henkilökunta on oikeutettu estämään osapuolen yhteys datahubiin päin.
Henkilöstö
Vaatimus 11: Markkinaosapuolen johdon on otettava ylin vastuu Fingrid Datahubin asettamien tietoturvavaatimusten toteutumisesta.
Vaatimus 12: Kaikkien datahubin käyttäjien sekä sen organisaation sisäiseen käyttöön oleellisesti liittyvien työntekijöiden on ymmärrettävä markkinaosapuolen tietoturvaohjelma asemansa velvoittamassa määrin.
Vaatimus 13: Markkinaosapuolen johdon on nimitettävä henkilö tai ryhmä, joka vastaa tietoturvaohjelman alullepanosta.
Vaatimus 14: Markkinaosapuolen johdon on nimettävä tietoturvaohjelman jatkuvuudesta, toimivuudesta sekä päivityksestä vastaava henkilö sekä vähintään yksi varahenkilö.

Taulukko 5. Vaatimus 1, täsmennykset ja perustelut.

Suunnittelu	**Vaatimus 1.** Markkinaosapuolen on toteutettava sisäinen riskiarvio roolistaan datahubin käyttäjänä sekä datahubiin liittyvästä tietoturvastaan.	Lähteet: [54: ID.BE-1 - 2, ID.BE-4 - 5, ID.GV-1, ID.GV-3, ID.RA-1, ID.RA-3 - 5, ID.RM-2 - 3, ID.SC-1 - 2, RS.MI-3][55: T04.5, T05.3][56: A.5.1.2, A.12.6.1, A.14.1.1, A.16.1.6, A.17.1.2,][57: 0.2, 14.1.1, 15.1.1, 15.2.2, 15.1.3, 16.1.6, 17.1.3, 18.2.1, 18.2.3][111][113][114]
	Täsmennyksiä Riskiarviossa on tunnistettava ainakin seuraavat alakohdat: 1. Mitkä tahot ovat riippuvaisia osapuolen toimivasta ja luotettavasta datahubin käytöstä ja miten? 2. Miten osapuolen oma liiketoiminta on riippuvainen toimivasta ja luotettavasta datahub-yhteydestä, sekä sen valtuuttamista kolmansista osapuolista datahubin käytössä? 3. Mitä teknisiä ja organisatorisia haavoittuvaisuuksia osapuolen organisaatiossa tulee olemaan datahubin käyttöönoton jälkeen niin, että kohdissa 1.1 ja 1.2 tunnistetut kohdat voivat joutua uhatuksi osapuolen tietoturvan vaarantuessa? Mitkä spesifit teknologiat ja palvelut sisältävät tai ovat osa näitä haavoittuvaisuuksia (esimerkiksi mitkä järjestelmät tuottavat tietoa datahubiin)? 4. Mitkä toimijat saattavat käyttää hyväksi kohdassa 1.3 todettuja haavoittuvaisuuksia ja miksi? 5. Mille uhille organisaatio sekä siitä riippuvat osapuolet altistuvat, jos osapuolen yhteys datahubiin joudutaan katkaisemaan. Uhkien arvioinnissa on otettava huomioon tilanteiden kehittyminen, jos osapuolen takaisinkytkentä datahubiin pitkittyy? Riskiarvio on dokumentoitava. Kaikki riskiarvioon tehdyt muutokset on dokumentoitava. Riskiarvio on katselmoitava ja tarvittaessa uusittava säännöllisesti, vähintään vuosittain. Riskiarvio on myös katselmoitava ja tarvittaessa päivitettävä jos: 1. Teknologiahankinnoissa tai organisaation toiminnoissa tapahtuu asiaa koskevia merkittäviä muutoksia, esimerkiksi alihankkijoiden tai tietoteknisten ratkaisujen vaihtuminen tai lisääntyminen. 2. Osapuoli joutuu odottamattoman tietoturvaloukkauksen uhriksi, tunnistettu tietoturvauhka ilmentyy odottamattomalla tavalla tai osoittautuu, että uhkaan liittyvä riski on arvioitu väärin. 3. Jos osapuoli vastaanottaa tietoa uusista asiaan kuuluvista haavoittuvaisuuksista esimerkiksi datahubilta tai osapuolen omilta järjestelmätoimittajilta.	

	Perustelut Osapuolikohtainen riskiarvio on kaikkien jälkeenpäin tulevien velvoitteiden lähtökohta. Tarkoituksena on saada osapuolet itse hahmottamaan oman tilanteensa riskitekijät niin, että ne voivat tehdä optimaalisia päätöksiä kaikkien hyväksi. Vaatimuksessa on nostettu esille joitakin aiheita, joita riskiarviossa tulisi vähintään käydä läpi. Tämä ei kuitenkaan tarkoita sitä, että riskiarvion tulisi perustua vain näihin vähimmäisvaatimuksiin. Vaikka Fingrid Datahub ei vaatisi dokumentaatiota kaikilta osapuolilta sopimuksenteon yhteydessä, voi olemassa olevasta dokumentaatiosta tai sen olemattomuudesta olla hyötyä tietoturvaloukkauksen sattuessa. Vaadittaessa osapuolta dokumentoimaan riskiarvioprosessinsa voidaan siitä vaatia näyttöä esimerkiksi tilanteessa, jossa osapuoli liittyy jatkuviin tietoturvaloukkauksiin ja sen valmistautumisen voidaan epäillä olevan puutteellista. Toisin sanoen, dokumentaatiolla varmistetaan todennettavuus mahdollisia tulevaisuuden tarpeita varten. On luonnollista, että olemassaolevat riskit sekä ymmärrys niistä kehittyvät useiden tapahtumien johdosta. Riskiarvio joka ei päivity varsinkaan vaatimuksessa eriteltyjen tapahtumien kohdalla menettää helposti arvonsa. Päivitettävyyden vaatiminen lisää myös todennettavuutta. Jos mahdollisessa dokumentaation katselmoinnissa huomataan, ettei osapuoli ole huomioinut joitakin tärkeitä elementtejä kehittyvässä uhkaympäristössään, on jatkotoimenpiteiden suunnittelu helpompaa.	

Taulukko 6. Vaatimus 2, täsmennykset ja perustelut.

Suunnittelu	**Vaatimus 2.** Riskiarvion pohjalta on luotava tietoturvaohjelma.	Lähteet: [54: ID.GV, ID.RA-6, ID.SC-1 - 2, PR.DS-4, PR.IP-1, PR.IP-7, PR.IP-9, PR.IP-12, RS.RP-1, RS.AN-4, RS.MI-1 - 2, RC.RP-1], [55: T04.1, T04.5 - 7, T05.1 - 2, T05.4, T06.1, I07, I20.1, I20.3][56: A.5.1.1, A.6.1.1, A.12.1.1, A.17.1.1 - 2][57: 5.1.1 - 2, 12.1.1, 14.1.1, 16.1.1, 17.1.1, 17.1.3, 18.2.1, 18.2.3]
	Täsmennyksiä Tietoturvaohjelma on kommunikoitava asianmukaiselle henkilökunnalle ja otetaan viimeistään käyttöön datahubin käyttöönoton yhteydessä. Tietoturvaohjelman on otettava kantaa kaikkiin riskiarviossa ilmeneviin riskeihin ja joko hyväksyttävä ne tai määriteltävä tarpeelliseksi nähdyt varotoimenpiteet (suojaus, vastaus ja palautuminen) perustellusti. Tietoturvaohjelman on kuvattava kaikki riskiarviossa tunnistettu suojattava omaisuus selkeästi asianmukaisina suojauskäytäntöineen. Tietoturvaohjelman on otettava huomioon henkilöstön rooli tietoturvan toteuttamisessa. Tietoturvaohjelman on sisällytettävä ja otettava huomioon tässä työssä esitettävien tietoturvavaatimusten kategorioiden "Tekniset kontrollit", "Reagointi" ja "Henkilöstö" sisältämät vaatimukset. Tietoturvaohjelma on dokumentoitava perusteluineen. Kaikki muutokset tietoturvaohjelmaan on dokumentoitava. Tietoturvaohjelma on tarkistettava ja tarvittaessa päivitettävä säännöllisesti, vähintään vuosittain. Tietoturvaohjelma on myös katselmoitava ja tarvittaessa päivitettävä jos: 1. Riskiarvio päivittyy, jolloin tietoturvaohjelma on katselmoitava ja tarvittaessa päivitettävä muuttuneen riskiarvion perusteella. 2. Jos tulee ilmi, että asetetut tietoturvakäytännöt eivät vastaa tavoiteltuja lopputuloksia. Tietoturvaohjelman voi toteuttaa osana laajempaa, mahdollisesti jo olemassa olevaa tietoturvasuunnitelmaa.	

	Perustelut Tämä vaatimus on riskiarvion luonnollinen jatke sekä jälkeenpäin tulevien tietoturvavaatimusten kriittinen, tukeva elementti. Fingrid Datahub ei juurikaan kykene vaatimaan spesifejä tietoturvakäytäntöjä, mutta se kykenee vaatimaan tavoitteita. Vaatiessa osapuolta luomaan oma tietoturvaohjelmansa aiemmin määritellyn riskiarvion pohjalta oletetaan, että osapuolet osaavat luoda asianmukaiset, itselleen parhaiten soveltuvat käytännöt. Tietoturvaohjelma on dokumentoitava samoista syistä kuin riskiarvio. Lisäksi, koska tietoturvaohjelman vaaditaan pohjautuvan riskiarvioon on luonnollista, että riskiarvion päivittyessä myös tietoturvasuunnitelma päivitetään. On myös otettava huomioon tilanne, missä riskiarvio itsessään ei muutu, mutta arvio riskien oikeanlaisesta hallinnasta muuttuu.	

Taulukko 7. Vaatimus 3, täsmennykset ja perustelut.

Suunnittelu	**Vaatimus 3.** Riskiarvion pohjalta on luotava erikseen erityinen toipumissuunnitelma sille tilanteelle, että osapuoli joudutaan kytkemään irti datahubista.	Lähteet: [54: ID.GV-3 - 4, ID.RM-1, ID.SC-1, PR.DS-4, PR.IP-9, PR.IP-12, RS.RP-1, RS.CO-4, RS.AN-2, RS.AN-4, RC.RP-1, RC.CO-3][55: T04.1, T04.7, T05.1 - 2, T06.1, I20.1, I20.3][56: A.12.1.1, A.17.1.1 - 2][57: 12.1.1, 14.1.1, 16.1.1, 17.1.1 - 3, 18.2.1, 18.2.3]
	Täsmennyksiä Suunnitelman on oltava riittävän kattava niin, että osapuoli pystyy jatkamaan liiketoimintaansa liittyviä velvollisuuksia myös datahub-yhteyden katkon aikana. Toipumissuunnitelman on kyettävä onnistumaan mahdollisimman tehokkaasti olettaen tilanteen pahimman mahdollisen kehityksen, josta markkinaosapuoli kykenee vielä toipumaan. Toipumissuunnitelman vaatimien käytäntöjen käynnistyessä osapuolen on kommunikoitava tilanteensa etenemisestä kaikille asianmukaisille tahoille perustuen sen riskiarvioissa ilmentyneisiin riippuvuussuhteisiin. Toipumissuunnitelma on dokumentoitava perusteluineen. Kaikki muutokset toipumissuunnitelmaan on dokumentoitava. Toipumissuunnitelma on tarkistettava ja tarvittaessa päivitettävä säännöllisesti, vähintään vuosittain. Toipumissuunnitelma on myös katselmoitava ja tarvittaessa päivitettävä jos: 1. Riskiarvio päivittyy, jolloin toipumissuunnitelma on katselmoitava ja tarvittaessa päivitettävä muuttuneen riskiarvion perusteella. 2. Jos tulee ilmi, että toipumissuunnitelma ei vastaa tavoiteltuja lopputuloksia.	

	Perustelut Yhteyden katkaisu datahubiin nähdään yhtenä sellaisena erityistilanteena, jossa osapuolen normaali toiminta tulee häiriytymään. Tämän vaatimuksen tarkoituksena on varmistaa, että osapuolet ymmärtävät tämän ja ovat valmistautuneet siihen asianmukaisin keinoin. Dokumentointi ja suunnitelman päivitettävyys noudattavat samoja perusteluja kuin tietoturvaohjelma.	

Taulukko 8. Vaatimus 4, täsmennykset ja perustelut.

Tekniset kontrollit	**Vaatimus 4.** Ne järjestelmät, jotka luovat datahubiin tietosisältöä tai hakevat tietoa datahubista, sekä kaikki yhteydet niihin ja niistä pois päin, on suojattava. ***Täsmennyksiä*** Vaatimuksessa kuvattuja järjestelmiä ovat kaikki organisaation omassa hallinnassaan olevat järjestelmät, joiden tieto kulkeutuu datahubiin tai jotka osallistuvat datahubin B2B-rajapintaan lähetettävien sanomien muodostamiseen. Vaatimuksessa kuvattuihin järjestelmiin tulee sallia kirjautuminen vain siten, että käyttäjän henkilöllisyys voidaan todentaa. Käyttäjätunnuksiin, joilla on mahdollista kirjautua vaatimuksessa kuvattuihin järjestelmiin, on sovellettava vähimpien oikeuksien periaatetta. Käyttäjätunnuksia, joilla on mahdollista kirjautua vaatimuksessa kuvattuihin järjestelmiin, on hallittava ja katselmoitava säännöllisesti. Vaatimuksessa kuvattujen järjestelmien valvontaan on kuuluttava ainakin: 1. Riittävät menettelyt turvallisuuteen liittyvien tapahtumien jäljitettävyyteen sekä poikkeamien ja haavoittuvuuksien havainnointikykyyn, esimerkiksi toteuttamalla asianmukainen lokitusjärjestelmä. 2. Valvontamenetelmien asianmukaisen aktiivinen käyttö niin, että tietoturvapoikkeamat ja mahdolliset haavoittuvuudet havaitaan ja selvitetään riskien minimoimiseksi. 3. Valvontamenetelmiin oleellisesti kuuluvien havaintojen tallennusjärjestelmien kuten lokituksen suojaus niin, että niiden sisältämän tiedon luvaton muuttaminen tai tuhoaminen estetään. Niiden palvelinten kellot, joissa vaatimuksessa kuvatut järjestelmät sijaitsevat, on synkronoitava noudattamaan samaa kellonaikaa.	Lähteet: [38][54: ID.AM-5, PR.AC-1, PR.AC-3 - 5, PR.AC-6 - 7, PR.PT-1, PR.PT-4 - 5, DE.AE-1 - 5, DE.CM-1, DE.CM-7, DE.DP-1 - 2, RS.AN-1 - 3, RS.AN-5, RS.MI-2][55: I07][56: A.9.1.2, A.9.4.2, A.12.2.1, A.12.4.1 - 2, A.12.4.4, A.13.1.1, A.16.1.4][57: 8.2.3, 9.1.1 - 2, 9.2, 9.3.1, 9.4.1 - 2, 12.2.1, 12.4.1 - 2, 12.4.4, 12.6.1, 13.1.1, 14.1.2 - 3, 16.1.7, 17.2.1][111][112][114][115]

	Perustelut Fingrid Datahub ei voi määrittää spesifisiä suojausasetuksia tai teknologiavaatimuksia datahubiin kytkeytyville tai siihen tietoa luoville järjestelmille. Vaadittaessa määriteltyjen järjestelmien suojaamista asianmukaisesti mutta teknologianeutraalisti osapuolten tulisi kyetä ratkaisemaan suojaus itselleen parhaaksi näkemällään tavalla. Osa-alueelle asetetaan tällaisia erityisvaatimuksia, koska se nähdään niin tärkeänä, että osapuolten tulisi kiinnittää siihen erityistä huomiota. Henkilöllisyyden todentamisen vaatiminen datahubin käytössä mahdollistaa paremman todennettavuuden sekä kasvattaa mahdollisuutta tehokkaampaan jälkiselvitykseen. Lisäksi, vaatimuksen nähdään olevan myös pienemmille osapuolille helposti toteutettavissa oleva passiivinen suojauskeino. Vaikka teknologianeutraaliutta vaalitaan, ilman asianmukaisia seurantamenetelmiä tietoturvaloukkausten selvittäminen voi olla mahdotonta. Menetelmissä on otettava myös huomioon sen asianmukainen järjestäminen niin, että siitä on hyötyä. Tähän kuuluvat muun muassa asianmukaisen kapasiteetin sekä tarpeeksi pitkän säilytysajan takaaminen. Valvottujen palvelimien kellojen synkronointi on myös yksi oleellinen tehokkaan valvonnan mahdollistava tekijä. Tällä varmistetaan muun muassa se, ettei eri palvelimilta haettujen lokitietojen tapahtuma-aikoja tarvitse laskea aikaero huomioon ottaen jotta päästäisiin selville tarkasta tapahtumien kulusta.	

Taulukko 9. Vaatimus 5, täsmennykset ja perustelut.

Tekniset kontrollit	***Vaatimus 5.*** Kaikki tieto, joka tulee muodostamaan datahubiin välitettävän tietosisällön, on suojattava asianmukaisin keinoin.	Lähteet: [54: PR.DS.1 - 3, PR.DS.5][56: A.8.2.3, A.13.1.1, A.13.2.3, A.14.1.2 - 3, A.18.1.3 - 4][57: 8.2.1, 8.2.3, 13.1.1, 13.2.1, 13.2.3, 14.1.2 - 3, 18.1.4]
	Täsmennyksiä Suojauksen on katettava tiedon säilytysaika, käsittely sekä sen liikkuminen syntyhetkestään datahubiin. Suojaus on toteutettava niin, että suojeltava tieto ei vuoda oikeudettomien osapuolten käsiin eikä datahubiin pääse oikeudettomasti muutettua tietoa.	
	Perustelut Datahubiin saapuvan tiedon muuttaminen ennen SOAP-sanoman lähetystä nähdään yhtenä uhkaskenaariona Fingrid Datahubin suorittamissa riskiarvioissa [33][34]. Fingrid Datahub ei voi myöskään vaatia tiedon allekirjoittamista ennen varsinaisen viestin luontia.	

Taulukko 10. Vaatimus 6, täsmennykset ja perustelut.

Tekniset kontrollit	**Vaatimus 6.** Kaikki datahubista vastaanotettu tieto on suojattava asianmukaisin keinoin.	Lähteet: [54: PR.DS.1-3, PR.DS-5][55: I03, I09, I10, I11][56: A.8.2.3, A.13.1.1, A.13.2.3, A.14.1.2 - 3, A.18.1.3 - 4][57: 8.2.1, 8.2.3, 13.1.1, 13.2.1, 13.2.3, 14.1.2 - 3, 18.1.4]
	Täsmennyksiä Suojauksen on katettava tieto sen aikaa, kun tieto kulkeutuu datahubista osapuolen järjestelmiin, tiedon säilytysaika, sekä tiedon käsittely. Suojaus on toteutettava niin, että suojeltava tieto ei vuoda oikeudettomien osapuolten käsiin eikä sitä muuteta oikeudettomasti.	
	Perustelut Datahubista haetun tiedon varastaminen on yksi uhkaskenaario joka on hahmotettu datahubin sisäisissä riskiarvioinneissa [25][26][27]. Vaikka lähtökohtaisesti osapuoli kykenee hakemaan vain itselleen kuuluvaa tietoa ja näin ollen omaa useampia velvoitteita suojella sitä (kuten yleisessä tietosuoja-asetuksessa ja tietosuojalaissa mainittavat vaatimukset [28][29]), Fingrid Datahub ei silti tiedon osittaissuojelijana voi sivuuttaa tätä kohtaa kokonaan. Tämänkin vaatimuksen tarkoituksena on saada osapuoli hahmottamaan vastuunsa myös tältä osin.	

Taulukko 11. Vaatimus 7, täsmennykset ja perustelut.

Tekniset kontrollit	**Vaatimus 7.** Markkinaosapuoli ei saa missään tapauksessa luovuttaa datahubiin tunnistautumiseen käytettävää sertifikaattiaan toisen organisaation järjestelmiin.	Lähteet: [38][57: 8.2.3][112] [113]
	Täsmennyksiä Kaikki osapuolen sertifikaatilla suoritetut toiminnot datahubissa tulkitaan osapuolen itsensä suorittamiksi riippumatta siitä, onko toiminnon suorittanut jonkin toisen tahon edustaja.	
	Perustelut Sitä mahdollisuutta, että osapuoli haluaa luovuttaa sertifikaattinsa tietyn alihankkijan käsittelyyn esimerkiksi tuotteen testausta varten tai toimenpiteen hoitamiseksi ilman valtuutusta ei voida poissulkea. Sertifikaatin luovuttamiselle ei nähdä mitään perusteita, vaikka se nähdäänkin mahdollisena. Näin ollen osapuolille on asetettava riittävä pelote ja vastuu mahdollisesta paljastuneesta väärinkäytöstä.	

Taulukko 12. Vaatimus 8, täsmennykset ja perustelut.

<table>
<tr><td rowspan="2">Reagointi</td><td>Vaatimus 8.
Sellaisen tietoturvahaavoittuvuuden ilmetessä, joka liittyy datahubin käyttöön, markkinaosapuolen on viipymättä raportoitava datahubille.</td><td rowspan="2">Lähteet:
[54: ID.BE-1 - 2, ID.BE-4 - 5, ID.RA-5 - 6, ID.RM-3, ID.SC-1 - 2, DE.AE-4, DE.DP-4, RS.CO-1 - 4, RS.AN-2 - 3, RS.AN-5, PR.IP-8][55: I23][56: A.6.1.3, A.12.6.1, A.16.1.2 - 3][57: 6.1.3, 12.6.1, 16.1.3]</td></tr>
<tr><td>Täsmennyksiä
Raportissa on oltava mahdollisimman tarkasti se tieto, mitä osapuoli osaa sanoa raportointihetkellä haavoittuvaisuudesta.

Jos osapuoli omaa tietoa haavoittuvuudelta suojautumisesta tai sen korjaamisesta, on myös tämä jaettava muun tiedon yhteydessä.

Ensisijaisen raportoinnin jälkeen osapuolen on tarvittaessa jatkettava haavoittuvuuden selvittämistä mahdollisimman tarkasti resurssiensa puitteissa sekä raportoitava kaikista uusista löydöksistä.

Jos haavoittuvuus liittyy kolmannen osapuolen järjestelmiin, on raportoitava myös saman käytännön mukaan järjestelmän kehittämisestä ja toimittamisesta vastaaville asianmukaisille tahoille, jotta haavoittuvuus pystytään korjaamaan ja sen asettama uhka voidaan hillitä mahdollisimman tehokkaasti.

Jos haavoittuvuus liittyy osapuolen itsensä kehittämiin ja hallinnoimiin järjestelmiin joita toiset osapuolet käyttävät, on datahubin lisäksi raportoitava samat tiedot kaikille käyttäjille, joille haavoittuvuudesta voisi koitua vahinkoa.

Jos haavoittuvuus liittyy osapuolen itsensä kehittämiin ja hallinnoimiin järjestelmiin joita toiset osapuolet käyttävät, haavoittuvuuden korjaamiseksi on tilanteen vakavuuden mukaisesti aloitettava asianmukaiset selvitys- ja korjaustyöt.</td></tr>
</table>

	Perustelut Tietoturvahaavoittuvuuksien tullessa ilmi on ehdottoman tärkeää jakaa mahdollisimman tarkka tieto eteenpäin sitä koskeville osapuolille [64]. Näin pyritään pienentämään sitä aikaikkunaa, jossa haavoittuvuuksia voitaisiin käyttää hyväksi, sekä estämään mahdolliset tietoturvaloukkaukset. Jos tiedossa on haavoittuvuuden torjuntaan soveltuvia menetelmiä, on nämä myös tärkeää jakaa samoista syistä. On myös huomioitava, että osapuolilla itsellään ei välttämättä ole täydellistä ymmärrystä haavoittuvuuden vakavuuksista raportointihetkellä. Näin välittömästi aloitettu, jatkuva koordinointi asianmukaisten tahojen kanssa nopeuttaa haavoittuvuudelta suojautumista sekä sen korjaamista. Toisaalta jos osapuoli itse on vastuussa sen järjestelmän kehittämisestä, jossa haavoittuvuus ilmenee, sen vastuu haavoittuvuuden korjaamisessa muuttuu luonnollisesti keskeisemmäksi. Tietoturvahaavoittuvuuksien oikeanlaiseen jakamiseen liittyvät myös omat turvallisuusnäkökulmansa [64]. On huomioitava, että haavoittuvuuksien jakamiseen tulisi mahdollisesti laatia omat tekniset menetelmät ja käytännöt. Tämän aiheen syvällisempi tutkiminen ei kuitenkaan kuulu tämän työn alueeseen.	

Taulukko 13. Vaatimus 9, täsmennykset ja perustelut.

Reagointi	**Vaatimus 9.** Tietoturvaloukkauksen ilmetessä markkinaosapuolen on viipymättä raportoitava datahubille.	Lähteet: [54: ID.BE-1 - 2, ID.BE-4 - 5, ID.RA-5 - 6, ID.RM-3, ID.SC-1 - 2, DE.AE-4, DE.DP-4, RS.AN-2 - 3][56: A.6.1.3, A.12.6.1, A.16.1.2 - 3][57: 6.1.3, 16.1.1 - 2, 16.1.4]
	Täsmennyksiä Poikkeuksena tilanteet, joissa voidaan aukottomasti todistaa, että tietoturvaloukkaus on tapahtunut niin, ettei se voi vaikuttaa osapuolen datahub-yhteyteen. Osapuolen on selvitettävä mahdollisimman tarkasti haavoittuvuuteen liittyvät yksityiskohdat. Ensisijaisen raportoinnin jälkeen osapuolen on tarvittaessa jatkettava haavoittuvuuden selvittämistä mahdollisimman tarkasti resurssiensa puitteissa sekä raportoitava kaikista uusista löydöksistä. Osapuolen tulee välittömästi arvioida loukkauksen vaikutus muihin osapuoliin datahubin kautta ja tiedottaa näille, jos voidaan nähdä, että tällaiset osapuolet saattavat kärsiä edes teoriassa tietoturvaloukkauksesta.	

	Perustelut Datahubin on saatava tietää mahdollisimman ajoissa tietoturvaloukkauksista, jotka saattavat vaikuttaa siihen tai joilta se kykenee suojelemaan muita datahubiin kytkeytyneitä osapuolia. Osapuolet eivät välttämättä hahmota tietoturvaloukkauksen vaikutuksia täysin, joten niillä on oltava aukottomat perusteet tiedon salaamiseksi datahubilta jos ne haluavat välttyä mahdollisilta sanktioilta. Kuten tietoturvahaavoittuvuuksien kanssa myös tietoturvaloukkausten kohdalla on tärkeää, että osapuolet ovat valmiita tarvittaessa koordinoimaan datahubin sekä muiden asiaa koskevien osapuolten kanssa mahdollisten vahinkojen tehokkaaksi torjumiseksi.	

Taulukko 14. Vaatimus 10, täsmennykset ja perustelut.

Reagointi	**Vaatimus 10.** Markkinaosapuoli hyväksyy sen, että Fingrid Datahubin valtuutettu henkilökunta on oikeutettu estämään osapuolen yhteys datahubiin päin.	Lähteet: [54: ID.BE, ID.GV-2 - 4, ID.RA-5 - 6, ID.RM-3, ID.SC-1, PR.AT-4 - 5, PR.DS-1 - 2, PR.DS-4 - 5, PR.PT-4 - 5, DE.AE-4, RS.AN-2, RS.MI-1 - 2] [56: A.16.1.7][57: 16.1.4 - 5, 16.1.7]
	Täsmennyksiä Yllä oleva pätee aina, jos osapuolen päässä ilmenee tietoturvaloukkaus, joka ei näy asian käsittelyhetkenä epätavallisena tietoliikenteenä datahubin suuntaan. Jos osapuolen päässä ilmenee tietoturvaloukkaus, joka ei näy asian käsittelyhetkenä epätavallisena tietoliikenteenä datahubin suuntaan, yllä oleva pätee, jos Fingrid Datahubin henkilökunta katsoo tietoturvaloukkauksen asettavan hyväksymättömän riskin datahubille. Jos osapuoli riitauttaa Fingrid Datahubin päätöksen katkaista yhteys argumentoiden, että tietoturvaloukkaus ei aseta riskejä datahubin turvallisuudelle, tulee osapuolen pystyä todistamaan väitteensä. Jos osapuoli ei kykene todistamaan, että tietoturvaloukkaus ei aseta riskejä datahubille, tai osapuolen esittämä aineisto ei tyydytä Fingrid Datahubin henkilökunnan esiin nostamia huolia, tilanteessa noudatetaan Fingrid Datahubin henkilökunnan arvioihin perustuvaa päätöstä.	
	Perustelut Osapuoli ei välttämättä ehdi itse havaita tietoturvaloukkausta ennen kuin se havaitaan datahubin päässä. Toisaalta vaikka tietoturvaloukkaus ei näkyisi vielä datahubin päässä, saattaa Fingrid Datahubin henkilökunta olla paremmin tietoinen loukkauksen aiheuttamista riskeistä datahubin suuntaan kuin osapuoli. Tällaisessa tilanteessa Fingrid Datahubilla tulee olla oikeus toimia ylimpänä auktoriteettina päätöksenteossa mahdollisten suurempien vahinkojen torjumiseksi. Osapuolen on luonnollisesti pystyttävä riitatilanteessa todistamaan oma kantansa oikeaksi. Tämän vaatimuksen toivotaan myös antavan osapuolille kannusteen sijoittaa seurantaan ja lokitukseen.	

Taulukko 15. Vaatimus 11, täsmennykset ja perustelut.

Henkilöstö	**Vaatimus 11.** Markkinaosapuolen johdon on otettava ylin vastuu Fingrid Datahubin asettamien tietoturvavaatimusten toteutumisesta.	Lähteet: [54: ID.AM-6, ID.GV-1 - 2, ID.RM-1, ID.SC-1, PR.AT-4, PR.IP-11][55: T01.1, T02][56: A.5.1.1, A.6.1.1, A.16.1.1][57: 5.1.1, 6.1.1, 7.2.1, 7.2.2, 14.1.1][111]
	Täsmennyksiä Johdon on ymmärrettävä ja hyväksyttävä riskiarvio, tietoturvaohjelma sekä toipumissuunnitelma. Johdon on otettava vastuu riskiarvion, tietoturvaohjelman ja toipumissuunnitelman kannalta asianmukaisten henkilöiden nimeämisestä ja varmistettava, että nämä osaavat ja pystyvät suorittamaan asiaankuuluvissa kohdissa määritellyt vastuut.	
	Perustelut Markkinaosapuolen johdon on luonnollisesti otettava vastuu muun henkilöstön toiminnasta. Lisäksi johdon on hyvä olla tietoinen vaatimuksista ja muun muassa varmistaa, että henkilöt kykenevät suorittamaan heille annetut velvollisuutensa.	

Taulukko 16. Vaatimus 12, täsmennykset ja perustelut.

Henkilöstö	**Vaatimus 12.** Kaikkien datahubin käyttäjien sekä sen organisaation sisäiseen käyttöön oleellisesti liittyvien työntekijöiden on ymmärrettävä markkinaosapuolen tietoturvaohjelma asemansa velvoittamassa määrin.	Lähteet: [54: ID.GV-1, PR.AT-1, PR.AT-5, PR.IP-11, RS.CO-1][55: T02, I22.2][56: A.6.1.1, A.7.2.1][57: 5.1.1, 6.1.1, 7.2.2, 14.1.1, 16.1.2]
	Täsmennyksiä Henkilökunnan on oltava tietoisia muutoksista tietoturvaohjelmaan niiden koskettaessa heidän työtehtäviään. Osapuolen on pidettävä huolta, että henkilökunta on tehtäviinsä nähden asianmukaisen tietoinen osapuolen tietoturvakäytännöistä.	
	Perustelut On olennaista, että kaikki datahubin tietoturvaa edistävä tai vaarantava henkilöstö ovat tietoisia osapuolikohtaisista tavoista suojata datahubiin liittyviä toimintoja. Asianmukaisen henkilökunnan on myös tärkeää osata ilmoittaa ilmenevistä tietoturvauhista tai -loukkauksista.	

Taulukko 17. Vaatimus 13, täsmennykset ja perustelut.

Henkilöstö	**Vaatimus 13.** Markkinaosapuolen johdon on nimitettävä henkilö tai ryhmä, joka vastaa tietoturvaohjelman alullepanosta.	Lähteet: [54: PR.AT-2, PR.AT-4, PR.AT-5, PR.IP-11][55: T02, I03.2][56: A.6.1.1, A.7.2.1, A.7.2.2, A.16.1.5][57: 6.1.1]
	Täsmennyksiä Kyseisen ryhmän tai henkilön on kannettava vastuu tietoturvakäytäntöjen riittävästä alulle panosta vielä tietoturvakäytäntöjen käyttöönoton jälkeenkin ja oltava tarvittaessa mukana niiden päivityksessä Kyseisen ryhmän tai henkilön on osattava perustella tietoturvakäytäntöjen toimeenpanossa tehdyt ratkaisut tätä vaadittaessa.	
	Perustelut On olennaista, että joku vastaa päätettyjen tietoturvakäytäntöjen toimeenpanosta niin, etteivät ne jää ainoastaan suunnitteluasteelle. Lisäksi kyseisiä henkilöitä saatetaan tarvita perustelemaan tehtyjä päätöksiään katselmointitilanteissa tai tietoturvaohjelmaa kehitettäessä. Näin varmistetaan aiemmin tehtyjen päätösten ja huomioiden ymmärrettävyys sen hetkisessä kontekstissa.	

Taulukko 18. Vaatimus 14, täsmennykset ja perustelut.

Henkilöstö	**Vaatimus 14.** Markkinaosapuolen johdon on nimettävä tietoturvaohjelman jatkuvuudesta, toimivuudesta sekä päivityksestä vastaava henkilö sekä vähintään yksi varahenkilö.	Lähteet: [44][54: ID.AM-3, ID.GV-2, PR.AT-2, PR.AT-4, PR.AT-5, PR.IP-11, RS.CO-1][55: T02, T03, T06.2 I03.2][56: A.6.1.1, A.6.1.3, A.7.2.1, A.7.3.1, A.12.6.1, A.15.2.1, A.16.1.1 - 3][57: 5.1.1, 5.1.2, 6.1.1, 6.1.3, 12.1.2, 14.1.1, 16.1.1 - 2, 17.1.3,
	Täsmennyksiä Henkilöillä on oltava vähintään välittömät oikeudet sulkea/antaa lupa sulkea datahubin suuntaan kommunikoivat järjestelmät ilman erillistä lupaa muilta tahoilta. Henkilöiden on tunnettava riskiarvio, tietoturvaohjelma sekä toipumissuunnitelma niin, että he kykenevät suorittamaan tehtävänsä perustellusti ja ymmärtävät sen roolin laajemmassa kuvassa. Henkilöiden on oltava ryhmänä mahdollisimman suuren osan vuorokaudesta valmiina vastaanottamaan turvallisuushavainnot muualta organisaation datahubin kanssa suoraan tai epäsuorasti työskenteleviltä työntekijöiltä. Henkilöiden on vastattava turvallisuushavaintojen käsittelystä ja ulospäin kommunikoinnista asianmukaisilla tavoilla. Henkilöiden on vastattava riskiarvion, tietoturvaohjelman sekä toipumissuunnitelman tarkistamisesta ja tarvittaessa niiden päivityksestä.	

	Perustelut Vaikka asianmukaisiksi nähdyt tietoturvakäytännöt asetettaisiin alulle ei ole itsestään selvää, että tietoturvakäytäntöjen jatkuvaa noudattamista valvotaan. Lisäksi datahubin käytön aikana on oltava tarkasti määriteltynä henkilö, jolla on osaaminen ja vastuu tietoturvaloukkauksiin reagoimisesta tai reagoimisen koordinoinnista. On myös huomioitava, että Fingrid Datahubin mahdollisesti havaitessa osapuolen päästä epänormaalia toimintaa Fingrid Datahubilla saattaa olla tarve saada kiireellisesti ja viiveettä tarvittavaa tietoa osapuolen päästä. Pahimmassa tapauksessa datahubilla saattaa olla tarve osapuolen päässä olevien järjestelmien välittömään sammutukseen. Kriisitilanteissa tapahtuvan yhteistyön estyessä tai hankaloituessa mahdollinen hyökkäys saattaa ehtiä aiheuttamaan paljon raskaampaa vahinkoa.	18.2.1 - 3][116]

7 Osapuolten tietoturvan tason todentaminen

Kuten luvussa 6 sivuttiin, datahubiin liittyvien osapuolten tietoturvan tason todentamiseen ei nähdä tämän työn teon hetkellä järkeviä vaihtoehtoja [33][65][109]. Vaikka Fingrid Datahubilla onkin lainsäädännön velvoittama vastuu suojella datahubin tietoturvaa, asianmukaisesta tietoturvasta huolehtiminen tulee olemaan ensisijaisesti osapuolten vastuu. Analyyseissa useiden auditointimenetelmien nähdään nostavan kustannuksia Fingrid Datahubille sekä pidentävän projektin aikataulua. Suomen sähkön vähittäismarkkinat kattavat tämän työn teon aikana suurin piirtein 100 sähkön myyjää, 80 jakeluverkkoyhtiötä sekä tuntemattoman määrän kolmansia osapuolia [11]. Tämän kokoluokan kohderyhmää auditoitaessa ulkoistetusti voidaan turvallisesti arvioida kustannusten tulevan liian kalliiksi julkiselle projektille ja hankkeen osapuolille [33][65].

Työn aikana on myös analysoitu voisiko Fingrid Datahub todentaa tietoturvan toteutumista tehokkaasti ottamatta siitä liikaa vastuuta itselleen. Satunnaisesti suoritetut auditointiprosessit kuten pistokokeet olisivat teoriassa kustannustehokas tapa todentaa osapuolille asetettujen tietoturvavaatimusten täyttymistä [33]. Suorittamalla kokeita vain osaan kaikista sähkömarkkinoiden osapuolista voitaisiin välttyä suuremmilta kustannuksilta antamalla samalla osapuolille kannuste tietoturvavaatimusten täyttämiselle. Osapuolista vain osan auditoiminen voisi kuitenkin kyseenalaista toiminnan puolueettomuuden, vaikka pistokokeiden satunnaisuus voitaisiinkin taata [65][90]. On esimerkiksi mahdollista, että pistokokeissa huomattaisiin joidenkin markkinaosapuolten rikkovan asetettuja tietoturvavaatimuksia, mutta samalla saadaan tietää pistokokeisiin joutumattomien osapuolten tekevän samoin. Riitatilanne saattaa syntyä, jos vain pistokokeisiin joutuneet rikkurit saavat sanktioita toisin kuin muut epäilyksen alaiset osapuolet. Tällaisessa hypoteettisessa tilanteessa pistokokeet olisi siis joka tapauksessa ulotettava kaikille osapuolille, joka mitätöisi suunnitellut resurssisäästöt.

Sopivien tietoturvasertifikaattien suoritus, joilla osapuolet voisivat todistaa täyttävänsä jonkin hyväksi todetun kriteeristön standardit, olisi tapa, joka poistaisi auditointivastuun Fingrid Datahubilta. Kuten luvussa 5.3.3 kuitenkin selitettiin ISO/IEC 27000 -sarjan kohdalla tällaiset sertifikaatit nähdään liian suureksi rasitukseksi osapuolille itselleen [33][90]. Monien yleisesti hyväksi nähtyjen tietoturvasertifikaattien kokonaisvaatimusten täyttäminen nähdään kalliina prosessina. On mahdollista, että jotkin osapuolista omistaisivat sertifikaatteja, joilla ne voisivat osoittaa täyttävänsä datahubiin liittymiselle asetetut tietoturvavaatimukset. Jonkin tietyn sertifikaatin vaatiminen kaikilta liittyviltä osapuolilta asettaisi kuitenkin sellaiset osapuolet epäedulliseen asemaan, joilla tällaista sertifikaattia ei olisi. Sertifikaatin hankkimiseksi näiden osapuolten olisi käytettävä toisia osapuolia enemmän aikaa ja rahaa, vaikka niiden tietoturva olisikin todellisuudessa riittävä datahubia varten. Samalla saatettaisiin velvoittaa osapuolia käyttämään jonkin tietyn yrityksen palveluita. Puolueettomuus ei kuitenkaan kärsi silloin, kun vaaditaan tiettyä tietoturvan tasoa osapuolilta ja samalla annetaan niille vapaus täyttää annetut vaatimukset itselleen parhaaksi näkemällä tavalla.

Edellä mainituista syistä luvun 6 tietoturvavaatimukset on suunniteltu niin, että ne täyttäisivät erityisesti kaksi asiaa. Ensinnäkin tietoturvavaatimuksissa pyritään "todennettavuuteen" vaikka minkäänlaisia tietoturvatason todennustoimenpiteitä ei Fingrid Datahubin puolesta tällä hetkellä nähtäisi järkevänä [101][113]. Todennettavuudella tarkoitetaan tietoturvavaatimusten suunnittelemista niin, että tilanteen mahdollisesti salliessa osapuolen tietoturva olisi mahdollista esimerkiksi auditoida. Tällaisia asioita ovat esimerkiksi riskianalyysin, tietoturvaohjelman ja toipumissuunnitelman dokumentointivelvolli-

suus sekä asianmukaisen lokituksen vaatiminen. Sen lisäksi, että todennettavuudella pyritään säilyttämään mahdollisuus tietoturvan todentamiseen tulevaisuudessa, tämän menettelytavan toiveena on myös saada osapuolet ottamaan asetetut tietoturvavaatimukset vakavammin korvausvelvollisuuden näkökulmasta. Esimerkiksi tietoturvaloukkausten jälkiselvityksissä Fingrid Datahubilla saattaa olla perusteltu syy nähdä osapuolen edellä mainittu dokumentaatio ja lokitus. Toiveena on, että osapuolet ymmärtävät tällaisen tilanteen muun muassa nostavan niihin kohdistuvia taloudellisia riskejä entisestään. Jos jälkiselvityksissä esimerkiksi tulee ilmi, että vaatimuksissa vaadittua materiaalia ei ole saatavilla tai se on puutteellista, osapuolten on ymmärrettävä, että tilanteesta saattaa koitua seurauksia.

Todennettavuuden lisäksi lopputuloksena määritetyillä tietoturvavaatimuksilla pyritään osapuolten kannustamiseen omatoimisuuteen [113]. Vaatimalla osapuolia kokoamaan omakohtaiset riskianalyysinsa sekä riskienhallinta menetelmät datahubin käyttöä varten toivotaan, että osapuolet ymmärtäisivät itse asemansa suuremmassa ekosysteemissä. Loppujen lopuksi ainoastaan osapuoli itse on parhaassa mahdollisessa asemassa kartoittaakseen juuri sitä kohtaavat riskit sekä niihin sopivat asianmukaiset hallintamenetelmät. Paras mahdollinen tilanne olisi, että koko toimiala tulisi tietoisemmaksi tietoturvauhkien vakavuudesta, laajemmista ja odottamattomista vaikutuksista sekä miten suhtautua niihin käytännössä. Voidaan pitää todennäköisenä, että suuri osa markkinaosapuolista pyrkii täyttämään annettavat tietoturvavaatimukset minimimäärällä resursseja. Markkinaosapuolien kannustaminen parempaan tietoturvatietoisuuteen vähäiselläkin resurssien käytöllä on kuitenkin lähestymistapa, josta voi olla ainoastaan hyötyä [90][113]. Seuraavissa kappaleissa annetaan joitakin esimerkkejä siitä, miten osapuolet voivat omatoimisesti parantaa tietoturvaansa. Osaa menetelmistä on käsitelty jo luvussa 5.3.

Kuten luvussa 5.3.1 mainittiin, NIST:n viitekehys kriittisten infrastruktuurien kyberturvallisuuden kehittämiseen on pääasiassa organisaatioiden omatoimiseen tietoturvan kehitykseen tarkoitettu itsearviointityökalu [54]. Muun muassa monet Yhdysvaltojen yksityisen sektorin toimijat käyttävät viitekehystä rakentaakseen itselleen pidemmän tähtäimen tavoitteita sen mukaan mitä ne kokevat tarvitsevansa [101]. Niin kuin aiemmin mainittiin, tämän työn tietoturvavaatimuksia laadittaessa on käytetty viitekehyksen ydinosaa varsin laajasti [54]. Ydinosan alakategoriat sisältävät silti paljon hyväksi nähtyjä käytäntöjä, joita osapuolet voivat hyödyntää halutessaan parantaakseen tietoturvaansa. Yhdessä viitekehyksen profiilin luontiin tarkoitettujen ohjeiden sekä toteutustasojen kanssa todetaan asiantuntijoiden tukemana NIST:n viitekehyksen olevan eräs hyödyllinen työkalu kokonaisvaltaisemman tietoturvaohjelman kokoamiseksi itsenäiselle osapuolelle [33][101].

Luvussa 5.3.2 kuvattiin kansallinen turvallisuusauditointikriteeristö Katakri pääpirteiltään [55]. Luvussa todettiin myös, että Katakri soveltuu tässä työssä suoritettuun tietoturvavaatimusten määritykseen tarjoten viitteitä hyväksi todetuista tietoturvakäytännöistä. Katakrissa esiintyvien vaatimusten keskeisyyttä perusteltiin sen laajalla käytöllä eri tietoturva-asiantuntijoiden ja tahojen kesken sekä sen päivityshistorialla [33][55][90][105][108]. Samalla Katakri todettiin kokonaisuudessaan liiankin laajaksi kriteeristöksi, jotta datahubiin liittyvien osapuolten voisi odottaa täyttävän kaikki sen vaatimukset [33][90][105]. Kiinnostuneille osapuolille Katakri tarjoaa kuitenkin paljon esimerkkivaatimuksia, joita esimerkiksi turvallisuusselvityslain mukaisessa yritysturvallisuusselvityksessä tultaisiin auditoimaan [55][117].

Jotkin organisaatiot kuten Liikenne- ja viestintäviraston alainen Kyberturvallisuuskeskus välittävät ajantasalla olevaa tietoa erilaisista ajankohtaisista tietoturvauhista [118]. Käyttöön otettujen tietoturvakäytäntöjen tasosta huolimatta tällaisen informaation seuraaminen nähdään kaikille markkinaosapuolille hyvänä käytäntönä. Sen toteuttaminen ei tuota suuria investointikustannuksia, mutta sen noudattaminen on täysin organisatorisesta tietoturvakulttuurista tai työntekijöiden kiinnostuksesta kiinni. Ajankohtainen informaatio tietoturvauhista saattaa käsittää esimerkiksi haittaohjelman levitykseen tarkoitettuja sähköpostikampanjoita tai tietoa haavoittuvuuksista eri ohjelmistoissa. Vaikka ilmenneet uhat eivät suoraan liittyisi datahubin käyttöön osapuolen näkökulmasta, ne saattavat levitä muihin järjestelmiin yllättävästi tai haitata osapuolten liiketoimintaa muulla tavoin. Kyberturvallisuuskeskus on myös esimerkki tahosta, joka tarjoaa konsultaatiota tietoturvan arvioinnissa ja tietoturvaloukkausten selvityksissä [119]. Monet Kyberturvallisuuskeskuksen palveluista eivät kuitenkaan ole tarjolla kaikille datahubin markkinaosapuolille. Esimerkiksi tietoturvaneuvonta rajoitetaan vain valtionhallinnolle tai huoltovarmuuskriittisille toimijoille, joista jälkimmäiseen lukeutuvat jakeluverkkoyhtiöt, mutta esimerkiksi sähkönmyyjät eivät välttämättä.

8 Yhteenveto

Tämän työn tavoitteena on ollut selvittää tietoturvataso, joka vaaditaan datahubiin liittyviltä markkinaosapuolilta. Selvityksen tärkeys osoitettiin viittaamalla voimassa olevaan lainsäädäntöön, joka velvoittaa Fingrid Datahubin järjestämään datahubin tietoturva asianmukaiseksi. Lainsäädäntö ei kuitenkaan täsmennä, mitä tällä asianmukaisella tietoturvalla tarkoitetaan. Datahubin sisäisissä riskiarvioissa on todettu, että datahubiin liittyvät osapuolet aiheuttavat järjestelmälle tietoturvauhkia. Tämä johtaa siihen, että Fingrid Datahubin on asetettava järjestelmään liittyville osapuolille tietoturvavaatimuksia. Lisäksi muuta sähkön vähittäismarkkinoiden osapuolien tietoturvaa koskevaa lainsäädäntöä tarkasteltaessa huomattiin, ettei voimassa oleva lainsäädäntö määrää osapuolten tietoturvaa varmuudella riittäväksi datahubin turvallisuuden kannalta. Näin ollen osoitettiin, että Fingrid Datahubille on tarve asettaa itse tietoturvavaatimuksia datahubiin liittyville osapuolille.

Seuraavaksi työssä tehtiin riskiarvio datahubiin liittyvien osapuolten kohdistamista riskeistä järjestelmälle. Tämä tehtiin ensin tarkastelemalla sitä, millaisia datahubiin kytkeytyvät markkinaosapuolet tulevat olemaan sekä miten ne tulevat käyttämään sitä. Sen jälkeen tutkittiin tietoturvauhkia kirjallisuuden ja historiasta saatujen esimerkkien avulla. Nämä kaksi tarkastelua loivat pohjan suoritetulle riskiarviolle. Turvallisuussyistä riskiarvio suoritettiin Fingrid Datahubissa sisäisesti.

Riskiarvio ohjasi työn seuraavaan vaiheeseen eli kirjallisuustutkimukseen. Kirjallisuustutkimuksen tavoitteena oli selvittää yhdessä riskiarvion kanssa, millaisia hyviä käytäntöjä tietoturvavaatimusten asettamiseksi on ja mitä liittyviltä osapuolilta voidaan vaatia. Kirjallisuustutkimus tehtiin tutkimalla sellaista lähdeaineistoa, joka auttoi ymmärtämään, miten samankaltaisia ongelmia on lähestytty aiemmin. Lähdeaineisto koostui akateemisesta tutkimuksesta, suomalaisista referenssijärjestelmistä sekä eri asiantuntijaorganisaatioiden laatimista työkaluista.

Akateemisen tutkimuksen tarkastelussa huomio kiinnitettiin erityisesti sellaisiin tutkimuksiin, jotka koettivat löytää yleispäteviä malleja hyvän tietoturvan määrittämiseksi vähintään organisaatiotasolla. Tutkimuksia tarkastellessa huomattiin, että niiden tulokset ovat yleisesti liian epävarmoja tietoturvavaatimusten määritykseen käytännössä. Samalla kuitenkin todettiin, että jotkin tutkimuksista nostavat esiin varmemmin todennettavissa olevia huomioita, jotka voivat auttaa ohjaamaan tietoturvavaatimusten määritystä. Tarkastelussa huomattiin myös, että kaikki tutkitut yleispätevän tietoturvan muodostamiseen tarkoitettua mallia tavoitelleet ryhmät aloittivat tutkimuksensa asiantuntijahaastatteluilla. Tässä yhteydessä esitettiin väite, että kokeneet asiantuntijat saattavat toimia eräinä sellaisina lähteinä, joihin voi luottaa, sillä he omaavat käytännön työssä muodostuneita näkemyksiä hyvän tietoturvan muodostamisesta.

Referenssijärjestelminä työtä varten tarkasteltiin Kanta-palveluita, Nordea Web Servicesiä sekä Suomi.fi-palveluväylää. Referenssijärjestelmät valittiin sen perusteella, että kuten datahubilla jokaisella valitulla järjestelmällä on tarve asettaa tietoturvavaatimuksia niihin liittyville osapuolille. Referenssijärjestelmien tietoturvavaatimuksia tarkasteltiin pääasiassa tunnistautumistapoihin, lokitukseen ja seurantaan, palveluntarjoajalle luovutettaviin tietoihin sekä tietojen käsittelyyn liittyviltä vaatimuksilta. Tarkastelussa todettiin, että vaikka jokainen referenssijärjestelmä erosi toisistaan sekä datahubista tarpeissaan ja toiminnoissaan, referenssijärjestelmien tietoturvavaatimuksissa esiintyi silti yhtäläisyyksiä. Osa näistä yhtäläisyyksistä antoi lisäviitteitä sille, miten datahubiin liittyvien osapuolten tietoturvavaatimukset voitaisiin järjestää.

Asiatuntijaorganisaatioiden kehittämistä työkaluista tarkasteltiin NIST:n kriittisten infrastruktuurien kyberturvallisuuden kehittämiseen tarkoitettua viitekehystä, Katakriä sekä kahta ISO/IEC 27000-sarjan standardia. Jokainen työkaluista erosi hieman varsinaiselta käyttötarkoitukseltaan, mutta osoittautui keskeiseksi avuksi tämän työn lopputuloksena määritellyssä tietoturvavaatimusten viitekehyksessä. Tämä johtui siitä, että jokainen tarkastelluista työkaluista oli laajasti tunnettu hyvien tietoturvakäytäntöjen muodostamisen suhteen. Lisäksi niitä oli muokattu käytännön kokemuksen mukaan.

Lopuksi sisäisen riskiarvion, kirjallisuustutkimuksen sekä asiantuntijahaastatteluiden pohjalta luotiin työn lopputuloksena tavoiteltu tietoturvavaatimusten viitekehys. Viitekehys muodostuu sarjasta datahubin tarpeita palvelevia, liittyville osapuolille asetettavia tietoturvavaatimuksia. Kehitetty viitekehys käytiin datahubin tuntevien asiantuntijoiden kanssa läpi niin monta kertaa, että saavutettiin yksimielisyys viitekehyksen sopivuudesta datahubin tarpeisiin. Näin päästiin lopputulokseen, joka koostuu sellaisista yleisesti hyväksi todetuista tietoturvakäytännöistä, jotka on sovellettu erityisesti datahub-projektia varten.

Tietoturvavaatimuksien viitekehys korostaa osapuolien oma-aloitteisuutta omakohtaisessa riskiarviossa sekä niiden hahmottamien riskien hallinnan suunnittelussa. Oma-aloitteisuuden lisäksi viitekehys edellyttää osapuolilta kykyä tarvittaessa todistaa datahubiin liittyvien tietoturvauhkien valmistautumisen tasonsa. Tätä valmiutta kuvattiin työssä termillä todennettavuus. Todennettavuuden täyttymistä perusteltiin sillä, että vaikka Fingrid Datahub ei kykene todentamaan kaikkien liittyvien osapuolten tietoturvakäytäntöjä, sille on hyödyksi omata mahdollisuus tähän tulevaisuudessa. Omakohtaisen suunnittelun lisäksi viitekehys antaa joitakin erityisiä tietoturvavaatimuksia liittyville osapuolille. Nämä vaatimukset nähtiin tärkeinä nostaa esille erillisinä vaatimuksina riippumatta siitä, mihin toimenpiteisiin osapuoli päättää ryhtyä omakohtaisen suunnittelunsa perusteella. Ne suunniteltiin kuitenkin siten, että ne ovat mahdollisimman teknologianeutraaleja ja antavat osapuolelle mahdollisuuden toteuttaa ne suurelta osin itselleen parhaaksi näkemällään tavalla.

Työn tavoite eli datahubiin liittyviltä markkinaosapuolilta vaadittavan tietoturvan tason selvitys onnistui. Selvitys kiteytyi lopputuloksena tavoitellussa viitekehyksessä, joka saavutti sille asetetut vaatimukset. Viitekehyksen hyödyllisyys datahub-projektille on todennettu yhteistyössä Fingrid Datahubin asiantuntijoiden kanssa. Viitekehys antaa mallin datahubiin liittymistä varten tarkoitetun palvelusopimuksen tietoturvavaatimusten suunnittelua varten. Samalla se vie datahub-projektia merkityksellisesti eteenpäin toimien pohjatyönä kriittiselle, projektiin liittyvälle lainsäädäntöön pohjautuville ongelmille.

Työ nostaa esille myös ongelmia tietoturvakäytäntöihin liittyvässä tutkimuksessa. Työssä osoitetaan, että suuri osa tutkimusta on vielä varsin kehittymätöntä, eikä sen tuloksena kehitettyjen kokonaisvaltaisen tietoturvan muodostamiseen tarkoitettujen mallien ole yleisesti todistettu toimivan käytännössä. Kun tämän lisäksi huomioidaan työssä osoitettu tietoturvauhkien kasvava vakavuus ja arvaamattomuus, voidaan esittää, että tietoturvan paremmalle tutkimukselle on kasvava tarve. Tutkimuksen tulee pysyä perässä kasvavien ja monimutkaistuvien tietoturvauhkien kanssa ja samalla kyetä todentamaan, että käytetyt tutkimusmenetelmät tuottavat käytännössä toimivia tuloksia.

Lähdeluettelo

[1] European Comission [verkkosivu]. Bryssel, Belgia: European Comission. Digital transformation [viitattu 26. helmikuuta 2020]. Saatavissa: https://ec.europa.eu/growth/industry/policy/digital-transformation_en.

[2] Valtiovarainministeriö [verkkosivu]. Helsinki, Suomi: Valtiovarainministeriö. Digitalisaation edistämisen ohjelma [viitattu 26. helmikuuta 2020]. Saatavissa: https://vm.fi/digitalisaation-edistamisen-ohjelma.

[3] McKinsey & Company | Global Management Consulting [verkkosivu]. New York, Yhdysvallat: McKinsey & Company. Infographic: The accelerating digitization of the US economy [viitattu 26. helmikuuta 2020]. Saatavissa: https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/infographic-the-accelerating-digitization-of-the-us-economy.

[4] Department of Energy [verkkosivu]. Washington, D.C., Yhdysvallat: U.S. Department of Energy. Grid Modernization and the Smart Grid [viitattu 26. helmikuuta 2020]. Saatavissa: https://www.energy.gov/oe/activities/technology-development/grid-modernization-and-smart-grid.

[5] Gangale F, Vasiljevska J, Covrig F, Mengolini A, Fulli G. Smart grid projects outlook 2017: facts, figures and trends in Europe, EUR 28614 EN [verkkodokumentti]. Bryssel, Belgia: European Union; 2017 [viitattu 26 helmikuuta 2020]. Saatavissa: https://doi.org/10.2760/701587.

[6] European Commission, official website [verkkosivu]. Bryssel, Belgia: European Commission; 31. heinäkuuta 2014. Smart grids and meters [päivitetty 20. tammikuuta 2020; viitattu 26. helmikuuta 2020]. Saatavissa: https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/overview.

[7] SmartGrid.gov [verkkosivu]. Washington, D.C., Yhdysvallat: U.S. Department of Energy. The Smart Grid [viitattu 26. helmikuuta 2020]. Saatavissa: https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[8] Goldbach K, Rotaru AM, Reichert S, Stiff G, Gölz S. Which digital energy services improve energy efficiency? A multi-criteria investigation with European experts. Energy Policy [sähköinen julkaisu]. Huhtikuu 2018 [viitattu 26. helmikuuta 2020];115:239-48. Saatavissa: https://doi.org/10.1016/j.enpol.2017.12.036.

[9] Immonen A, Kiljander J, Aro M. Consumer viewpoint on a new kind of energy market. Electr Pow Syst Res [sähköinen julkaisu]. Maaliskuu 2020 [viitattu 26. helmikuuta 2020];180:1-11. Saatavissa: https://doi.org/10.1016/j.epsr.2019.106153.

[10] Fingrid [verkkosivu]. Helsinki, Suomi: Fingrid. Datahub-palvelut [viitattu 30. syyskuuta 2020]. Saatavissa: https://www.fingrid.fi/sahkomarkkinat/vahittaismarkkinoiden-tiedonvaihto/.

[11] EDIELfi [verkkosivu]. Helsinki, Suomi: Fingrid; 2019. Datahub - kohti keskitettyä tiedonvaihtoa [viitattu 30. syyskuuta 2019]. Saatavissa: https://www.ediel.fi/datahub.

[12] Fingrid Datahub. Sähkön vähittäismarkkinoiden liiketoimintaprosessit datahubissa [verkkodokumentti]. Helsinki, Suomi: Fingrid Datahub Oy; 11. heinäkuuta 2019 [viitattu 30. syyskuuta 2020]. Saatavissa: https://www.ediel.fi/sites/default/files/S%C3%A4hk%C3%B6n%20v%C3%A4hitt%C3%A4ismarkkinoiden%20liiketoimintaprosessit%20datahubissa%20v1.9.pdf.

[13] Fingrid Datahub. Sähkökaupan keskitetyn tiedonvaihdon palvelujen (datahub) käyttöönottosuunnitelma [verkkodokumentti]. Helsinki, Suomi: Fingrid Datahub Oy; 28. toukokuuta 2019 [viitattu 30. syyskuuta 2020]. Saatavissa: https://www.ediel.fi/sites/default/files/Datahub_k%C3%A4ytt%C3%B6%C3%B6nottosuunnitelma_v1.41.pdf.

[14] Sähkömarkkinalaki 2013/588.

[15] Urquhart L, McAuley D. Avoiding the internet of insecure industrial things. Comput Law Secur Rev [sähköinen julkaisu]. Kesäkuu 2018 [viitattu 15. marraskuuta 2019];34(3):450-66. Saatavissa: https://doi.org/10.1016/j.clsr.2017.12.004.

[16] Han CH, Park ST, Lee SJ. The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. Int J Crit Infrastruct Prot [sähköinen julkaisu]. Syyskuu 2019 [viitattu 20. marraskuuta 2019];26:1-10. Saatavissa: https://doi.org/10.1016/j.ijcip.2019.100312.

[17] ENISA. Smart Grid Security. Annex II. Security aspects of the smart grid [verkkodokumentti]. Heraklion, Kreikka: European Network and Information Security Agency; 25. huhtikuuta 2012 [viitattu 20. marraskuuta 2019]. Saatavissa: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf.

[18] Symantec. Internet Security Threat Report [verkkodokumentti]. Mountain View, Yhdysvallat: Symantec Corporation; huhtikuu 2016 [viitattu 29. marraskuuta 2019]. Saatavissa: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf?aid=elq_&om_sem_kw=elq_11155730&om_ext_cid=biz_email_elq_&elqTrackId=283a3acdb3ff42f4a70ab5a9f236eb71&elqaid=2902&elqat=2.

[19] Symantec. Internet Security Threat Report [verkkodokumentti]. Mountain View, Yhdysvallat: Symantec Corporation; helmikuu 2019 [viitattu 2. maaliskuuta 2020]. Saatavissa: https://docs.broadcom.com/doc/istr-24-2019-en.

[20] Valtioneuvoston päätös huoltovarmuuden tavoitteista 2008/539.

[21] CISA [verkkosivu]. Yhdysvallat: Cybersecurity and Infrastructure Security Agency. Energy Sector [viitattu 17. marraskuuta 2019]. Saatavissa: https://www.dhs.gov/cisa/energy-sector.

[22] EU Science HUB [verkkosivu]. Brussels, Belgium: Joint Research Centre. Critical infrastructure protection [päivitetty 27. elokuuta 2019; viitattu 17. marraskuuta 2019]. Saatavissa: https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection.

[23] Alsharthry S. Cyber attack on Saudi Aramco. Int J Technol Manag [sähköinen julkaisu]. Helmikuu 2017 [viitattu 27. marraskuuta 2019];11(5):3037-9. Saatavissa: https://pdfs.semanticscholar.org/6a0e/dae9946d64eef4450328d08a5cc38340a1a3.pdf.

[24] Södö, F. Erikoisasiantuntija, Fingrid Datahub. Sähkön vähittäismarkkinat ja kriittinen infrastruktuuri [haastattelu]. Helsinki, Suomi; 9 maaliskuuta 2020.

[25] Fingrid Datahub. Datahub Security Testing Threat Modelling [yhtiön sisäinen asiakirja]. Helsinki, Suomi [viitattu 18. marraskuuta 2019].

[26] Fingrid Datahub. DPIA Riskikartta [yhtiön sisäinen asiakirja]. Helsinki, Suomi [viitattu 18. marraskuuta 2019].

[27] Fingrid Datahub. Datahubin sisäisen riskiarvioryhmän raportti [yhtiön sisäinen asiakirja]. Helsinki, Suomi [viitattu 18. marraskuuta 2019].

[28] Neuvoston asetus (EU) N:o 2016/679.

[29] Tietosuojalaki 2018/1050.

[30] Kivipuro, A. Lakimies, Fingrid. Voimassaoleva lainsäädäntö ja Fingrid Datahub [haastattelu]. Helsinki, Suomi; 3. maaliskuuta 2020.

[31] Kyberturvallisuuskeskus [verkkosivu]. Helsinki, Suomi: Traficom; 21. lokakuuta 2019. Digitaaliset palvelut ja infrastruktuuri [viitattu 4. maaliskuuta 2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaaliset-palvelut-ja-infrastruktuuri.

[32] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148.

[33] Kyberturvallisuuskeskus. Datahubiin liittyville osapuolille asetettavat tietoturvavaatimukset [ryhmähaastattelu]. Helsinki, Suomi; 22. tammikuuta 2020.

[34] Puukangas, M. Erikoisasiantuntija, Fingrid Datahub. Markkinaosapuolten prosessien häiriintyminen [haastattelu]. Helsinki, Suomi; 3. joulukuuta 2019.

[35] Puukangas, M. Erikoisasiantuntija, Fingrid Datahub. Markkinaosapuolten toiminnot Datahubissa [haastattelu]. Helsinki, Suomi; 9. maaliskuuta 2020.

[36] Sähkön vähittäismarkkinoiden menettelytapa- ja sanomaliikenne ohje [verkkodokumentti]. Helsinki, Suomi: Energiateollisuus; 15. joulukuuta 2016 [päivitetty 21. lokakuuta 2019; viitattu 9. maaliskuuta 2020]. Saatavissa: https://energia.fi/files/4567/Vahittaismarkkinoiden_menettelytapa-_ja_sanomaliikenneohje_20191021_paivitetty_20200226_%28002%29.pdf.

[37] Rajala, A. Sähkökaupan datahub - lainsäädäntö ja tavoitteet [sähköinen diaesitys]. Helsinki, Suomi: Työ- ja elinkeinoministeriö; 20. syyskuuta 2018 [viitattu 30. syyskuuta 2020]. Saatavissa: https://valtioneuvosto.fi/documents/1410877/2132296/Datahub+lains%C3%A4%C3%A4d%C3%A4nt%C3%B6+Rajala+20092018.pdf/b4964ca8-7d2e-426c-bdd0-7f0eec186483/Datah

[38] Kuuranne, O. Asiantuntija, Fingrid Datahub. Datahubin B2B-rajapinnan tekniset toimintaperiaatteet [haastattelu]. Helsinki, Suomi; 18. helmikuuta 2020.

[39] Puukangas, M. Erikoisasiantuntija, Fingrid Datahub. Datahubiin liittyvät osapuolet [haastattelu]. Helsinki, Suomi; 4. lokakuuta 2019.

[40] Energiavirasto [verkkosivu]. Helsinki, Suomi: Energiavirasto. Verkkotoiminnan luvanvaraisuus [viitattu 30. syyskuuta 2020]. Saatavissa: https://energiavirasto.fi/verkkotoiminnan-luvanvaraisuus.

[41] Fingrid Datahub. Prosessikartta [verkkodokumentti]. Helsinki, Suomi: Fingrid Datahub Oy [viitattu 4. maaliskuuta 2020]. Saatavissa: https://www.ediel.fi/sites/default/files/Datahub%20Prosessikartta%20v1.11.pdf.

[42] Kimari, P. Tietosuoja-asiantuntija, Fingrid Datahub. Datahubia varten tehdyt teknologiavalinnat [haastattelu]. Helsinki, Suomi; 24. maaliskuuta 2020.

[43] Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtionhallinnon tietoturvasanasto [verkkodokumentti]. Helsinki, Suomi: Valtiovarainministeriö; 2008 [viitattu 13. marraskuuta 2019]. Saatavissa: https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229.

[44] Limnéll J. Digitaalinen yhteiskunta ja sen turvallisuus [julkaisematon esitys]. Espoo-Kauniainen reserviupseerit: Kauniaisten kaupungintalo; seminaari pidetty 12 marraskuuta 2019.

[45] Schmidt A. The Estonian Cyberattacks. In: Healey J, Grindal K, editors. The fierce domain - conflicts in cyberspace 1986-2012. Washington, D.C., Yhdysvallat: Atlantic Council; 2013 [viitattu 26. helmikuuta 2020]. Saatavissa: https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks.

[46] Estonian Information System Authority. Republic of Estonia Annual Cyber Security Assessment 2017 Estonian Information System Authority [verkkodokumentti]. Tallinna, Eesti: Estonian Information System Authority; 2017 [viitattu 26. helmikuuta 2020]. Saatavissa: https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.

[47] Mansfield-Devine S, editor. The state of operational technology security. Netw Secur [sähköinen julkaisu]. Lokakuu 2019 [viitattu 29. marraskuuta 2019];2019(10):9-13. Saatavissa: https://doi.org/10.1016/S1353-4858(19)30121-7.

[48] Lilienthal G, Ahmad N. Cyber-attack as inevitable kinetic war. Comput Law Secur Rev [sähköinen julkaisu]. Kesäkuu 2015 [viitattu 25. helmikuuta 2020]:31(3):490-400. https://doi.org/10.1016/j.clsr.2015.03.002.

[49] Hutchins EM, Cloppert MJ, Amin RM; Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains [verkkodokumentti]. Bethesda, Yhdysvallat: Lockheed Martin Corporation [viitattu 15. marraskuuta 2019]. Saatavissa: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[50] Bhardwaj A, Goundar S. Reducing the threat surface to minimise the impact of cyber-attacks. Netw Secur [sähköinen julkaisu]. Huhtikuu 2018 [viitattu 26. helmikuuta 2020];2018(4):15-9. Saatavissa: https://doi.org/10.1016/S1353-4858(18)30034-5.

[51] Chadwick DW, Fan W, Costantino G, de Lemos R, Cerbo FD, Herwono I, et al. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Gener Comp Sy [sähköinen julkaisu]. Tammikuu 2020 [viitattu 26. helmikuuta 2020];102:710-22. Saatavissa: https://doi.org/10.1016/j.future.2019.06.026.

[52] Työ- ja elinkeinoministeriö [verkkosivu]. Helsinki, Suomi: Työ- ja elinkeinoministeriö. Datahub kokoaisi sähkön käyttö- ja käyttäjätiedot yhteen järjestelmään - helpottaisi myös uusien palvelujen kehittämistä [päivitetty 20. syyskuuta 2018; viitattu 6. lokakuuta 2019]. Saatavissa: https://tem.fi/artikkeli/-/asset_publisher/datahub-kokoaisi-sahkon-kaytto-ja-kayttajatiedot-yhteen-jarjestelmaan-helpottaisi-myos-uusien-palvelujen-kehittamista?_101_INSTANCE_Ocg4pelPPCDJ_languageId=en_US.

[53] Mueller P, Yadegari B. The Stuxnet Work [verkkodokumentti]. Tucson, Yhdysvallat: The University of Arizona [viitattu 4. joulukuuta 2019]. Saatavissa: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf.

[54] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity [verkkodokumentti]. Gaithersburg, Yhdysvallat: National Institute of Standards and Technology; 16. huhtikuuta 2018 [viitattu 2. helmikuuta 2020]. Saatavissa: https://doi.org/10.6028/NIST.CSWP.04162018.

[55] Puolustusministeriö. Katakri 2015 Tietoturvallisuuden arviointityökalu viranomaisille [verkkodokumentti]. Helsinki, Suomi: Puolustusministeriö; 2015 [viitattu 2. helmikuuta 2020]. Saatavissa: https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf.

[56] International Organization for Standardization. ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. Geneve, Sveitsi: ISO; lokakuu 2013.

[57] International Organization for Standardization. ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls. Geneve, Sveitsi: ISO; 2013.

[58] Karabacak B, Yildrim SO, Baykal N. A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. Int J Crit Infrastruct Prot [sähköinen julkaisu]. Joulukuu 2016 [viitattu 19. joulukuuta 2019];15:47-59. Saatavissa: https://doi.org/10.1016/j.ijcip.2016.10.001.

[59] Vishwanath A, Neo LS, Goh P, Lee S, Khader M, Ong G, Chin J. Cyber Hygiene: The Concept, its Measure, and its Initial Tests. Decis Support Syst [sähköinen julkaisu]. Syyskuu 2019 [viitattu 22. joulukuuta 2019];128:1-11. Saatavissa: https://doi.org/10.1016/j.dss.2019.113160.

[60] Trim PRJ, Lee YI. The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. Ind Mark Manag [sähköinen julkaisu]. Marraskuu

2019 [viitattu 24. joulukuuta 2019];83:224-38. Saatavissa: https://doi.org/10.1016/j.indmarman.2019.04.003.

[61] Valkeinen H, Anttila H, Paltamaa J. Opas toimintakyvyn mittarin arviointiin TOIMIA-verkostossa (1.0) [verkkodokumentti]. Helsinki, Suomi: THL; 1. kesäkuuta 2014 [viitattu 27. joulukuuta 2019]. Saatavissa: https://thl.fi/documents/974257/1449823/Mittariopas_VALMIS_090614+(2).pdf/b53595b9-15b8-4fa3-8765-23cd9221de8f.

[62] Noble H, Mitchell G. What is grounded theory?_Evid-Based Nurs [sähköinen julkaisu]. 2016 [viitattu 19. joulukuuta 2019];19:34-35. Saatavissa: http://dx.doi.org/10.1136/eb-2016-102306.

[63] Hasson F, Keeney S, McKenna H, Research guidelines for the Delphi Survey Technique. J Adv Nurs [sähköinen julkaisu]. Lokakuu 2000 [viitattu 19. joulukuuta 2019];32(4):1008-15. Saatavissa: https://www.ncbi.nlm.nih.gov/pubmed/11095242.

[64] Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Comput Secur [sähköinen julkaisu]. Cyber threat intelligence sharing. Marraskuu 2019 [viitattu 20. helmikuuta 2020];87:1-13. Saatavissa: https://doi.org/10.1016/j.cose.2019.101589.

[64] Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions. Comput Secur [sähköinen julkaisu]. Marraskuu 2019 [viitattu 17. marraskuuta 2019];87:1-13. Saatavissa: https://doi.org/10.1016/j.cose.2019.101589.

[65] Södö, F. Erikoisasiantuntija, Fingrid Datahub. Datahubiin liittyville osapuolille asetettavat tietoturvavaatimukset [haastattelu]. Helsinki, Suomi; 28. tammikuu 2020.

[66] Kansalaiset - Kanta.fi [verkkosivu]. Helsinki, Suomi: Kansaneläkelaitos. Mitä Kanta-palvelut ovat? [päivitetty 8. marraskuuta 2019; viitattu 27. maaliskuuta 2020]. Saatavissa: https://www.kanta.fi/mita-kanta-palvelut-ovat.

[67] Henkilöasiakkaat - kela.fi [verkkosivu]._Helsinki, Suomi: Kansaneläkelaitos; 15. joulukuuta 2009. Tutustu Kansalliseen Terveysarkistoon verkossa [viitattu 30. joulukuuta 2019]. Saatavissa: https://www.kela.fi/-/tutustu-kansalliseen-terveysarkistoon-verkossa.

[68] Kanta-palvelut. Tekniset liittymismallit Kanta-palveluihin [verkkodokumentti]. Helsinki, Suomi: Kansaneläkelaitos; 9. joulukuuta 2019 [viitattu 7. lokakuuta 2019]. Saatavissa: https://www.kanta.fi/documents/20143/106828/Tekniset+liittymismallit+Kanta-palveluihin.pdf/a057c34a-f822-71fd-b2df-097245d582ee.

[69] Omakanta - Kanta.fi [verkkosivu]. Helsinki, Suomi: Kansaneläkelaitos. Lainsäädäntö [päivitetty 13. helmikuuta 2020; viitattu 25. maaliskuuta 2020]. Saatavissa: https://www.kanta.fi/omakanta

[70] Kansalaiset - Kanta.fi [verkkosivu]. Helsinki, Suomi: Kansaneläkelaitos. Lainsäädäntö [päivitetty 2. huhtikuuta 2019; viitattu 4. marraskuuta 2019]. Saatavissa: https://www.kanta.fi/lainsaadanto.

[71] Kansalaiset - Kanta.fi [verkkosivu]. Helsinki, Suomi: Kansaneläkelaitos. Sertifiointi, olennaiset vaatimukset ja omavalvonta [päivitetty 18. helmikuuta 2020; viitattu 27. lokakuuta 2019]. Saatavissa: https://www.kanta.fi/jarjestelmakehittajat/sertifiointi.

[72] Fingrid Datahub. Testaus- ja sertifiointisuunnitelma [verkkodokumentti]. Helsinki, Suomi: Fingrid Datahub Oy; 31. tammikuuta 2020 [viitattu 30. helmikuuta 2020]. Saatavissa: https://www.ediel.fi/sites/default/files/Testaus-%20ja%20sertifiointisuunnitelma_v1.2.pdf.

[73] Kansalaiset - Kanta.fi [verkkosivu]. Helsinki, Suomi: Kansaneläkelaitos. HL7-määrittelyt [päivitetty 20. tammikuuta 2020; viitattu 7. lokakuuta 2019]. Saatavissa: https://www.kanta.fi/jarjestelmakehittajat/hl7.

[74] HL7 Finland ry [verkkosivu]. Jyväskylä, Suomi: HL7 Finland. Esittely [viitattu 30. joulukuuta 2019]. Saatavissa: http://www.hl7.fi/esittely/.

[75] THL. Tietoturvavaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille [verkkodokumentti]. Helsinki, Suomi: THL [viitattu 12. lokakuuta 2019]. Saatavissa: https://thl.fi/documents/920442/1449818/Liite_1_THL_M%c3%a4%c3%a4r%c3%a4ys_1_2015_Tietoturvavaatimukset_201501.pdf/f2817278-2843-4c2d-b038-bac88dd9691d.

[76] VM - Vahti-ohjeet [verkkosivu]. Helsinki, Suomi: Valtiovarainministeriö. Sisäverkko-ohje [viitattu 30 joulukuuta 2019]. Saatavissa: https://www.vahtiohje.fi/web/guest/3/2010-sisaverkko-ohje.

[77] Valtiovarainministeriö [verkkosivu]. Helsinki, Suomi: Valtiovarainministeriö. Voimassa olevat tietoturvaohjeet ja -määräykset [viitattu 30. joulukuuta 2019]. Saatavissa: https://vm.fi/julkaisut/vahti.

[78] Kansallinen terveysarkisto. Vaatimukset potilastietojärjestelmien käyttölokeille [verkkodokumentti]. Helsinki, Suomi: Kansaneläkelaitos; 4. joulukuuta 2013 [viitattu 30. joulukuuta 2019]. Saatavissa: https://www.kanta.fi/documents/20143/107839/Potilastietoj%C3%A4rjestelmien+k%C3%A4ytt%C3%B6tapaukset+Liite5+Vaatimukset+potilastietoj%C3%A4rjestelmien+k%C3%A4ytt%C3%B6lokeille.pdf/4e5675ec-1cf3-7baf-a5ad-aeee66a10950.

[79] Terveyden ja hyvinvoinnin laitos [verkkosivu]. Helsinki, Suomi: THL. OID-yksilöintitunnukset [päivitetty 26. heinäkuuta 2018; viitattu 5. tammikuuta 2020]. Saatavissa: https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/koodistopalvelu/tekniset-ohjeet/oid-yksilointitunnukset.

[80] International Organization for Standardization. ISO/IEC 9843-1:2012. _Information technology — Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree - Part 1. Geneve, Sveitsi: ISO; toukokuu 2012.

[81] Kansallinen terveysarkisto. Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset [verkkodokumentti]. Helsinki, Suomi: Kansaneläkelaitos; 14. joulukuuta 2015

[viitattu 7. lokakuuta 2019]. Saatavissa: https://www.kanta.fi/documents/20143/106828/Kanta-palvelut+tieto-+ja+sanomaliikenteen+tietoturvavaatimukset.pdf/e97ca7b7-9225-0d17-86ac-44c96861efbe.

[82] Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 2009/298.

[83] Nordea.fi. Web Services File Transfer Service Description [verkkodokumentti]. Helsinki, Suomi: Nordea Bank Danmark A/S; tammikuu 2017 [viitattu 30. lokakuuta 2019]. Saatavissa: https://www.nordea.fi/Images/146-85800/web_services.pdf.

[84] Kenton, W. What Is Cash Management? [sähköinen julkaisu]. New York, Yhdysvallat: Investopedia; 2019 [päivitetty 17. heinäkuuta 2019; viitattu 5. tammikuuta 2019]. Saatavissa: https://www.investopedia.com/terms/c/cash-management.asp.

[85] Nordea-konserni [verkkosivu]. Helsinki, Suomi: Nordea Bank Danmark A/S. Your Cash Management partner [viitattu 5. tammikuuta 2020]. Saatavissa: https://www.nordea.com/fi/palvelut/cashmanagement/yourrelationshipbank/your-cash-management-bank/.

[86] SSH.com [verkkosivu]. Helsinki, Suomi: SSH Communications Security, Inc. PKI - Public Key Infrastructure [viitattu 5. tammikuuta 2019]. Saatavissa: https://www.ssh.com/pki.

[87] Nordea.fi. Web Services - Verkko- ja mobiilipalvelut [verkkosivu]. Helsinki, Suomi: Nordea Bank Danmark A/S [viitattu 30. lokakuuta 2019]. Saatavissa: https://www.nordea.fi/yritysasiakkaat/palvelumme/verkko-mobiilipalvelut/web-services.html#tab=Aineistotyypit.

[88] Nordea.fi. Nordea Bank Oyj:n yritysten elektronisten palvelujen yleiset ehdot [verkkodokumentti]. Helsinki, Suomi: Nordea Bank Danmark A/S; lokakuu 2018 [viitattu 16. lokakuuta 2019]. Saatavissa: https://www.nordea.fi/Images/146-72150/mmye030dl.pdf.

[89] Nordea. Web Services Security and Communication [verkkodokumentti]. Helsinki, Suomi: Nordea Bank Danmark A/S; elokuu 2017 [viitattu 6. tammikuuta 2020]. Saatavissa: https://www.nordea.fi/Images/147-163432/web-services-security-and-communication-description.pdf.

[90] Fingrid Datahub. Ohjausryhmän säännöllinen kokous [haastattelu]. Helsinki, Suomi; 5. marraskuuta 2019.

[91] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto. Luotettavaa tiedonsiirtoa [viitattu 7. tammikuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/sivut/palveluvayla/esittely.

[92] Suomi.fi. Suomi.fi-palveluväylän käyttöehdot [verkkodokumentti]. Helsinki, Suomi: Digi- ja väestövirasto; 4. heinäkuuta 2016 [viitattu 25. maaliskuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/storage/cms.files/mCIkgj4nD954f3u5.pdf.

[93] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto; 1. tammikuuta 2020. X-Road-tiedonsiirtoprotokolla [viitattu 7. tammikuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/592bf54a03f6d100018db5d4.

[94] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto. Käyttönoton prosessi [viitattu 25. maaliskuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/sivut/palveluvayla/kayttoonotto/prosessi.

[95] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto; 1. tammikuuta 2020. Liityntäpalvelimien liittäminen testi- tai tuotantoympäristöön [viitattu 25. maaliskuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/59145e7b14bbb10001966f72.

[96] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto; 1. tammikuuta 2020. Palveluväylässä käytetyt tunnisteet [viitattu 25. maaliskuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/591da44c14bbb10001966fc9.

[97] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto; 1. tammikuuta 2020. Uuden alijärjestelmän liittäminen liityntäpalvelimeen ja sen poistaminen [viitattu 25. maaliskuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/591ac1e314bbb10001966f9c.

[98] Suomi.fi [verkkosivu]. Helsinki, Suomi: Digi- ja väestövirasto; 1. tammikuuta 2020. Liityntäpalvelimen valvonta [viitattu 25. maaliskuuta 2020]. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/591ea2ab14bbb10001966fce.

[99] National Institute of Standards and Technology [verkkosivu]. Gaithersburg, Yhdysvallat: National Institute of Standards and Technology; 5. tammikuuta 2015. About NIST [päivitetty 14. kesäkuuta 2017; viitattu 2. helmikuuta 2020]. Saatavissa: https://www.nist.gov/about-nist.

[100] Cybersecurity Enhancement Act of 2014.

[101] Martinez, R. Kyberturvallisuusasiantuntija, Amazon. NIST:n viitekehys kriittisten infrastruktuurien kyberturvallisuuden kehittämiseen [puhelinhaastattelu]. Helsinki, Suomi & Seattle, Yhdysvallat; 19. helmikuuta 2020.

[102] National Institute of Standards and Technology [verkkosivu]. Gaithersburg, Yhdysvallat: National Institute of Standards and Technology; 15. lokakuuta 2019. Succes Story: Israel National Cyber Directorate [viitattu 2. helmikuuta 2020]. Saatavissa: https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate.

[103] Kyberturvallisuuskeskus. Datahubiin liittyville osapuolille asetettavat tietoturvavaatimukset [haastattelu]. Helsinki, Suomi; 22. tammikuuta 2020.

[104] Army Publishing Directorate. Army Regulation 25-2, Information Management: Army Cybersecurity [verkkodokumentti]. Washington, D.C., Yhdysvallat: Army Publishing Directorate; 4. huhtikuuta 2019 [viitattu 2. helmikuuta 2020]. Saatavissa: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN17503_AR25_2_Admin_FINAL.pdf.

[105] Insta. Tietoturvavaatimusten määrittäminen [puhelinhaastattelu]. Helsinki, Suomi; 27. marraskuuta 2019.

[106] Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 2010/681.

[107] Neuvoston päätös (EU) 2013/488/EU.

[108] Kyberturvallisuuskeskus [verkkosivu]. Helsinki, Suomi: Traficom; 25. kesäkuuta 2019. Hyväksytyt tietoturvallisuuden arviointilaitokset [viitattu 10. helmikuuta 2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta/hyvaksytyt-tietoturvallisuuden-arviointilaitokset.

[109] Södö, F. Erikoisasiantuntija, Fingrid Datahub. Datahubiin liittyvien markkinaosapuolten tietoturvan todentaminen [haastattelu]. Helsinki, Suomi; 23. maaliskuuta 2020.

[110] Suomen Standardisoimisliitto SFS [verkkosivu]. Helsinki, Suomi: Suomen Standardisoimisliitto. ISO/IEC 2700 Tietoturvallisuuden hallintajärjestelmä [viitattu 16. helmikuuta 2020]. Saatavissa: https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta?gclid=Cj0KCQiA7aPyBRChARIsAJ-fWCgIB4FgcNz1VndtpPFHBUYHtBamLByRdvQbuN2knimtFmWRx8GKZoIY-aAohOEALw_wcB.

[111] Fingrid Datahub. Ohjausryhmän säännöllinen kokous [haastattelu]. Helsinki, Suomi; 24. helmikuuta 2020.

[112] Kyberturvallisuuskeskus. Diplomityön lopputulosten katselmointi [haastattelu]. Helsinki, Suomi; 6. maaliskuuta 2020.

[113] Fingrid Datahub. Tietoturvavaatimusten esittely Fingrid Datahubin henkilöstölle [haastattelu]. Helsinki, Suomi; 25. helmikuuta 2020.

[114] Martinez, R. Kyberturvallisuusasiantuntija, Amazon. Todennettavuus tietoturvavaatimuksissa ja teknologianeutraalit tavat sen saavuttamiseksi [puhelinhaastattelu]. Helsinki, Suomi & Seattle, Yhdysvallat; 28. helmikuuta 2020.

[115] Fingrid Datahub. Tietoturvatestauksen palaveri [haastattelu]. Helsinki, Suomi; 7. helmikuuta 2020.

[116] Kimari, P, Tietosuoja-asiantuntija, Fingrid Datahub & Lintunen P, Kehityspäällikkö, Fingrid Datahub. Markkinaosapuolten kohdistamat riskit datahubiin [haastattelu]. Helsinki, Suomi; 26. marraskuuta 2019.

[117] Turvallisuusselvityslaki 726/2014.

[118] Kyberturvallisuuskeskus [verkkosivu]. Helsinki, Suomi: Traficom. Ajankohtaista [viitattu 25. helmikuuta 2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaiset.

[119] Kyberturvallisuuskeskus [verkkosivu]. Helsinki, Suomi: Traficom; 7. tammikuuta 2019. Arviointi, hyväksyntä ja neuvonta [viitattu 25. helmikuuta 2020]. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta.

[120] Tietosuojalaki 2018/1050.

[121] Kivipuro, A. Lakimies, Fingrid. Voimassaoleva lainsäädäntö ja Fingrid Datahub [haastattelu]. Helsinki, Suomi; 3. maaliskuuta 2020.

[122] Puukangas, M. Erikoisasiantuntija, Fingrid Datahub. Datahubissa liikkuva tieto [haastattelu]. Helsinki, Suomi; 7. helmikuuta 2020.

[123] Morteza Safaei P, Bou-Harb P, Varma K, Neshenko N, Pados DA, Choo KKR. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns. Digit Invest [sähköinen julkaisu]. Huhtikuu 2019 [viitattu 29. maaliskuuta 2020];28:40-9. Saatavissa: https://doi.org/10.1016/j.diin.2019.01.014.