Euroopan Unionin kyberturvallisuusdirektiivin vaatimat toimenpiteet organisaatioissa

Tuomas Pelttari

2023 Laurea

Laurea-ammattikorkeakoulu

Euroopan Unionin kyberturvallisuusdirektiivin vaatimat toimenpiteet organisaatioissa

Tuomas Pelttari

Turvallisuus ja riskienhallinta

Opinnäytetyö

Huhtikuu 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuus ja riskienhallinta
Tradenomi (AMK)

Tuomas Pelttari

Euroopan Unionin kyberturvallisuusdirektiivin vaatimat toimenpiteet organisaatioissa

Vuosi 2023 Sivumäärä 50

Euroopan Unioni hyväksyi joulukuussa 2022 direktiivin toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa (ns. NIS2-direktiivi). Uuden kyberturvallisuusdirektiivin tarkoitus on vastata alati kehittyviin ja yleistyviin kyberturvallisuusuhkiin määrittämällä tiettyjä vaatimuksia kyberturvallisuuden toteuttamiselle yhteiskunnan kannalta merkittävissä organisaatioissa.

Tässä opinnäytetyössä käydään läpi direktiivin sisältämät vaatimukset sekä esitetään keinoja vaatimusten täyttämiseksi direktiivin soveltamisalaan kuuluvissa organisaatioissa. Soveltamisala sisältää merkittävän osan eurooppalaisista yrityksistä ja julkisesta hallinnosta, jotka voivat hyödyntää opinnäytetyötä vapaasti tarvittavien toimenpiteiden suunnittelussa ja valmistauduttaessa direktiivin voimaantuloon. Opinnäytetyön toimeksiantajana toimi Digi- ja väestötietovirasto, jonka tehtävänä on edistää yhteiskunnan digitalisaatiota, turvata tietojen saatavuutta ja tarjota palveluja asiakkaiden elämäntapahtumiin.

Opinnäytetyön tarkoituksena oli kytkeä olemassa olevat kyberturvallisuuden käytännöt ja mallit direktiivin vaatimuksiin ja siten tuottaa helposti hyödynnettävää valmista aineistoa vaatimusten täyttämisen tueksi. Direktiivin vaatimien toimenpiteiden pohdinnassa hyödynnetty tietoperusta rakentuu kattavasti aikaisemman tutkimustiedon sekä erilaisten tieto- ja kyberturvallisuuden standardien ja hyvien käytäntöjen pohjalle. Tutkimusmenetelmänä opinnäytetyössä käytettiin laadullisen tutkimuksen sisällönanalyysiä.

Opinnäytetyön tuotoksena syntyi analyysi direktiivin soveltamisalasta ja vaatimuksista sekä lukuisia toimenpide-ehdotuksia keinoista, joilla vaatimuksiin voidaan vastata organisaatioissa. Direktiivi koskettaa varsin suurta joukkoa eurooppalaisia organisaatioita, joiden kyberturvallisuuteen liittyviä toimenpiteitä ei ole aikaisemmin säännelty välttämättä lainkaan. Direktiivissä vaadittavat toimenpiteet perustuvat kuitenkin hyvin pitkälti kansainvälisiin standardeihin ja muihin kyberturvallisuuden malleihin. Kehittämällä kyberturvallisuutta tässä työssä esiteltyjen käytäntöjen mukaisesti organisaatiot voivat täyttää uuden direktiivin vaatimukset.

Asiasanat: digitaalinen turvallisuus, Euroopan Unioni, kyberturvallisuus, kyberturvallisuusdirektiivi, lainsäädäntö

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security, Safety and Risk Management
Bachelor's Thesis

Tuomas Pelttari
Measures Required by the European Union's Cybersecurity Directive in Organizations
Year 2023 Pages 50

The European Union adopted a Directive on measures to ensure a common high level of cybersecurity across the Union (the so-called NIS2 Directive) in December 2022. The aim of the new cybersecurity directive is to respond to the evolving and increasing cybersecurity threats by defining requirements for the implementation of cybersecurity in organizations of significant importance to society.

This thesis explains the requirements of the directive and outlines ways to meet the requirements in the organisations. The scope of the directive includes a significant part of European companies and public administration, which can use this thesis to plan the necessary measures while preparing for the directive. The thesis was commissioned by the Digital and Population Data Services Agency, whose mission is to promote the digitalisation of society, to secure the availability of information, and to provide services related to customers' life events.

The objective of the thesis was to connect the existing cybersecurity practices and models with the requirements of the directive, thus producing readily usable material to support the compliance of the organisations. The theoretical framework used in defining the required measures is built on a comprehensive foundation of previous research and various information security and cybersecurity standards and good practices. The research method used in the thesis was content analysis of qualitative research.

As a result of the thesis, an analysis of the scope and requirements of the directive was produced, as well as numerous proposals for measures to meet the requirements. The Directive affects a large number of European organisations whose cybersecurity measures have not necessarily been regulated at all in the past. However, the measures required are based on international standards and well-established models of cybersecurity. By developing cybersecurity in line with the practices outlined in this paper, organisations can meet the requirements of the new Directive.

Keywords: cybersecurity, cybersecurity directive, digital security, European Union, legislation

Sisällys

1 Johdanto

Nykyisin lähes kaikki yhteiskunnan kannalta kriittiset toiminnot ja kansalaisille tarjottavat palvelut ovat tavalla tai toisella riippuvaisia tietojärjestelmistä ja tietoverkoista, sekä niiden toimivuudesta ja turvallisuudesta. Tietoverkkoihin kohdistuvat kyberturvallisuusuhat ovat monimuotoistuneet ja moninkertaistuneet maailmanlaajuisesti viimeisen vuosikymmenen aikana ja riittävästä suojautumisesta näitä uhkia vastaan onkin tullut entistä tärkeämpää. Yhteiskunnan palveluiden häiriötön ja vakaa toiminta luo pohjaa kansalaisten luottamukselle yhteiskuntaa kohtaan.

Euroopan Unionin keskeisiä tavoitteita ovat muun muassa jäsenvaltioidensa turvallisuuden ja yhtenäisen eurooppalaisen alueen sekä tieteen ja teknologian kehityksen edistäminen. Vastatakseen alati kasvaviin kyberturvallisuusuhkiin Euroopan Unioni sääti vuonna 2016 direktiivin 2016/1148/EU *toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa* eli NIS-direktiivin (security of network and information systems). Siitä huolimatta, että NIS-direktiivi on parantanut huomattavasti unionin kyberturvallisuutta, siinä havaittiin kuitenkin sisältölähtöisiä puutteita. Näitä puutteita Euroopan Unioni pyrki paikkaamaan julkaisemalla vuoden 2022 joulukuussa uuden kyberturvallisuusdirektiivin 2022/2555/EU *toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi koko unionissa*. Uusi kyberturvallisuusdirektiivi, jota on toisinaan kutsuttu myös NIS2-direktiiviksi, määrittää kyberturvallisuuden vähimmäistason, joka tulee saattaa osaksi kunkin jäsenmaan kansallista lainsäädäntöä 21 kuukauden kuluessa julkaisusta.

Uuden kyberturvallisuusdirektiivin tarkoituksena on yhtenäistää kyberturvallisuuden korkea taso koko Euroopan Unionin alueella määrittämällä tiettyjä vaatimuksia kyberturvallisuuden toteuttamiselle yhteiskunnan kannalta merkittävissä organisaatioissa. Tässä opinnäytetyössä selvitetään direktiivin sisältämät vaatimukset sekä esitetään keinoja niiden toteuttamiseksi organisaatioissa. Uuden kyberturvallisuusdirektiivin soveltamisala sisältää merkittävän osan eurooppalaisista yrityksistä ja julkisesta hallinnosta, joten opinnäytetyötä voi vapaasti hyödyntää tarvittavien toimenpiteiden suunnittelussa ja valmistauduttaessa direktiivin voimaantuloon.

Opinnäytetyön toimeksiantajana toimi Digi- ja väestötietovirasto. Viraston tehtävänä on edistää yhteiskunnan digitalisaatiota, turvata tietojen saatavuutta ja tarjota palveluja asiakkaiden elämäntapahtumiin. Virastossa työskentelee yli 900 työntekijää ja se toimii yli 30 paikkakunnalla eri puolilla Suomea. (Digi- ja väestötietovirasto 2023a.). Virasto kehittää julkisen hallinnon digitaalisen turvallisuuden hallintaa muun muassa järjestämällä koulutuksia, tapahtumia ja käytännön harjoituksia, rakentamalla ja ylläpitämällä yhteistyöverkostoja sekä

tuottamalla julkaisuja ja digitaalisen turvallisuuden hallinnollista tilannekuvaa (Digi- ja väestötietovirasto 2023b). Toimeksiantaja voi hyödyntää opinnäytetyön tuloksia julkisen hallinnon digitaalisen turvallisuuden informaatio-ohjauksessa uuden kyberturvallisuusdirektiivin vaatimiin toimenpiteisiin liittyen.

1.1 Opinnäytetyön tavoite ja tutkimuskysymykset

Opinnäytetyön tavoitteena oli tutkia laadullisen tutkimuksen menetelmin joulukuussa 2022 Euroopan Unionissa julkaistun ja vuosien 2023–2024 aikana jäsenvaltioiden kansallisissa lainsäädännöissä voimaan astuvan uuden kyberturvallisuusdirektiivin vaatimuksia ja täytäntöönpanon vaikutuksia sen soveltamisalan organisaatioissa.

Opinnäytetyön tutkimuskysymykset ovat:

- Millaisia organisaatioita uusi kyberturvallisuusdirektiivi koskee?
- Millaisia vaatimuksia kyberturvallisuuden parantamiseksi uusi kyberturvallisuusdirektiivin sisältää sen soveltamisaloilla toimiville organisaatioille?
- Millaisin konkreettisin toimenpitein organisaatiot voivat täyttää uuden kyberturvallisuusdirektiivin vaatimukset?

Opinnäytetyön tuotoksena syntyi analyysi direktiivin soveltamisalasta ja olennaisimmista vaatimuksista sekä toimenpide-ehdotuksia keinoista, joilla vaatimuksiin voidaan vastata organisaatioissa. Toimenpide-ehdotusten koostamisessa on hyödynnetty kattavasti erilaisia olemassa olevia kyberturvallisuuden käytäntöjä, standardeja ja ohjeistuksia.

Opinnäytetyön raportin ensimmäisessä luvussa esitellään opinnäytetyön aihe, toimeksiantaja sekä tavoitteet. Toisessa luvussa esitellään työn kannalta olennainen tietoperusta. Kolmannessa luvussa kuvataan itse tutkimusprosessin toteutus sekä tutkimuksessa käytetyt menetelmät. Neljännessä ja viidennessä luvussa käydään läpi varsinaisen analyysin tulokset eli direktiivin soveltamisala ja direktiivin vaatimat käytännön toimenpiteet.

1.2 Rajaukset

Opinnäytetyössä ei tarkastella minkään yksittäisen organisaation tai toimialan nykyhetken valmiuksia direktiivin vaatimusten täyttämiseksi, eikä myöskään tehdä tarkkaa kuiluanalyysiä nykyhetken ja tavoitetilan välillä. Opinnäytetyössä käydään kursiivisesti direktiivin vaatimukset läpi ja esitetään niille yleisen tason toimenpiteitä, jotta mahdollisimman moni eri toimialoilla toimiva organisaatio voisi hyötyä opinnäytetyöstä.

Direktiivissä asetetaan huomattava määrä vaatimuksia, jotka on suunnattu vain joko jäsenvaltiolle itselleen tai jäsenvaltion kansalliselle kyberturvallisuudesta vastaavalle viranomaiselle.

Nämä vaatimukset eivät kosketa muita toimijoita, joten ne rajattiin tämän opinnäytetyön tarkastelun ulkopuolelle.

Koska kyseessä on Euroopan Unionin direktiivi, jää jäsenvaltiolle kohtalaisissa määrin vapautta sisällyttää direktiivissä esitellyt asiat ja vaatimukset kansalliseen lainsäädäntöön. Kansallinen lainsäädäntötyö oli tätä opinnäytetyötä tehtäessä edelleen kesken, joten työssä keskitytään nimenomaisesti Euroopan Unionin asettaman direktiivin vaatimuksiin ja velvoitteisiin. Kansallisessa lainsäädännössä voidaan päätyä säätämään myös direktiiviä vaativampia velvoitteita. Direktiivi toimii kuitenkin pohjatasona koko Euroopan Unionin jäsenmaiden lainsäädännölle siten, että sitä vähäisempiä vaatimuksia ei voida kansallisessa laissa säätää. Kansallisen lainsäädännön on määrä valmistua viimeistään vuonna 2024.

2 Kyberturvallisuuden käsitteistöä ja käytäntöjä

Direktiivissä esitettyjen vaatimusten täyttämiseksi tarvittavien keinojen pohdinnassa hyödynnetty tietoperusta rakentuu kattavasti aiemman tutkimustiedon sekä erilaisten tieto- ja kyberturvallisuuden standardien ja hyvien käytäntöjen pohjalle. Kyberturvallisuus on jatkuvassa muutoksessa tietotekniikan ja digitalisaation kehityksen myötä ja se on osittain huomaamattakin noussut yhteiskunnassa hyvin keskeiseen rooliin. Tässä kappaleessa esitetään työn kannalta keskeiset käsitteet sekä analyysissä ja toimenpide-ehdotusten laatimisessa hyödynnetty tietoperusta.

2.1 Keskeiset käsitteet ja niiden määritelmät

Keskeisiä käsitteitä työssä ovat muun muassa direktiivissä esitetyt asiakokonaisuudet, kuten soveltamisala, kyberturvallisuus, riskienhallinta ja toiminnan jatkuvuus.

Direktiivi on yksi Euroopan Unionin säädöstyypeistä. Euroopan Unionin jäsenmailleen laatimia säädöksiä ovat asetukset, direktiivit, päätökset, suositukset ja lausunnot. Käyttäessään unionin toimivaltaa toimielimet hyväksyvät asetuksia, direktiivejä ja päätöksiä sekä antavat suosituksia ja lausuntoja. Direktiivi velvoittaa saavutettavaan tulokseen nähden jokaista jäsenvaltiota, jolle se on osoitettu, mutta jättää kansallisten viranomaisten valittavaksi muodon ja keinot. (Euroopan Unioni 2016.)

Soveltamisala määrittelee sen, mihin asioihin taikka keihin henkilöihin tai organisaatioihin lakia sovelletaan (Tieteen termipankki 2023). Soveltamisalaa koskevat säännökset on esitelty direktiivin toisessa artiklassa. Uuden kyberturvallisuusdirektiivin soveltamisalaan kuuluvat tietyt edellytykset täyttävät julkiset ja yksityiset toimijat, jotka harjoittavat toimintaansa Euroopan Unionissa (Direktiivi 2022/2555/EU). Edellytykset soveltamisalaan kuulumiselle on esitelty tarkemmin opinnäytetyön neljännessä kappaleessa.

Toimivaltaisella viranomaisella tarkoitetaan jäsenvaltion nimeämää tai perustamaa yhtä tai useampaa viranomaista, joka vastaa kyberturvallisuudesta ja direktiiviin 2022/2555/EU liittyvistä valvontatehtävistä. Mikäli jäsenvaltiossa on vain yksi toimivaltainen viranomainen, kyseinen toimivaltainen viranomainen toimii myös jäsenvaltion keskitettynä yhteyspisteenä. (Direktiivi 2022/2555/EU, 8 artikla.)

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille kybertoimintaympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa, myös häiriötilanteissa. Kybertoimintaympäristöllä tarkoitetaan yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä. (Digi- ja väestötietovirasto 2022b, 16-17.) Kyberturvallisuuteen kuuluu oleellisesti toimenpiteet, joilla kybertoimintaympäristön uhkia voidaan hallita. Tietoturva liittyy olennaisesti kyberturvallisuuteen. Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. (TSK 2018, 22.)

Riskienhallinnalla tarkoitetaan järjestelmällistä ja suunnitelmallista toimintaa, joka tukee organisaation tavoitteiden saavuttamista tunnistamalla organisaation toimintaan vaikuttavia mahdollisia tapahtumia. Riskienhallinta sisältää muun muassa riskien ja mahdollisuuksien analysoinnin sekä riskien hallitsemiseksi tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet. (TSK 2017, 50.)

Poikkeama tarkoittaa mitä tahansa tapahtumaa, joka vaikuttaa haitallisesti kyberturvallisuuteen. Poikkeamien käsittelyllä tarkoitetaan menettelyjä, jotka tukevat poikkeaman havaitsemista, analyysia ja sen vaikutusten rajoittamista sekä poikkeamaan reagointia. (Direktiivi 2016/1148/EU, 4 artikla.)

Toiminnan jatkuvuudella tarkoitetaan organisaation kykyä jatkaa toimintojen, palveluiden ja tuotteiden toimittamista häiriön tai poikkeaman jälkeen (ISO 22301, 9). Jatkuvuudenhallinnaksi kutsutaan prosessia, jonka avulla organisaatio tunnistaa toimintaansa kohdistuvat uhkat, riskit, häiriötilanteet ja riippuvuudet sekä arvioi uhkien vaikutukset organisaatiossa. Jatkuvuudenhallinnan avulla organisaatio järjestää ja toteuttaa menettelytavat häiriötilanteiden varalle sekä varmistaa kriittisten kumppaneidensa kyvyn toimia häiriötilanteissa. Jatkuvuudenhallinnalla luodaan toimintatavat vakavia häiriötilanteita varten. (Huoltovarmuuskeskus 2023.)

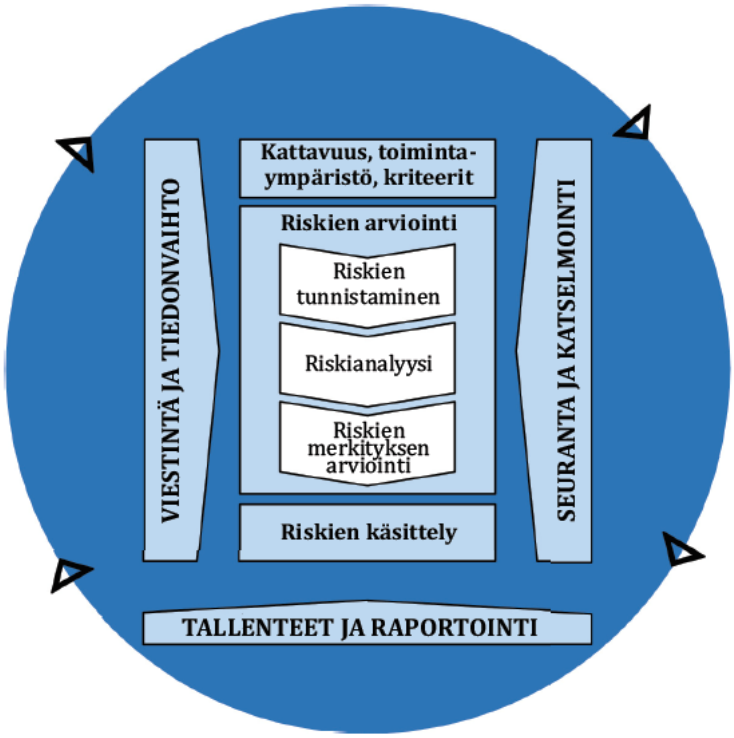
2.2 Standardit ja hyvät käytännöt kyberturvallisuuden kehittämisen tukena

Kyberturvallisuuden toteuttamiseen on pitkään haettu organisaatioissa tukea teknologisista ratkaisuista sekä erilaisista standardeista. Kansainvälisistä standardeista keskeisiä tämän opinnäytetyön kontekstissa ovat erityisesti SFS-ISO 27001 tietoturvallisuuden

hallintajärjestelmän standardi, SFS-ISO 31000 riskienhallinnan standardi sekä SFS-EN ISO 22301 jatkuvuudenhallinnan standardi. Kyberturvallisuuteen liittyvän lainsäädännön kehittyessä toimintaohjeita on haettu usein myös viranomaisten julkaisemista suosituksista tai oppaista. Kyberturvallisuuden toteuttamiseen liittyvien toimenpiteiden voidaankin sanoa olevan usein sekoitus teknologiatoimittajien ohjeistuksia, kansainvälisiä standardeja sekä viranomaisten ohjeistusta ja lainsäädännön muodostamia kriteeristöjä.

SFS-ISO 27001 on kansainvälinen standardi, jossa ohjeistetaan kattavasti tietoturvan hallintajärjestelmän vaatimuksista. Tietoturvan hallintajärjestelmän avulla pyritään suojaamaan tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Standardi koostuu vaatimuksista, jotka koskevat tietoturvan hallintajärjestelmän laatimista, ylläpitoa ja jatkuvaa parantamista. Vaatimukset on pyritty laatimaan niin, että kaikki organisaatiot niiden koosta tai toiminnan luonteesta riippumatta pystyvät soveltamaan niitä. (SFS-ISO 27001, 5.) Standardin uusin, vuonna 2022 julkaistu versio sisältää yhteensä 93 tietoturvallisuuden hallintakeinoa, jotka jakautuvat organisaatioon, henkilöstöön, fyysiseen turvallisuuteen ja teknologiaan liittyviin hallintakeinoihin (SFS-ISO 27001, 16–23). Tietotuvan hallintajärjestelmän sertifiointi SFS-ISO 27001 standardin mukaisesti on yleisesti käytetty tapa osoittaa organisaation sitoutumista tietoturvaan.

SFS-ISO 31000 on kansainvälinen riskienhallinnan standardi. Standardissa esitetään kaikentyyppisten riskien hallintaan soveltuva yleinen toimintamalli. Toimintamalli koostuu riskienhallinnan periaatteista, puitteista ja prosessista. Riskienhallinnan periaatteet kuvaavat vaikuttavan ja tehokkaan riskienhallinnan ominaisuuksia ja määrittelevät riskienhallinnan tarkoituksen ja tavoitteet. Riskienhallinnan puitteiden tarkoitus on auttaa organisaatiota yhdistämään riskienhallinta muuhun toimintaansa. Kuviossa 1 esitetty riskienhallinnan prosessi on johtamiseen ja päätöksentekoon sisältyvä iteratiivinen prosessi, joka auttaa organisaatiota toteuttamaan riskien hallintaa toiminnan eri tasoilla. (SFS-ISO 31000.)



Kuvio 1. Riskienhallinnan prosessi (tiedot: SFS-ISO 31000)

SFS-EN ISO 22301 on kansainvälinen jatkuvuudenhallinnan standardi, joka määrittelee periaatteet toiminnan jatkuvuuden hallintajärjestelmän toteuttamiselle ja ylläpidolle. Jatkuvuuden hallintajärjestelmän tavoitteena on valmistella organisaatiota häiriöiden aikaiseen toimintaan. Hallintajärjestelmä muodostuu organisaatioon kohdistuvien lakien, organisaation tuottamien palveluiden ja tuotteiden sekä toimialan vaatimusten perusteella. (SFS-EN ISO 22301, 5-6.) Jatkuvuuden hallintajärjestelmää voidaan hyödyntää kaikenlaisiin häiriöihin varauduttaessa, pitäen sisällään myös kyberturvallisuuden häiriöt.

Kyberturvallisuuteen liittyvää viranomaisohjeistusta ja käytäntöjä tuottaa Suomessa ja Euroopan Unionissa useampikin eri toimija. Sekä Liikenne- ja viestintävirasto Traficomin, Digi- ja väestötietoviraston, että Euroopan Unionin kyberturvallisuusviraston julkaisut toimivat osaltaan tietoperustana tämän työn tutkimusaiheille.

Liikenne- ja viestintävirasto Traficomin yhteydessä toimiva Kyberturvallisuuskeskus tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä sekä ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta. (Laki liikenne- ja viestintävirastosta 935/2018.)

Digi- ja väestötietovirasto kehittää julkisen hallinnon tietohallintoa, tietoturvallisuutta, digitaalisia palveluja ja sähköistä asiointia koskevia menetelmiä ja välineitä (Valtioneuvoston

asetus Digi- ja väestötietovirastosta 30.1.2020/53). Digi- ja väestötietovirasto vastaa muun muassa VAHTI-toiminnasta. VAHTI-verkoston työryhmien tehtävä on edistää digitaalisen turvallisuuden eri osa-alueita tuottamalla hyviä käytäntöjä, työkaluja ja mallipohjia, jotka auttavat organisaatioita kehittämään digiturvallisuuttaan. (Digi- ja väestötietovirasto 2023c.)

Euroopan unionin kyberturvallisuusvirasto, ENISA, on unionin virasto, jonka työn tarkoituksena on saavuttaa korkea kyberturvallisuuden taso koko EU:ssa. Virasto perustettiin vuonna 2004, ja sitä on myöhemmin vahvistettu EU:n kyberturvallisuusasetuksella. Euroopan unionin kyberturvallisuusvirasto osallistuu EU:n kyberpolitiikan laatimiseen, edistää tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien luotettavuutta kyberturvallisuuden sertifiointijärjestelmillä, tekee yhteistyötä jäsenvaltioiden ja EU:n elinten kanssa sekä auttaa EU:ta valmistautumaan tulevaisuuden kyberhaasteisiin. (ENISA 2023a.)

2.3 Cybersecurity framework -viitekehys

Yhdysvaltojen hallinnossa laadittiin vuonna 2014 presidentin määräyksestä kriittisen infrastruktuurin toimijoiden tueksi viitekehys, joka sisältää elementtejä sekä viittauksia keskeisistä tieto- ja kyberturvallisuuden standardeista ja kriteeristöistä helpottamaan näiden toimijoiden työtä tietoverkkojen ja tietojärjestelmien turvaamiseksi. Viitekehys on vuosien varrella kehittynyt akateemisen tutkimuksen, yritysten sekä julkisen sektorin yhteistyössä ja nykyään sitä hyödynnetään kansainvälisesti niin suuryritysten kuin useiden valtioidenkin toimesta. (National Institute of Standards and Technology 2023b.) Tästä syystä yhtenä tämän opinnäytetyön kannalta keskeisenä viitekehyksenä voidaan pitää Yhdysvaltain kansallisen standardisointi- ja teknologiainstituutin (National Institute of Standards and Technology, jatkossa myös NIST) laatimaa kyberturvallisuuden viitekehystä Cybersecurity Framework (jatkossa myös CSF-viitekehys). Kuviossa 2 on esitetty CSF-viitekehyksen avaintoiminnot.

Kuvio 2. CSF-viitekehyksen toiminnot (National Institute of Standards and Technology 2018).

CSF-viitekehys kokoaa yhteen käytäntöjä useasta eri standardista, joista huomionarvoisimpina on kappaleessa 2.2 esitelty SFS-ISO 27001 tietoturvallisuuden hallintajärjestelmästandardi, CIS-kontrollit sekä National Institute of Standards and Technology Special Publication 800–53. Vuonna 2000 Yhdysvalloissa perustetun voittoa tavoittelemattoman järjestön Center for Internet Securityn julkaisema CIS-kontrollit on priorisoitu ja yksinkertaistettu listaus hyviä käytäntöjä kyberturvallisuuden parantamiseen. CIS-kontrolleja kehitetään kollektiivisesti kyberturvallisuusalan asiantuntijoiden toimesta ja ne sisältävät ohjeistusta muun muassa järjestelmien turvallisesta konfiguroinnista (Center for Internet Security 2021). Alun perin Yhdysvaltain liittovaltion tietojärjestelmien yksityisyydensuoja- ja turvallisuusohjeistukseksi laadittu National Institute of Standards and Technology Special Publication 800–53-julkaisu on yksi laajimmista saatavilla olevista tieto- ja kyberturvallisuustoimenpiteiden katalogeista pitäen sisällään yhteensä yli 1000 hallintatoimenpidettä tieto- ja kyberturvallisuuden eri osa-alueille (National Institute of Standards and Technology 2020).

CSF-viitekehystä hyödynnetään myös muun muassa Suomessa julkisen hallinnon digitaalisen turvallisuuden arkkitehtuurin pohjana. Viitekehys koostuu viidestä kyberturvallisuuden avaintoiminnosta: tunnistaminen (*identify*), suojautuminen (*protect*), havainnointi (*detect*), reagointi (*respond*) ja palautuminen (*recover*). Toiminnot jakautuvat viitekehyksessä useampaan kategoriaan sekä näihin kategorioihin kuuluviin yksityiskohtaisempiin toimenpiteisiin. (Digi- ja väestötietovirasto 2022a.)

CSF-viitekehyksen viisi toimintoa jakautuvat yhteensä 23 kategoriaan, jotka on listattu kuviossa 3. Yksittäiset toimenpiteet on luokiteltu hienojakoisesti kategorioiden alle siten, että ylätasolla CSF-viitekehys muodostaa helposti ymmärrettävän kokonaisuuden

kyberturvallisuuden vaatimien toimenpiteiden aihealueista. Aihealueita ovat esimerkiksi IT-omaisuudenhallinta (*asset management*) ja suojausteknologiat (*protective technology*).

Function	Category
IDENTIFY (ID)	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
PROTECT (PR)	Identity Management, Authentication and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
DETECT (DE)	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND (RS)	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
RECOVER (RC)	Recovery Planning
	Improvements
	Communications

Kuvio 3. Kyberturvallisuustoimenpiteiden jaottelu CSF-viitekehyksessä (tiedot: National Institute of Standards and Technology 2018).

Kuviossa 4 on esitetty esimerkinomaisesti kaksi viitekehyksen sisältämää yksittäistä toimenpidettä. Kaikkien viitekehyksen toimenpiteiden esittely ei ole tarkoituksenmukaista, sillä lukija voi tutustua niihin tarkemmin perehtymällä lähdeaineistoon. Kuviossa 4 esitetyt toimenpiteet kuuluvat suojautuminen (*protect)* -toimintoon kuuluvaan tiedon suojaus (*data security)* -kategoriaan. Esimerkin toimenpiteet liittyvät tiedon suojaamiseen tallennettuna (PR.DS-1) ja siirrettäessä (PR.DS-2). Kukin kategoria sisältää lyhyen kuvauksen siitä, miksi toimenpiteiden

toteuttaminen on tärkeää sekä yksityiskohtaisemmat toimintaohjeet sekä kattavan luettelon viittauksista muihin standardeihin, kuten SFS-ISO 27001:een.

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	**CIS CSC** 13, 14 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12

Kuvio 4. Esimerkki Data Security -kategoriaan kuuluvista toimenpiteistä (tiedot: National Institute of Standards and Technology 2018).

Viitekehys sisältää yhteensä 5 toimintoa, jotka jakautuvat 23 kategoriaan (kuvio 3). Kategoriat jakautuvat yhteensä 108 kuvion 4 tyyppiseen toimenpiteeseen. Vaikka viitekehyksen ei olekaan tarkoitus olla täydellinen luettelo kaikista mahdollisista kyberturvallisuutta parantavista toimenpiteistä, muodostaa se hyvän pohjan organisaation omien tavoitteiden ja tarpeiden yhdistämisen relevantteihin toimenpiteisiin sekä muihin alan hyviin käytäntöihin ja standardeihin.

3 Tutkimuksen toteuttaminen

Opinnäytetyö on tutkimuksellinen ja sen ensisijaisena tutkimusmenetelmänä toimii sisällönanalyysi. Opinnäytetyössä käytiin sisällönanalyysin avulla läpi uuden kyberturvallisuusdirektiivin varsinainen sisältö, siihen olennaisesti liittyvät taustamateriaalit sekä muita direktiiviin liittyviä artikkeleita. Sisällönanalyysin avulla työssä pyrittiin löytämään vastaus kahteen ensimmäiseen tutkimuskysymykseen, eli siihen mitä toimijoita uusi direktiivi koskettaa ja millaisia vaatimuksia direktiivi pitää sisällään.

Kolmanteen tutkimuskysymykseen, eli siihen, millaisilla keinoilla organisaatiot voivat täyttää direktiivin vaatimuksia, vastatiin pohtimalla konkreettisia toimenpiteitä CSF-viitekehyksen ja muun relevantin tieto- ja kyberturvallisuuteen liittyvän tietoperustan pohjalta.

3.1 Sisällönanalyysi menetelmänä

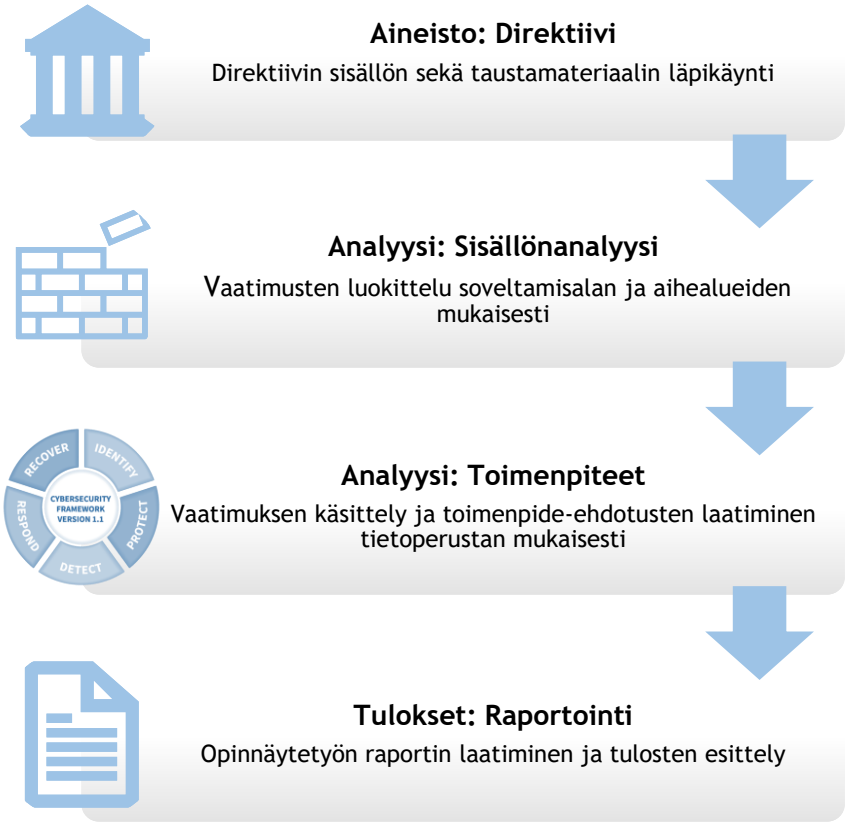
Sisällönanalyysi on laadullisen tutkimuksen menetelmä, jonka avulla voidaan analysoida dokumentteja systemaattisesti ja objektiivisesti (Tuomi & Sarajärvi 2018, 117.). Koska tässä opinnäytetyössä analysoitu materiaali koostuu yksinomaan dokumenttimuotoisista tekstiaineistoista, oli sisällönanalyysin valikoituminen laadullisen tutkimuksen menetelmäksi luontevaa.

Laadullista tutkimusta voidaan toteuttaa kolmella toisistaan erilaisella menetelmällä, jotka ovat aineistolähtöinen analyysi, teoriaohjaava analyysi ja teorialähtöinen analyysi. Aineistolähtöisessä analyysissä pyritään luomaan tutkimusaineistosta teoreettinen kokonaisuus, jolloin aikaisemmin tutkitulla tiedolla ei pitäisi olla merkitystä analyysin lopputuloksen kanssa. Teorialähtöinen analyysi sen sijaan nojaa johonkin tiettyyn aiemmin laadittuun malliin tai teoriaan, jolloin aineistoa käsitellään yksinomaan valitun teorian ehdoilla. Teoriaohjaava analyysimenetelmä yhdistelee kumpaakin edellä mainittua menetelmää siten, että aikaisemmin tutkittu tieto tai teoria voi toimia analyysin apuna, mutta analyysi ei pohjaudu suoraan teoriaan. (Tuomi & Sarajärvi 2018, 108–112.)

Koska tämän opinnäytetyön tutkimuskysymysten kannalta sekä itse aineisto, että aikaisemmin tuotettu tieto ovat hyvin keskeisessä roolissa, mainituista analyysimuodoista teoriaohjaava sisällönanalyysi soveltuu tämän opinnäytetyön menetelmäksi erityisen hyvin. Teoriaohjaavassa analyysissä pyritään yhdistelemään aikaisempaa tietoperustaa rajoittamatta kuitenkaan liikaa aineiston tulkintaa tiettyyn teoriaan. Teoriaohjaava analyysimuoto mahdollistaa sen, että analyysiyksiköt, eli analyysin kohteet ja teemat valitaan aineistosta, mutta teoria tai aiheesta aikaisemmin tuotettu tieto auttaa analyysin tekemisessä. (Tuomi & Sarajärvi 2018, 109). Voikin todeta, että analyysin tarkoituksena on kytkeä aikaisemmin tuotettu tieto, menetelmät ja mallit direktiivin vaatimuksiin ja siten tuottaa helposti hyödynnettävää valmista aineistoa vaatimusten täyttämisen tueksi.

3.2 Tutkimusprosessi

Varsinaisen tutkimusprosessin kulkua voidaan kuvata järjestelmällisesti jakamalla prosessi neljään eri vaiheeseen (kuvio 5); aineiston läpikäyntiin (1), sisällönanalyysiin (2), vaatimusten analysointiin ja toimenpidesuositusten laatimiseen (3) sekä tutkimuksen tulosten ja johtopäätösten raportointiin (4).



Kuvio 5. Tutkimusprosessi

Pääasiallisena tutkittavana aineistona opinnäytetyössä toimi Euroopan Unionin uusi kyberturvallisuusdirektiivi (Direktiivi 2022/2555/EU). Direktiivi koostuu johdanto-osasta, artiklaosasta sekä liitteistä. Johdanto-osassa esitetään perustelut säännöksille, artiklaosa sisältää varsinaiset säännökset ja liitteet sisältävät teknistä tai muuta lisätietoa säännöksiin liittyen. Ensimmäisessä vaiheessa koko aineisto luettiin läpi poimien samalla tutkimuskysymysten kannalta erityisen merkityksellisiltä vaikuttavia teemoja. Tässä vaiheessa ei vielä kuitenkaan toteutettu varsinaista sisällönanalyysiä, vaan tutustuttiin aineistoon.

Analyysivaiheessa aineistosta eroteltiin ensimmäisenä direktiivin varsinaiset säännökset, eli artiklat, sekä soveltamisalaan liittyvät määritteet direktiivin liitteistä. Artikloja direktiivissä on yhteensä 46 kappaletta. Artiklojen ja soveltamisalan erottelu muusta aineistosta tarjosi pohjan jatkoluokittelulle. Teoriaohjaavan sisällönanalyysin mukaisesti seuraavassa vaiheessa kaikki artiklat luokiteltiin yksitellen soveltamisalan mukaisiin luokkiin, jotta aineistosta saatiin erotettua opinnäytetyön rajausten mukaisesti analyysin ulkopuolelle jätettävät vaatimukset. Soveltamisaloittain luokittelu helpotti myös myöhempää toimenpiteiden tarkastelua, sillä erityyppisille kohdeorganisaatioille oli direktiivissä hieman erilaisia vaatimuksia. Tässä vaiheessa artiklat oli listattu ja kunkin artiklan kohdalta oli määritetty sen soveltamisala, eli mitä kohderyhmää se koskee. Aineiston 46 artiklasta tunnistettiin yhteensä 19 artiklaa, jotka

koskevat tärkeitä tai keskeisiä toimijoita ja ovat näin ollen tutkimuksen kannalta relevantteja. Näistä erityisesti artikla 21, otsikoltaan kyberturvallisuusriskien hallintatoimenpiteet, pitää sisällään merkittävän määrän toimijoita koskevia vaatimuksia.

Tämän jälkeen artiklat luokiteltiin aineiston ja tietoperustassa esitetyn viitekehyksen avulla aihealueiden mukaisesti pääluokkiin ja alaluokkiin. Pääluokat muodostuivat suoraan aineistosta tunnistettujen aihealueiden mukaan, kuten esimerkiksi tietojenvaihto, raportointivelvoitteet ja kyberturvallisuusriskien hallintatoimenpiteet. Lisäksi artiklat luokiteltiin alaluokkiin aiemmin esitellyn CSF-viitekehyksen sisältämien luokitusten perusteella. Tämä tehtiin, jotta aineiston artiklat olisivat helpommin yhdistettävissä relevanttiin tietoperustaan toimenpide-ehdotuksia laadittaessa. Kuviossa 6 on esitetty aineiston luokittelussa käytetyt määritykset artiklojen 23 ja 24 osalta.

Artikla (numero)	Artikla (otsikko)	Soveltamisala	Pääluokka	Alaluokka 1 (Viitekehys)	Alaluokka 2 (Viitekehys)
23	Raportointi-velvoitteet	Keskeiset ja tärkeät toimijat	RAPORTOINTIVELVOITTEET	REAGOINTI	Tietoturvatiedon jakaminen ja viestintä
24	Eurooppalaisten kyber-turvallisuuden sertifiointi-järjestelmien käyttö	Keskeiset ja tärkeät toimijat	KYBERTURVALLISUUSRISKIEN HALLINTATOIMENPITEET JA RAPORTOINTIVELVOITTEET	TUNNISTAMINEN	Toimitusketjujen hallinta

Kuvio 6. Esimerkki aineiston luokittelusta

Luokittelun jälkeen direktiivin artiklat muodostivat selkeitä asiakokonaisuuksia, joihin oli kohtalaisen yksinkertaista hakea tietoperustan mukaisia toimenpide-ehdotuksia ja toteutusmalleja aikaisemmin tuotetun tiedon pohjalta. Erityisesti CSF-viitekehys toimi erinomaisena työkaluna vaatimusten ja kansainvälisesti tunnettujen standardien sekä muun tietoperustan yhteensovittamisessa.

Opinnäytetyön tulokset on esitetty tämän raportin luvuissa 4 ja 5 mahdollisimman havainnollistavassa ja helppolukuisessa muodossa. Luvussa 4 vastataan ensimmäiseen tutkimuskysymykseen käymällä läpi direktiivin soveltamisala, eli ne toimialat ja organisaatiot, joita direktiivin vaatimukset koskevat. Luvussa 5 vastataan toiseen ja kolmanteen tutkimuskysymykseen. Luvussa on esitetty opinnäytetyön rajaukset huomioiden muita toimijoita kuin jäsenvaltioita tai toimivaltaisia viranomaisia koskevat vaatimukset. Luku sisältää lisäksi yleisellä tasolla esitettyjä konkreettisia, tietoperustaan pohjautuvia toimenpide-ehdotuksia kunkin vaatimuksen täyttämiseksi.

4 Direktiivin soveltamisala

Tässä luvussa vastataan ensimmäiseen tutkimuskysymykseen, eli siihen millaisia organisaatioita uusi kyberturvallisuusdirektiivi koskee. Luvussa taulukkomuotoisena esitelty soveltamisala saatiin selville yhdistelemällä tiedot sekä direktiivin artikloista, liitteistä, että muista soveltamisalaan liittyvistä säädöksistä.

Toimialat ja organisaatiot, joita direktiivi koskee, määritellään artikloissa kaksi ja kolme sekä direktiivin ensimmäisessä ja toisessa liitteessä. Toimialat on esitetty direktiivin liitteissä, joskin joidenkin toimialojen osalta tarkempia määrityksiä löytyy myös muualta Euroopan Unionin lainsäädännöstä. Organisaation kokoluokkaan liittyvät kynnysarvot on esitetty Euroopan Unionin suosituksessa 2003/361/EY mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä.

Toimijat jaetaan direktiivissä kahteen luokkaan: keskeisiin ja tärkeisiin toimijoihin, joita käsitellään hieman eri tavalla erityisesti toimivaltaisen viranomaisen suorittamien tarkastusten ja direktiivin rikkomisesta määräytyvien sanktioiden osalta. Direktiivin asettamat velvoitteet ovat kuitenkin pääsääntöisesti samat kummallekin toimijaryhmälle. Keskeisiin tai tärkeisiin toimijoihin jako tapahtuu pääsääntöisesti siten, että ensimmäisen liitteen mukaisesti erittäin kriittisillä toimialoilla toimivat organisaatiot ovat keskeisiä toimijoita ja toisen liitteen mukaisesti muilla kriittisillä toimialoilla toimivat organisaatiot ovat tärkeitä toimijoita. Keskeisten ja tärkeiden toimijoiden määrittelyssä on kuitenkin muutamia poikkeuksia, joten direktiivin liitteet eivät toimi sellaisenaan listauksina organisaatioiden luokittelussa. (Direktiivi 2022/2555/EU, artikla 3.)

Ensimmäinen olennainen poikkeus liitteiden mukaisesta keskeisten ja tärkeiden toimijoiden luokittelussa on organisaation koko. Organisaatiot luokitellaan niiden kokoluokan perusteella siten, että kynnysarvoissa otetaan huomioon organisaation henkilöstömäärä ja liikevaihto tai taseen loppusumma komission aiemmin antaman suosituksen 2003/361/EY mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä (EUVL L 124, 20.5.2003, s. 36) mukaisesti:

> ”Tätä direktiiviä sovelletaan liitteissä I ja II tarkoitettua toimijatyyppiä oleviin julkisiin ja yksityisiin toimijoihin, jotka täyttävät suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset tai ylittävät kyseisen artiklan 1 kohdassa säädetyt keskisuurten yritysten määrittelyssä käytettävät kynnysarvot ja jotka tarjoavat palvelujaan tai harjoittavat toimintaansa unionissa.” (Direktiivi 2022/2555/EU, artikla 2.)

Direktiiviä sovelletaan kuitenkin kriittisten toimijoiden häiriönsietokyvystä annetussa ns. CER-direktiivissä (Direktiivi 2022/2557/EU) kriittisiksi määritettyihin toimijoihin sekä verkkotunnusten rekisteröintipalveluja tarjoaviin toimijoihin niiden koosta riippumatta. Lisäksi

jäsenvaltiot voivat määrittää itsenäisesti yksittäisiä toimijoita, joihin direktiivin velvoitteita sovelletaan toimijan koosta riippumatta, mikäli toimijan katsotaan olevan yhteiskunnallisesti merkittävässä asemassa. (Direktiivi 2022/2555/EU, artikla 2.) Taulukossa 1 on listattu kumpaankin luokkaan kuuluvat toimialat.

Keskeiset toimijat	Tärkeät toimijat
Organisaatiot, joiden: - palveluksessa on yli 250 työntekijää ja - vuosiliikevaihto on yli 50 miljoonaa euroa, tai taseen loppusumma on yli 43 miljoonaa euroa sekä - Toimiala on jokin seuraavista:	Organisaatiot, joiden: - palveluksessa on yli 50 työntekijää ja - vuosiliikevaihto on yli 10 miljoonaa euroa, tai taseen loppusumma on yli 10 miljoonaa euroa sekä - Toimiala on jokin seuraavista:
Energia	Energia
Liikenne	Liikenne
Pankkitoiminta	Pankkitoiminta
Finanssimarkkinat	Finanssimarkkinat
Terveys	Terveys
Juomavesi	Juomavesi
Jätevesi	Jätevesi
Tieto- ja viestintäteknologian hallinta	Tieto- ja viestintäteknologian hallinta
Julkishallinto	Julkishallinto
Avaruus	Avaruus
CER-direktiivin (EU 2022/2557) mukaiset kriittiset toimijat	Digitaalinen infrastruktuuri
Digitaalinen infrastruktuuri - luottamuspalvelun tarjoajat, aluetunnusrekisterit ja DNS-palveluntarjoajat niiden koosta riippumatta - yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat, joiden palveluksessa on yli 50 työntekijää ja liikevaihto on yli 10 miljoonaa	Posti- ja kuriiripalvelut
	Jätehuolto
	Kemikaalien valmistus, tuotanto ja jakelu
	Elintarvikkeiden tuotanto, jalostus ja jakelu
	Valmistus
	Digitaalisten palveluiden tarjoajat
	Tutkimustoiminta

Taulukko 1. Keskeiset ja tärkeät toimijat kokoluokan ja toimialan mukaan, (tiedot: Direktiivi 2022/2555/EU)

Jäsenvaltiot voivat myös erikseen säätää, että direktiivin asettamia velvoitteita sovelletaan myös paikallistason julkishallinnon toimijoihin sekä opetus- ja koulutusalan laitoksiin, jotka eivät lähtökohtaisesti kuulu direktiivissä määritettyihin toimialoihin. (Direktiivi 2022/2555/EU, artikla 2.)

Kuten taulukosta 1 on havaittavissa, direktiiviä sovelletaan varsin useaan eri toimialaan. Soveltamisalan ulkopuolelle jää kuitenkin myös joitain suuria toimialoja kuten esimerkiksi rakentaminen sekä matkailu- ja ravintolatoimialat. Kokoluokkaan perustuvalla määrittelyllä eritellään usean toimialan osalta keskeiset ja tärkeät toimijat, mutta käytännössä direktiivin velvoitteet ovat hyvin samankaltaiset kummallekin kohderyhmälle. Suurimmat erot keskeisten ja tärkeiden toimijoiden osalta ovat valvonnan toteuttamisessa ja mahdollisten hallinnollisten sanktioiden määrässä. Luvussa 5 käsitellään tarkemmin näille toimijoille asetettuja velvoitteita ja niiden vaatimia toimenpiteitä.

5 Direktiivin velvoitteet ja niiden vaatimat toimenpiteet

Tässä luvussa vastataan jäljellä oleviin kahteen tutkimuskysymykseen, eli siihen millaisia vaatimuksia direktiivi sisältää ja millaisin konkreettisin toimenpitein organisaatiot voivat täyttää vaatimukset. Vaatimukset on esitetty luvun leipätekstissä ja tietoperustaan pohjautuvat toimenpide-ehdotukset vaatimusten toteuttamiseksi on selkeyden vuoksi erotettu muusta tekstistä sijoittamalla ne kuvioiden sisään.

Keskeisenä direktiivin tavoitteena on yhtenäistää kyberturvallisuuden korkea taso Euroopan Unionin jäsenvaltioiden kesken. Tämän tavoitteen toteuttamiseksi direktiivissä säädetään seuraavista velvoitteista (EU 2022/2555, artikla 1.):

- jäsenvaltioiden velvoitteet kyberturvallisuusstrategioista sekä toimivaltaisten viranomaisten nimeämisestä
- kyberturvallisuusriskien hallintatoimenpiteet ja raportointivelvoitteet,
- kyberturvallisuustietojen jakamista koskevat velvoitteet sekä
- jäsenvaltioiden valvonta- ja täytäntöönpanovelvoitteet.

Direktiivin sisältämät velvoitteet voidaan luokitella ensisijaisesti sen perusteella, mitä tahoa tai kohderyhmää kyseinen velvoite koskee. Velvoitteita kohdistuu pääasiallisesti joko kansalliselle toimivaltaiselle viranomaiselle, jäsenvaltiolle itselleen tai keskeisille ja tärkeille toimijoille. Tässä opinnäytetyössä käsitellään rajausten mukaisesti vain luvussa 4 esitetyille tärkeille ja keskeisille toimijoille asetettuja velvoitteita.

Direktiivi sisältää keskeisiä ja tärkeitä toimijoita koskevia vaatimuksia organisaation toiminnan ja toimintaympäristön tunnistamisesta, kyberturvallisuusriskien hallintatoimenpiteistä,

poikkeamien raportoinnista, toimijoiden rekistereistä, tietojenvaihdosta sekä valvonnasta ja täytäntöönpanosta (Direktiivi 2022/2555/EU). Teoriaohjaavan sisällönanalyysin menetelmien mukaisesti direktiivin vaatimukset ja niiden tarvitsemat toimenpiteet voidaankin luokitella mukailemalla edellä mainittuja aihealueita. Kappaleen 5 otsikointi noudattaa tätä luokittelua ja tietoperustaan pohjautuvat toimenpiteet on esitetty kunkin alaotsikon alla olevissa kuvioissa.

5.1 Organisaation toiminnan ja toimintaympäristön tunnistaminen

Koska direktiivi nojaa vahvasti tunnistettuihin riskeihin perustuviin kyberturvallisuustoimenpiteisiin, on looginen ensimmäinen askel näiden toimenpiteiden toteuttamiseksi organisaation oman toimintaympäristön, toimialan sekä toiminnan kannalta tärkeiden tietojärjestelmien ja -verkkojen sekä toimitusketjujen ja sidosryhmien tunnistaminen.

Organisaation on määriteltävä ensinnäkin se, kuuluuko se ylipäätään direktiivin soveltamisalaan. Mikäli organisaatio kuuluu direktiivin soveltamisalaan, sen on kartoitettava, kuuluuko se direktiivin määrittelemiin keskeisiin vai tärkeisiin toimijoihin. Tätä määritystä tehdessä olennaisinta on tunnistaa, millä kriittisillä toimialoilla organisaatio toimii sekä organisaation kokoluokka, joka vaikuttaa olennaisesti siihen, kumpaan luokkaan organisaatio kuuluu. Direktiivin soveltamisalaa ja keskeisten sekä tärkeiden toimijoiden luokkia esitellään tarkemmin tämän opinnäytetyön luvussa 4.

Tämän lisäksi organisaation on tunnistettava minkä Euroopan Unionin jäsenmaan lainkäyttövaltaan organisaatio kuuluu. Lainkäyttövalta direktiivin osalta perustuu määrityksiin siitä, missä maassa organisaation päätoimipaikka on ja siihen, missä maassa se tarjoaa palvelujaan. (Direktiivi 2022/2555/EU, artikla 26.) Kuviossa 7 on listattu olennaisia apukysymyksiä, jotka auttavat organisaatiota tunnistamaan kuuluuko se direktiivin soveltamisalaan.

Apukysymykset soveltamisalan sekä toimijatyypin tunnistamiseksi liittyen artikloihin 2 ja 3.
1. Millä toimialalla organisaatio toimii? 2. Kuuluuko toimiala direktiivin soveltamisalaan? 3. Onko organisaatio direktiivin määrittelemä keskeinen vai tärkeä toimija? 4. Minkä Euroopan Unionin jäsenmaan lainkäyttövaltaan organisaatio kuuluu? 5. Velvoittaako muu toimialakohtainen Euroopan Unionin tai kansallinen lainsäädäntö kyberturvallisuustoimenpiteiden toteuttamista? 6. Mikä on organisaation asema kriittisten toimialojen toimitusketjussa?

Kuvio 7. Soveltamisala sekä keskeiset ja tärkeät toimijat

Toimintaympäristöä tunnistettaessa, organisaation on lisäksi otettava huomioon alakohtaiset unionin tai jäsenmaan kansalliset säädökset. Jos alakohtaisissa säädöksissä määritetään kyberturvallisuuteen liittyviä toimenpiteitä, joiden vaikutukset vastaavat vähintään tätä direktiiviä, tässä direktiivissä olevia säännöksiä ei sovelleta. Sen sijaan sovelletaan alakohtaisia säädöksiä. (Direktiivi 2022/2555/EU, artikla 4.)

5.2 Kyberturvallisuusriskien hallintatoimenpiteet

Direktiivin edellyttämät kyberturvallisuusriskien hallintatoimenpiteet sisältävät laajalti käytännön toimenpiteitä, jotka toimijoiden tulisi toteuttaa kyberturvallisuuden varmistamiseksi. Toimenpiteet sisältävät niin hallinnollisia, operatiivisia kuin teknisiäkin menettelyitä, jotka toteuttamalla toimijat parantavat omaa kyberturvallisuuttaan ja samalla edesauttavat korkean kyberturvallisuuden tason saavuttamista koko Euroopan Unionin alueella.

Direktiivi velvoittaa kyberturvallisuusriskeihin liittyvien asioiden käsittelyn organisaatioiden hallintoelinten tasolla. Tämä tarkoittaa sitä, että esimerkiksi osakeyhtiöiden tapauksessa yhtiön hallituksen tulisi käsitellä ja hyväksyä kyberturvallisuusriskien hallintatoimenpiteet. (Direktiivi 2022/2555/EU, artikla 20.)

Tarve nostaa kyberturvallisuuteen liittyvät asiat organisaation hallintoelinten tasolle on todettu myös Liikenne- ja viestintävirasto Traficomin julkaisemassa Kyberturvallisuus ja yrityksen hallituksen vastuu -oppaassa. Oppaan mukaan yrityksessä hallituksen keskeinen tehtävä on edistää yhtiön etua ja siksi sen jäsenillä on oltava riittävät tiedot myös kyberturvallisuudesta ja siihen liittyvistä liiketoimintariskeistä. (Liikenne ja viestintävirasto Traficom 2020a.) Kyseinen opas toimii myös erinomaisena koulutus- ja tukimateriaalina hallintoelimissä toimiville henkilöille asiaan perehtymisessä. Kuviossa 8 on listattu toimenpiteitä hallinnoinnin toteuttamiseksi organisaatioissa.

Toimenpiteet hallinnoinnin toteuttamiseksi liittyen artiklaan 20
Organisaatioiden hallintoelinten jäsenten on hyväksyttävä riskienhallintatoimenpiteet. Hallintoelinten jäsenten on lisäksi osallistuttava riskienhallinnan ja kyberturvallisuuden koulutukseen. 1. Hallintoelinten tulisi hyväksyä organisaation riskienhallintakäytännöt. Riskienhallintakäytännöt tulisi katselmoida ja hyväksyä uudelleen säännöllisin väliajoin esimerkiksi vuosittain, tai mikäli käytäntöihin tulee muutoksia. 2. Hallintoelinten tulisi hyväksyä tunnistetut riskit ja niiden hallintatoimenpiteet säännöllisesti ja hyväksynnästä tulisi muodostaa kirjallinen dokumentaatio. Hallintoelimen tulisi ottaa kyberturvallisuusriskien tarkastelu ja toimenpiteiden hyväksyntä osaksi vuosikellon mukaista työjärjestystä siten, että kyberturvallisuusriskit käsiteltäisiin osana normaalia kokousagendaa esimerkiksi neljännesvuosittain. 3. Hallintoelinten jäsenille tulisi järjestää koulutusta kyberturvallisuusriskeistä ja säilyttää todistus koulutuksen suorituksesta. Yksi tapa koulutuksen järjestämiseen on laatia tai ottaa käyttöön valmis verkkokurssi, jossa avataan kyberturvallisuuden ja riskienhallinnan perusteita sekä organisaation toimintaan liittyviä yleisimpiä kyberturvallisuusuhkia. Tätä samaa koulutusta voi hyödyntää myös muun henkilöstön koulutuksessa.

Kuvio 8. Toimenpiteet hallinnoinnin toteuttamiseksi

Varsinaisten kyberturvallisuusriskien hallintatoimenpiteiden osalta direktiivin 21 artiklassa listataan suuri joukko toimenpiteitä, joilla kyberturvallisuutta voidaan parantaa, määrittelemättä kuitenkaan tarkemmin millä tavoin nämä toimenpiteet tulisi toteuttaa. Direktiivissä velvoitetaan organisaatiot suunnittelemaan ja toteuttamaan toimenpiteet sekä laatimaan dokumentoidut politiikat ja toimintaohjeet:

- riskienhallinnasta,
- tietojärjestelmien turvallisuudesta,
- poikkeamien käsittelystä,
- jatkuvuudenhallinnasta,
- toimitusketjujen turvallisuudesta,
- hankintojen, kehittämisen ja ylläpidon turvallisuudesta,
- haavoittuvuuksienhallinnasta,
- kryptografian ja salauksen käytöstä,
- henkilöstöturvallisuudesta,
- pääsynhallinnasta,

- omaisuudenhallinnasta sekä
- suojattujen viestintä- ja hätäviestijärjestelmien käytöstä.

Tämän lisäksi organisaation tulee arvioida säännöllisesti näiden toimenpiteiden tehokkuutta. Uhka- ja riskiarvioon pohjautuen organisaation itsensä harkittavaksi jää, millaiset ovat heidän kannaltaan oikeasuhtaiset kyberturvallisuusriskien hallintatoimenpiteet. (Direktiivi 2022/2555/EU, artikla 21.) Kuten edeltävästä listasta voi huomata, artikla 21 sisältää toimenpiteitä huomattavan monesta eri aihealueesta. Näihin aihealueisiin liittyvät toimenpiteet on esitelty kukin omissa kuvioissaan 9-21.

Riskienhallinnassa on yksinkertaisimmillaan kyse epävarmojen tapahtumien ennakoinnista ja näihin tapahtumiin varautumisesta. Riskienhallinnan toteuttamiseen on kehitetty lukuisia eri malleja, joista yksi tunnetuimmista on SFS-ISO 31000 standardiin perustuva malli. Riskienhallinta on kyseisen standardin mukaan koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta (SFS ISO 31000, 6).

Riskienhallintapolitiikka määrittelee organisaation tavat tunnistaa, analysoida, arvioida ja käsitellä riskejä. Kyberturvallisuusriskit eivät muodosta poikkeusta muista organisaation kohtaamista riskeistä, joten organisaation ei ole syytä laatia kyberturvallisuusriskeihin liittyviä käytäntöjä erikseen muusta riskienhallinnasta. Myös kyberturvallisuusriskien käsittely tulisi olla osa organisaation yleistä ja säännöllistä riskienhallintaa. Kuviossa 9 on esitetty toimenpiteitä SFS-ISO 31000 standardin mukaisen riskienhallinnan toteuttamiseen.

Toimenpiteet riskienhallinnan toteuttamiseksi liittyen artiklaan 21
Organisaatio voi toteuttaa riskienhallintaa SFS-ISO 31000 standardin mukaisesti, jossa kuvattu varsinainen riskienhallintaprosessi koostuu kolmesta vaiheesta: 1. Riskienhallinnan kattavuuden, toimintaympäristön ja kriteerien määrittäminen 2. Riskien arviointi, joka pitää sisällään: a. Uhkien sekä riskien tunnistamisen, jota tulisi toteuttaa säännöllisesti ja aina, kun tietojärjestelmissä tai -verkoissa tapahtuu laajoja muutoksia. b. Riskianalyysin, jossa arvioidaan tunnistettujen riskien todennäköisyyttä ja vaikutuksia. c. Riskien merkityksen arvioinnin, jossa arvioidaan, onko riskin pienentämiseksi syytä tehdä toimenpiteitä tai onko kyseistä riskiä syytä tarkastella tarkemmin. 3. Riskien käsittely, jonka tarkoituksena on valita ja toteuttaa ne hallintatoimenpiteet, jotka lieventävät negatiivisen tapahtuman todennäköisyyttä tai vaikutusta Tämän lisäksi prosessia tukee riittävä viestintä ja tiedonvaihto, säännöllinen riskien seuranta ja katselmointi sekä riskienhallinnasta syntyvät tallenteet ja raportointi, eli niin kutsutun riskirekisterin ylläpito. (SFS ISO 31000, 14.) Kyberturvallisuuteen liittyviin riskeihin vaikuttaa usein järjestelmissä, palveluissa ja sovelluksissa olevat haavoittuvuudet. Tunnistetut haavoittuvuudet tulisikin dokumentoida ja niistä sekä tiedonvaihtoverkostoista ja muista lähteistä kerättyä uhkatietoa tulisi käyttää riskien tunnistamisen apuna (National Institute of Standards and Technology 2018, 26–27).

Kuvio 9. Toimenpiteet riskienhallinnan toteuttamiseksi

Tietojärjestelmien turvallisuuteen liittyvät toimintamallit sekä hallintakeinot riippuvat yleensä hyvin paljon tietojärjestelmän tyypistä ja toteutustavasta. Organisaation tulisi kuitenkin määritellä yleisesti sovellettava vähimmäistaso tietojärjestelmien turvallisuudelle laatimalla esimerkiksi järjestelmien yleiset tietoturvavaatimukset. Kunkin tietojärjestelmän kohdalla turvallisuuden tarkastelua tulee lisäksi tehdä riskiperusteisesti ottamalla huomioon muun muassa kyseisen tietojärjestelmän kriittisyys ja toimitusketjut. Kuviossa 10 on esitetty muutamia oleellisia tietojärjestelmien turvallisuuteen liittyviä kontrolleja ja kriteeristöjä.

Toimenpiteet tietojärjestelmien turvallisuuden toteuttamiseksi liittyen artiklaan 21
Tietoturvavaatimuksia voi toteuttaa esimerkiksi hyödyntämällä olemassa olevia kriteeristöjä tai listauksia turvallisuuskontrolleista organisaation omien vaatimusten mukaisesti. Tällaisia listauksia on lukuisia, joista muutamia esimerkkejä ovat: • CIS-turvallisuuskontrollit (Center for Internet Security 2021), • Pilvipalveluiden turvallisuuskontrollien katalogi CCM (Cloud Security Alliance 2021), • Web-pohjaisten sovellusten turvallisuuteen liittyvät OWASP-viitekehykset ja -kontrollit (The Open Worldwide Application Security Project 2023) sekä • Julkisen hallinnon tietoturvallisuuden arviointikriteeristö Julkri (Valtiovarainministeriö 2022). Lisäksi eri toimialoilla, kuten esimerkiksi terveydenhoitoalalla, saattaa olla myös velvoittavia alakohtaisia kriteeristöjä tiettyihin käyttötapauksiin liittyen.

Kuvio 10. Toimenpiteet tietojärjestelmien turvallisuuden toteuttamiseksi

Poikkeamien hallinta muodostaa keskeisen osan kyberturvallisuutta. Vaikka tietojärjestelmät ja -verkot suojattaisiin kattavasti ja tehokkaasti, on silti mahdollista, että organisaatio joutuu kyberhyökkäyksen kohteeksi. Tietoturvayhtiö Check Pointin mukaan kyberhyökkäykset lisääntyivät vuonna 2022 maailmanlaajuisesti yli kolmanneksella verrattuna edeltävään vuoteen, eikä ole odotettavissa, että tämä trendi taittuisi laskuun (Check Point 2023).

Poikkeamalla tarkoitetaan toki muutakin kuin suoranaisen kyberhyökkäyksen aiheuttamaa häiriötä. Kyberturvallisuuspoikkeama voi olla mikä tahansa tapahtuma, joka vaarantaa verkko- ja tietojärjestelmien saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Kuviossa 11 on lueteltu keskeisiä toimenpiteitä poikkeamien hallinnan toteuttamiseksi.

Toimenpiteet poikkeamien hallinnan toteuttamiseksi liittyen artiklaan 21
CSF-viitekehyksen mukaisesti poikkeaman hallinta koostuu poikkeamien havaitsemisesta, poikkeamiin reagoinnista ja poikkeamista palautumisesta (National Institute of Standards and Technology 2018, 7–8): 1. Poikkeamien hallinta tulee organisoida ja siihen liittyvät roolit ja vastuut on määritettävä etukäteen. Poikkeaman hallinnan periaatteet ja organisoituminen on hyvä kirjata erilliseen poikkeamien hallinnan suunnitelmaan. Mikäli roolit ja toimintamalli ei ole poikkeaman sattuessa selvät, vaikeutuu poikkeaman käsittely huomattavasti. 2. Poikkeamien havaitsemiseen tarvitaan useimmiten teknisiä ja operatiivisia toteutuksia kuten esimerkiksi tietoturvavalvomoa ja valvontaan tarkoitettuja teknologioita, kuten verkkolaitteiden valvontaa, päätelaitteiden valvontaa ja järjestelmien lokitietoja. Myös henkilöstön tekemät ilmoitukset ovat tärkeässä roolissa poikkeamien havaitsemisessa. Poikkeamien havaitsemiseen liittyviä menettelyjä tulisi myös testata säännöllisesti. 3. Poikkeamiin reagointi sisältää havaitun poikkeaman analysoinnin, poikkeamasta viestinnän ja poikkeaman käsittelyn, eli esimerkiksi häiriön eristämisen ja juurisyyn korjaamisen. 4. Poikkeamista palautumista tukee ennalta suunniteltu palautumisprosessi sekä järjestelmäkohtaiset toimintaohjeet palautumiseen. Poikkeamatilanteiden harjoittelu auttaa hahmottamaan palautumisen puutteita. 5. Jokaisesta poikkeamasta on otettava opiksi koostamalla tiedot siitä, mikä johti poikkeamaan ja mitä voidaan kehittää, jotta vastaavalta vältytään jatkossa. Tietoturvahäiriöiden hallinnataan liittyvät periaatteet ja prosessi on kuvattu myös SFS-ISO 27035 standardissa (SFS ISO 27035). Standardissa kuvattu prosessi on hyvin samankaltainen kuin CSF-viitekehyksen mukainen prosessi, joskin käytetyissä määritelmissä on joitain eroavaisuuksia.

Kuvio 11. Toimenpiteet poikkeamien hallinnan toteuttamiseksi

Jatkuvuussuunnittelu tarkoittaa niitä toimia, joiden avulla pyritään pienentämään ja lyhentämään toimintaa haittaavien tapahtumien vaikutusta ja kestoa. Se sisältää varajärjestelyitä sekä toimenpiteitä, jotka parantavat toimintaa häiriötilanteissa tai toipumista ongelmien jälkeen. (VAHTI 2016, 24). Kuviossa 12 on käsitelty tarkemmin jatkuvuudenhallinnan toteuttamisen vaatimia toimenpiteitä.

Toimenpiteet jatkuvuudenhallinnan toteuttamiseksi liittyen artiklaan 21
Liiketoiminnan jatkuvuudenhallinnan standardin ISO 22301:n mukaisesti jatkuvuuden hallintamallin suunnittelu alkaa periaatteiden ja tavoitteiden määrittämisellä sekä toiminnan jatkuvuutta uhkaavien riskien tunnistamisella (ISO 22301, 16–17). Kyberturvallisuuteen liittyen jatkuvuudenhallinnassa tulee ottaa huomioon erityisesti organisaation eri tietojärjestelmien ja -verkkojen kriittisyys toiminnan kannalta sekä näiden muodostamat riippuvuussuhteet. Kriittisten kohteiden luokitteluun on saatavilla useita maksullisia ja ilmaisia työkaluja, joista yksi esimerkki on Digi- ja väestötietoviraston julkaisema luokittelutyökalu (Digi- ja väestötietovirasto 2022c). Kun jatkuvuudenhallinnan tavoitteet, riskit ja toiminnan kannalta kriittiset tietojärjestelmät ja -verkot on tunnistettu, on niille laadittava jatkuvuus- ja palautumissuunnitelmat. Jatkuvuus- ja palautumissuunnitelmat sisältävät useimmiten toimintaohjeet (VAHTI 2016, 69–70): • häiriöihin varautumisesta, • häiriöntilanteen aikaisesta toiminnasta, kuten varajärjestelyistä, korjaustoimenpiteistä ja palautumisvaatimuksista, • häiriötilanteen aikaisista rooleista ja vastuista sekä • häiriötilanteen aikaisesta viestinnästä. Keskeinen osa hyvää jatkuvuudenhallintaa on jatkuva parantaminen, jonka avulla tapahtuneista häiriöistä saatujen oppien perusteella pyritään välttämään vastaavia tapahtumia jatkossa. (ISO 22301, 28).

Kuvio 12. Toimenpiteet jatkuvuudenhallinnan toteuttamiseksi

Toimitusketjujen turvallisuuden varmistamiseksi organisaation tulisi sisällyttää myös toimitusketjujen ja keskeisten palveluntarjoajien tuottamien palveluiden ja tietojärjestelmien muodostamat riskit osaksi riskienhallintaa ja säännöllistä tarkastelua (National Institute of Standards and Technology 2018, 28). Toimitusketjujen turvallisuuteen liittyviä toimenpiteitä on käsitelty kuviossa 13.

Toimenpiteet toimitusketjujen turvallisuuden toteuttamiseksi liittyen artiklaan 21
Toimitusketjujen turvallisuutta voidaan lisätä määrittämällä sopimuksiin sisällytettävät turvallisuusvaatimukset tieto- ja viestintäteknologiakumppaneille. Näiden vaatimusten toteutumista tulisi arvioida säännöllisesti esimerkiksi turvallisuusauditointien, sertifiointien tai muun yleiseen toimittaja- ja palvelunhallintaan sisältyvän raportoinnin avulla. Lisäksi häiriöistä ja muista poikkeamista palautumista tulisi harjoitella säännöllisesti yhdessä toimitusketjuihin kuuluvien kumppanien kanssa. (National Institute of Standards and Technology 2018, 28–29).

Kuvio 13. Toimenpiteet toimitusketjujen turvallisuuden toteuttamiseksi

Vuonna 2018 voimaan astunut Euroopan Unionin yleinen tietosuoja-asetus toi mukanaan käsitteen oletusarvoinen ja sisäänrakennettu tietosuoja. Tällä tarkoitetaan sitä, että tietosuojaperiaatteet huomioidaan henkilötietojen käsittelyssä aivan alkuvaiheista saakka. (Euroopan komissio 2023.) Myös turvallisuuden tulisi olla oletusarvoisesti huomioituna ja sisäänrakennettuna jokaisessa nykyaikaisessa tietojärjestelmässä. Organisaation onkin huomioitava kyberturvallisuus niin järjestelmähankinnoissa, kuin myös itse kehittämissään ja ylläpitämissään tietojärjestelmissä. Kuviossa 11 esitetään muutamia kehittämisen ja ylläpidon turvallisuuteen liittyviä malleja.

Toimenpiteet tietojärjestelmien hankintojen, kehittämisen ja ylläpidon turvallisuuden toteuttamiseksi liittyen artiklaan 21
Tietojärjestelmien kehittämisen ja ylläpidon turvallisuuteen liittyvät menettelyt tulisi toteuttaa Software Development Lifecycle- mallia hyödyntäen, siten että tietojärjestelmien tai palveluiden koko elinkaari suunnitellaan relevanttien kumppaneiden kanssa. (National Institute of Standards and Technology 2018, 33). Turvalliseen sovelluskehitykseen on syntynyt viime vuosina huomattava määrä periaatteita ja ohjeistusta, jotka on syytä huomioida tietojärjestelmien hankintojen, kehittämisen ja ylläpidon turvallisuutta suunnitellessa. Eräänä hyvänä esimerkkinä tällaisista periaatteista on turvallisen sovelluskehityksen lähestymistapa DevSecOps, jonka avulla pyritään varmistamaan, että turvallisuus huomioidaan saumattomasti kehittämisen ja ylläpidon jokaisessa vaiheessa (U.S. Department of Defence 2021, 16–19).

Kuvio 14. Toimenpiteet tietojärjestelmien hankintojen, kehittämisen ja ylläpidon turvallisuuden toteuttamiseksi

Haavoittuvuus tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, prosesseissa, kotiautomaatiossa tai niitä voi aiheutua ihmisten toiminnan seurauksena. (Liikenne ja viestintävirasto Traficom 2020b.) Nollapäivähaavoittuvuus on tietojärjestelmässä oleva haavoittuvuus, johon ei ole saatavilla korjausta (TSK 2018, 15).

Haavoittuvuudet johtuvat usein tahattomista virheistä sovelluskehityksessä tai laitteiden valmistuksessa. Haavoittuvuuksia etsivät niin tietoturvatutkijat, sovellus- ja laitevalmistajat kuin rikollisetkin. Erilaisia laite- tai järjestelmähaavoittuvuuksia löytyy päivittäin useita kymmeniä, joten niiden korjaamiseen kannattaa varautua hyvissä ajoin määrittämällä selkeät prosessit. Kuviossa 15 on avattu tarkemmin haavoittuvuuksien hallinnan toimintamallin toteuttamista.

Toimenpiteet haavoittuvuuksien hallinnan toteuttaminen liittyen artiklaan 21
Haavoittuvuuksien hallintaan liittyvät suunnitelmat tulisi dokumentoida sekä itse kehitettyjen, että hankittujen tietojärjestelmien ja palveluiden osalta (National Institute of Standards and Technology 2018, 36). Haavoittuvuuksien hallintaan liittyy operatiivisia toimenpiteitä, kuten säännöllinen haavoittuvuuksien etsintä tähän tarkoitetuilla työkaluilla, haavoittuvuuksien korjaaminen sekä haavoittuvuuksista ilmoittaminen (ENISA 2023b). Haavoittuvuuksien hallinnan toimintamallista tulisi käydä ilmi ainakin: • haavoittuvuuksien hallinnan kohteet, • haavoittuvuuksien prioriteetit ja niitä vastaavat korjaustavoitteet, • haavoittuvuuksien korjaamiseen liittyvät käytännöt kuten muun muassa se, milloin eri haavoittuvuudet voidaan korjata ja miten korjauksista viestitään, • haavoittuvuuksien etsintään käytetyt työkalut ja aikataulu sekä • uudelleentarkastukset korjausten varmentamiseksi. Lisäksi, mikäli organisaatio kehittää tai tuottaa itse tieto- ja viestintäteknologian palveluita, haavoittuvuuksien hallinnan toimintamalleista tulisi käydä ilmi tavat miten löydetyt haavoittuvuudet voidaan ilmoittaa organisaatiolle ja miten organisaatio itse viestii ja ilmoittaa haavoittuvuuksista. Liikenne- ja viestintävirasto Traficom ohjeistaa artikkelissaan tapoja haavoittuvuuksien ilmoittamiselle sekä ilmoitusten vastaanottamiselle. (Liikenne ja viestintävirasto Traficom 2020b).

Kuvio 15. Toimenpiteet haavoittuvuuksien hallinnan toteuttamiseksi

Kyberturvallisuusriskien hallintatoimia tulisi myös arvioida säännöllisesti. Säännöllinen arviointi auttaa kehittämään toimenpiteitä sekä tarvittaessa luopumaan tehottomista hallintatoimenpiteistä. Kuviossa 13 on esitetty muutamia toimenpiteitä säännöllisen arvioinnin helpottamiseksi.

Toimenpiteet säännöllisen arvioinnin toteuttamiseksi liittyen artiklaan 21
Toimenpiteiden vaikuttavuutta ja tehokkuutta voidaan arvioida säännöllisesti osana jatkuvaa riskienhallintaprosessia, mutta sen lisäksi niitä voidaan arvioida hyödyntäen erilaisia oman organisaation kyberturvallisuuden kypsyystason arviointimenetelmiä ja -työkaluja. Eräs esimerkki tällaisesta työkalusta on maksuton Kyberturvallisuuskeskuksen Kybermittari (Traficom 2023a), jonka avulla organisaatio voi arvioida kattavasti kyberturvallisuuden eri osa-alueita. Kyberturvallisuusriskien hallintatoimenpiteiden vaikuttavuuden arvioinnin tulisi olla säännöllistä ja vuosikellon mukaista toimintaa siten, että arviointi ja tulosten dokumentointi toteutetaan esimerkiksi vuosittain tai kvartaaleittain. Arvioinnissa tulisi tarpeen mukaan käyttää myös ulkopuolista ja riippumatonta arvioijaa, jotta organisaatio saa objektiivisen kuvan kyberturvallisuuden tilasta.

Kuvio 16. Toimenpiteet säännöllisen arvioinnin toteuttamiseksi

Kyberturvallisuutta ei voida varmistaa ilman koko organisaation laajuisen turvallisuuskulttuurin muodostumista. Perustason kyberturvallisuuskäytäntöjen, kuten turvallisten työskentelytapojen omaksuminen henkilöstön keskuudessa on hyvin keskeisessä asemassa organisaation kyberturvallisuuden varmistamisessa. Tämä vaatii suunnitelmallista kouluttamista sekä viestintää kyberturvallisuuteen liittyvistä ohjeista ja käytännöistä. Kuviossa 10 on esitetty tapoja varmistaa riittävä perustason kyberturvallisuusosaaminen organisaatiossa.

Toimenpiteet perustason kyberhygienian ja kyberturvallisuuskoulutusten toteuttamiseksi liittyen artiklaan 21
Organisaation on varmistettava, että henkilöstölle ja kumppaneille tarjotaan riittävää perustason kyberturvallisuuskoulutusta, ja että henkilöstö saa koulutusta työtehtäviensä suorittamiseen organisaation turvallisuuteen liittyvien käytäntöjen ja ohjeistusten mukaisesti. (National Institute of Standards and Technology 2018, 31). Erityisesti suuremmissa usean toimipaikan organisaatioissa kustannustehokkain tapa järjestää kyberturvallisuuskoulutusta saattaa vaatia verkkokoulutusalustojen ja valmiiden verkkokurssien hyödyntämistä. Digitaalisen turvallisuuden aihepiiriin liittyviä maksuttomia verkkokursseja löytyy muun muassa Digi- ja väestötietoviraston laatimasta Digiturvallinen elämä -koulutuskokonaisuudesta (Digi- ja väestötietovirasto 2023d). Lisäksi useat korkeakoulut ovat julkaisseet ja tulevat julkaisemaan kyberturvallisuuteen liittyviä avoimia kursseja. Organisaation kannalta on oleellista varmistaa, että eri henkilöstöryhmät saavat työtehtäviensä mukaiset riittävät taidot kyberturvallisuusasioista ja että henkilöstön kouluttautumisesta pidetään kirjaa.

Kuvio 17. Toimenpiteet perustason kyberhygienian ja kyberturvallisuuskoulutusten toteuttamiseksi

Tiedon suojaaminen on yksi keskeisistä tieto- ja kyberturvallisuuteen vaikuttavista kokonaisuuksista. Tiedon suojaamisessa tulee ottaa huomioon tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen (National Institute of Standards and Technology 2018, 32). On suositeltavaa, että organisaatiossa laaditaan tiedon luokittelumalli (ISO/IEC 27001, 17), jossa jaotellaan vähintäänkin julkinen tieto ja salassa pidettävä tieto, sekä määritellään näitä luokituksia tukevat turvallisuusperiaatteet. Tiedon suojaamisessa hyödynnettäviä turvallisuusperiaatteita on esitetty kuviossa 18.

Toimenpiteet tiedon suojaamisen, kryptografian ja salausperiaatteiden toteuttamiseksi liittyen artiklaan 21
Suojattavan tiedon osalta turvallisuusperiaatteita ovat muun muassa (National Institute of Standards and Technology 2018, 32–33): 1. Suojattavat tiedot salataan riittävän vahvoilla salausmenetelmillä sekä tallennettuna (*data-at-rest*), että siirrettäessä (*data-in-transit*). 2. Käytettyihin salausteknologioihin liittyvät vähimmäisvaatimukset, kuten käytettävät salausalgoritmit, on määritetty. 3. Suojattavan tiedon käsittely sallitaan vain luotetuilla tai keskitetysti ylläpidetyillä laitteilla. 4. Turvallisen tietojenkäsittelyn suunnittelussa huomioidaan tiedon koko elinkaari aina tiedon tuottamisesta käsittelyyn ja tiedon turvalliseen tuhoamiseen. 5. Tietojärjestelmien ja -verkkojen riittävästä kapasiteetista huolehditaan, jotta järjestelmien tai palveluiden saatavuus ei vaarannu. 6. Tarvittavat tekniset suojaukset tietovuotojen estämiseksi on toteutettu. 7. Kehittämis- ja testausjärjestelmät eriytetään tuotantojärjestelmistä. 8. Ohjelmistojen ja laitteistojen eheys ja aitous varmistetaan ennen käyttöönottoa ja muutoksien yhteydessä.

Kuvio 18. Tiedon suojaaminen, kryptografia ja salausperiaatteet

Myöskään organisaatioiden henkilöstön roolia kyberturvallisuuden toteutumisessa ei sovi unohtaa. Tietoliikenneyhtiö Verizonin julkaiseman tietomurtoportin mukaan noin viidennes toteutuneista tietomurroista on peräisin organisaation sisältä, joko henkilöstön tahallisen tai tahattoman toiminnan seurauksena (Verizon 2021, 12). Suunnitelmallisilla henkilöstöturvallisuuden toimenpiteillä voidaan pienentää henkilöstön muodostamaa riskiä kyberturvallisuudelle. Kuviossa 19 on käsitelty tarkemmin henkilöstöturvallisuuden ja pääsynhallinnan käytäntöjä.

Toimenpiteet henkilöstöturvallisuuden ja pääsynhallinnan toteuttamiseksi liittyen artiklaan 21
Riittävä henkilöstöturvallisuus voidaan varmistaa kytkemällä turvallisuuteen liittyvät käytännöt saumattomaksi osaksi henkilöstöhallinnon prosesseja. Muun muassa henkilöstöstä rekrytoinnin yhteydessä tai säännöllisin väliajoin tehtävät turvallisuusselvitykset sekä eri henkilöstöryhmien käyttövaltuuksien ylläpito roolipohjaisen mallin mukaisesti edustavat tätä lähestymistapaa (National Institute of Standards and Technology 2018, 35). Pääsynhallinnan käytännöt tarkoittavat käytännössä sitä, että pääsy tietojärjestelmiin- ja verkkoihin sekä fyysisiin tiloihin myönnetään vain niille tahoille, jotka sitä tarvitsevat työtehtäviensä hoitamiseksi. Pääsyvaltuuksien ei tulisi myöskään mahdollistaa työtehtävien kannalta tarpeettoman laajaa käyttöoikeutta tietojärjestelmissä. On hyvä huomata, että pääsyvaltuuksia voidaan myöntää henkilöiden lisäksi myös esimerkiksi laitteille tai muille sovelluksille. Eräs viime vuosina yleistynyt pääsynhallinnan konsepti on nollaluottamusmalli (*Zero Trust*). Nollaluottamusmallin periaatteiden mukaisesti organisaation tietoverkkoja ei jaeta enää luotettavaan sisäverkkoon ja epäluotettavaan ulkoverkkoon, vaan kaikkea verkkoliikennettä pidetään lähtökohtaisesti epäluotettavana. Siksi mallissa jokainen käyttöoikeuspyyntö tietoverkoissa sijaitseviin resursseihin on varmistettava pääsynhallinnan keinoin. Luottamus käyttöoikeuspyynnön oikeellisuuteen perustuu jokaisen käyttötapahtuman yhteydessä käyttäjän identiteetin monivaiheiseen tunnistamiseen, valtuutukseen, päätelaitteiden vaatimustenmukaisuuteen ja käsiteltävien tietojen luokitteluun. (Digi- ja väestötietovirasto 2022d).

Kuvio 19. Toimenpiteet henkilöstöturvallisuuden ja pääsynhallinnan toteuttamiseksi

Riittävien ja tehokkaasti kohdistettujen kyberturvallisuustoimenpiteiden toteuttamisen perustana toimii omaisuudenhallinta. Organisaation on tunnistettava ja pidettävä kirjaa suojattavasta omaisuudestaan. Suojattava omaisuus pitää sisällään muun muassa organisaation käsittelemät tiedot, laitteet, sovellukset, tietojärjestelmät, tietoverkot sekä toimitilat. Kuviossa 20 on käsitelty omaisuudenhallinnan toteuttamiseen liittyviä toimenpiteitä.

Toimenpiteet omaisuudenhallinnan toteuttamiseksi liittyen artiklaan 21
Omaisuudenhallintaa voidaan toteuttaa tähän tarkoitukseen räätälöidyn tietokannan avulla. Markkinoilta löytyy lukuisia valmiita tai räätälöitäviä teknisiä ratkaisuja omaisuudenhallinnan toteuttamiseen. Tietokannan tulisi sisältää vähintään tiedot seuraavista: 1. fyysiset laitteet ja järjestelmät, 2. ohjelmistot ja sovellukset, 3. tietoliikenne, tietovirrat ja integraatiot sekä 4. ulkoiset tietojärjestelmät. Koska suojattavan omaisuuden kirjanpidosta syntyy nopeasti suuriakin tietomassoja, on suositeltavaa, että organisaatio priorisoi suojattavan omaisuuden esimerkiksi niiden liiketoimintaan tai organisaation tavoitteisiin liittyvän kriittisyyden perusteella, jotta relevanttien kyberturvallisuustoimenpiteiden kohdistaminen olisi helpompaa. (National Institute of Standards and Technology 2018, 24.)

Kuvio 20. Omaisuudenhallinnan toteuttaminen

Entistä useammin organisaatioiden sisäinen johtaminen ja kommunikaatio nojaa vahvasti erilaisiin tietoteknisiin viestintäratkaisuihin, jotka ovat niin ikään alttiita kyberturvallisuuden häiriöille tai luvattomalle käytölle. Tästä syystä organisaatioiden tulisi kuvion 21 mukaisesti riskiarvioinneissaan harkita edellyttääkö organisaation toiminta erityisten suojattavien viestintäratkaisujen ja hätäviestintäjärjestelmien käyttöä.

Suojatut puhe-, video-, tai tekstiviestinnän järjestelmät ja hätäviestintäjärjestelmät liittyen artiklaan 21
Mikäli riskiarvioinnissa todetaan, että suojattuja tai vaihtoehtoisia viestintäjärjestelmiä tarvitaan jonkin tunnistetun riskin lieventämiseksi, organisaation tulisi hankkia tai muulla tavoin ottaa käyttöön vaihtoehtoinen viestintäjärjestelmä, joka mahdollistaa tärkeiden toimintojen jatkamisen sellaisessakin tilanteessa, jossa ensisijaiset viestintäjärjestelmät eivät ole käytettävissä (National Institute of Standards and Technology 2020, 124).

Kuvio 21. Suojatut viestintäjärjestelmät ja hätäviestintäjärjestelmät

Valtio tai toimivaltainen viranomainen voi lisäksi määrätä toimijat käyttämään tiettyä sertifioitua tieto- ja viestintäteknologiaa. Sertifioinnin pohjana käytetään Euroopan unionin kyberturvallisuusvirasto ENISA:n valmistelemaa eurooppalaisen kyberturvallisuuden

sertifiointijärjestelmää. Direktiivissä ei kuitenkaan esitetä vaatimuksia tietyille toimijoille, vaan sertifioitujen tieto- ja viestintäteknologioiden käytöstä säädetään tarvittaessa erikseen. (EU/2022/2555 artikla 24.) Direktiivissä suositellaan toimijoita hyödyntämään toiminnassaan kansainvälisesti tai eurooppalaisittain standardoituja ratkaisuja (EU/2022/2555 artikla 25). Kuviossa 22 on havainnollistettu toimenpiteitä liittyen standardointiin ja sertifioitujen tieto- ja viestintäteknologioiden käyttöön.

Toimenpiteet sertifiointijärjestelmien ja kansainvälisten standardien käyttöön ja liittyen artikloihin 24 ja 25
Organisaatioiden on seurattava EU:n, ENISA:n ja kansallisten viranomaisten viestintää liittyen mahdollisiin vaatimuksiin sertifioitujen tieto- ja viestintäteknologioiden käytöstä. ENISA toimii eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän valmistelijana, joten heidän julkaisemiinsa aiheeseen liittyviin tiedotteisiin kannattaa kiinnittää erityistä huomiota. (ENISA 2023c.) Suunnitellessaan kyberturvallisuuden toimenpiteitä, olivatpa ne sitten hallinnollisia, operatiivisia tai teknisiä, organisaatioiden tulee huomioida eurooppalaiset ja kansainväliset standardit toimenpiteiden toteuttamiseksi. Esimerkiksi riskienhallinnan prosessien toteuttamisen osalta olisi hyvä huomioida laajasti niin yritysmaailmassa kuin julkisellakin sektorilla hyödynnetty ISO/IEC 31000 standardi.

Kuvio 22. Sertifiointijärjestelmien ja standardien käyttö

Erillisten Euroopan Unionin komission määritysten mukaisesti tietyille kriittisiksi luokitelluille tieto- ja viestintäteknologian toimitusketjuille voidaan tehdä koordinoituja riskiarviointeja (EU/2022/2555 artikla 22). Organisaation tulisikin seurata omalta osaltaan niin Euroopan Unionin komission, direktiivin toimeenpanon yhteydessä perustettavan yhteistyöryhmän, kuin Euroopan unionin kyberturvallisuusvirasto ENISA:nkin kriittisiksi arvioituihin toimitusketjuihin ja näiden koordinoituihin turvallisuusselvityksiin liittyvää viestintää.

5.3 Poikkeamien raportointivelvoitteet

Organisaation on ilmoitettava merkittävistä poikkeamista toimivaltaiselle viranomaiselle sekä palvelunsa vastaanottajalle tai käyttäjälle. Organisaation on myös tiedotettava palvelunsa käyttäjille sellaisista toimenpiteistä, joita käyttäjät voivat itse tehdä poikkeaman tai kyberuhan hallitsemiseksi omissa järjestelmissään. (Direktiivi 2022/2555/EU, artikla 23). Tarkat määritykset poikkeamailmoitusten sisällöistä ja aikarajoista on esitetty kuviossa 23.

Poikkeamien raportointivelvoitteet liittyen artiklaan 23
Organisaation on ilmoitettava merkittävistä poikkeamista viranomaiselle ja asiakkailleen seuraavien aikarajojen puitteissa: • 24 tunnissa: ennakkovaroitus sisältäen tiedon siitä epäilläänkö poikkeaman aiheuttajaksi lainvastaista tai vihamielistä tekoa ja voiko poikkeamalla olla rajatylittävä vaikutus. • 72 tunnissa: varsinainen poikkeamailmoitus sekä arvio poikkeaman vakavuudesta ja vaikutuksista sekä vaarantumisen indikaattoreista (*indicators of compromise*). • Kuukauden kuluessa: poikkeamaraportti sisältäen tiedot: yksityiskohtainen kuvaus, vakavuus ja vaikutukset, rajatylittävät vaikutukset, uhkan tai juurisyyn tyyppi sekä toimenpiteet poikkeaman lieventämiseksi. Tämän opinnäytetyön kirjoitushetkellä Liikenne- ja viestintävirasto Traficomilla on olemassa sähköinen ilmoituskanava tietoturvaloukkausten ilmoittamiseen (Liikenne- ja viestintävirasto Traficom 2023b).

Kuvio 23. Poikkeamien raportointivelvoitteet

Koska poikkeamatilanteessa saattaa olla käytännössä hankalaa selvittää vuorokauden kuluessa esimerikiksi toimijalle aiheutuvien taloudellisten tappioiden suuruutta ja sen perusteella sitä, onko kyseinen poikkeama raportointivelvoitteiden piirissä, olisi suositeltavaa lähettää ennakkovaroitus kaikista kyberturvallisuuteen liittyvistä poikkeamista.

5.4 Toimijoiden rekisterit

Direktiivin toimeenpanon yhteydessä Euroopan unionin kyberturvallisuusvirasto ENISA perustaa keskeisten digitaalisen infrastruktuurin toimijoiden rekisterin, joka sisältää kansallisen toimivaltaisen viranomaisen toimittamat tiedot digitaalisen infrastruktuurin toimijoista (Direktiivi 2022/2555/EU, artikla 27). Kuviossa 24 on käsitelty tarkemmin kyseisen rekisterin sisältöä ja toimijoita, joiden tulisi ilmoittaa vaaditut tiedot rekisteriin.

Toimenpiteet toimijoiden rekisterin toteuttamiseksi liittyen artiklaan 27
Digitaalisen infrastruktuurin toimijoiden on toimitettava kansalliselle toimivaltaiselle viranomaiselle seuraavat tiedot sekä ilmoittaa tiedoissa tapahtuvista muutoksista viipymättä ja joka tapauksessa viimeistään kolmen kuukauden kuluessa: • toimijan nimi, • toimiala, toimialan osa ja toimijatyyppi, • päätoimipaikan ja muiden unionissa sijaitsevien laillisten toimipaikkojen osoite, • toimijan edustajan ajantasaiset yhteystiedot, mukaan lukien sähköpostiosoitteet ja puhelinnumerot, • lista jäsenvaltioista, joissa toimija tarjoaa palveluita sekä • toimijan IP-osoitealueet. Toimivaltainen viranomainen toimittaa tiedon eteenpäin ENISA:lle toimijoiden rekisterin ylläpitämistä varten. Digitaalisen infrastruktuurin toimijoihin kuuluvat seuraavia palveluita tarjoavat toimijat: • DNS-palvelut, • aluetunnusrekisterit, • verkkotunnusten rekisteröintipalvelut, • pilvipalvelut, • datakeskuspalvelut, • sisällönjakeluverkot, • tietotekniikan hallintapalvelut, • tietoturvapalvelut, • verkossa toimivat markkinapaikat, • verkossa toimivat hakukoneet sekä • verkkoyhteisöalustat.

Kuvio 24. Toimenpiteet toimijoiden rekisterin toteuttamiseksi

Euroopan unionin kyberturvallisuusvirasto ENISA antaa tarvittaessa toimivaltaisille viranomaisille pääsyn toimijoiden rekisteriin sekä varmistaa tietojen luottamuksellisuuden suojaamisen (Direktiivi 2022/2555/EU, artikla 27).

Lisäksi direktiivi velvoittaa aluetunnusrekisterit ja verkkotunnusten rekisteröintipalveluja tarjoavat toimijat keräämään ja ylläpitämään tarkkoja verkkotunnusten rekisteröintitietoja asiakkaidensa osalta kuvion 25 mukaisesti (Direktiivi 2022/2555/EU, artikla 28).

Toimenpiteet verkkotunnusten rekisteröintitietojen tietokannan toteuttamiseksi liittyen artiklaan 28
Aluetunnusrekistereiden ja verkkotunnusten rekisteröintipalveluja tarjoavien toimijoiden tulee kerätä ja ylläpitää seuraavia tietoja verkkotunnusten rekisteröinneistä yhteistyössä keskenään: • verkkotunnus, • rekisteröintipäivä, • rekisteröijän nimi, • rekisteröijän yhteyssähköpostiosoite sekä • rekisteröijän puhelinnumero.

Kuvio 25. Toimenpiteet verkkotunnusten rekisteröintitietojen tietokannan toteuttamiseksi

Muut verkkotunnusten rekisteröintitiedot kuin henkilötiedot on asetettava julkisesti saataville. Lisäksi toimintaperiaatteet ja menettelyt tietojen keräämisestä sekä ylläpitämisestä on oltava julkisesti saatavilla (Direktiivi 2022/2555/EU, artikla 28).

5.5 Tietojenvaihto

Osallistuminen tiedonvaihtoryhmiin ja -alustoille mahdollistaa kattavan tilannekuvan muodostamisen myös oman organisaation ulkopuolisesta kyberturvallisuustilanteesta. On tärkeää, että kyberturvallisuuteen liittyviä tietoja, kuten esimerkiksi tietoja tunnistetuista uhista tai vaarantumisindikaattoreista jaetaan toimijoiden kesken. Direktiivi velvoittaa jäsenvaltioita varmistamaan, että vapaaehtoinen tiedonvaihto on mahdollista. Lisäksi keskeisten sekä tärkeiden toimijoiden tulee ilmoittaa osallistumisestaan tai vetäytymisestään tällaisesta tiedonvaihdosta. (Direktiivi 2022/2555/EU, artikla 29). Kuviossa 26 on esitetty kyberturvallisuustietojen jakamiseen tarkoitettuja yhteistyöverkostoja ja alustoja.

Toimenpiteet kyberturvallisuustiedon jakamisjärjestelyiden toteuttamiseksi liittyen artiklaan 29
Tiedonvaihtokanavina toimivat muun muassa erilaiset kyberturvallisuuteen keskittyvät yhteisöt ja alustat. Esimerkiksi toimivaltaisten viranomaisten ylläpitämät verkostot tai yhteisöt kuten ISAC-tiedonvaihtokanavat (*Information Sharing and Analysis Centre*) tai globaalit kyberturvallisuuden foorumit toimivat tiedonvaihtoverkostoina. Liikenne- ja viestintävirasto Traficomin kyberturvallisuuskeskus koordinoi Suomessa toimivia kriittisten toimialojen ISAC-tiedonvaihtoryhmiä. ISAC-tiedonvaihtoryhmät ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. ISAC-ryhmissä käsitellään luottamuksellisesti kyberturvallisuuteen liittyviä asioita, kuten uhkia, ilmiöitä ja hyviä käytäntöjä. (Liikenne- ja viestintävirasto Traficom 2023c). Lisäksi tiedonvaihtoon on tarjolla erilaisia alustoja ja malleja, joihin toimijoiden olisi syytä tutustua. Näitä alustoja ovat esimerkiksi erilaiset avoimen lähdekoodin uhkatietoalustat, kuten MISP-projekti (MISP project 2023) sekä tiedonvaihdon tekniset standardit. Tiedonvaihdon teknisistä standardeista huomionarvoisia ovat muun muassa STIX (*Structured Threat Information Expression*), joka on vakioitu formaatti kyberuhkatiedon vaihtamiseen (Oasis Open 2021a), sekä TAXII (*Trusted Automated Exchange of Indicator Information*), joka on sovellustason protokolla kyberuhkatietojen välittämiseen yksinkertaisella ja skaalautuvalla tavalla (Oasis Open 2021b).

Kuvio 26. Toimenpiteet kyberturvallisuustiedon jakamisjärjestelyiden toteuttamiseksi

Organisaatiot voivat myös vapaaehtoisesti ilmoittaa lievemmistä poikkeamista tai esimerkiksi havaitsemistaan mahdollisista kyberuhkista edesauttaakseen laajan ja kattavan kyberturvallisuuden tilannekuvan muodostamista. Poikkeamista voivat ilmoittaa myös direktiivin ulkopuoliset organisaatiot. (Direktiivi 2022/2555/EU, artikla 30.)

5.6 Valvonta ja täytäntöönpano

Direktiivin myötä toimivaltainen viranomainen voi suorittaa tarkastuksia organisaatioihin ja määrätä hallinnollisia sakkoja tai muita seuraamuksia direktiivin velvoitteiden laiminlyönnistä. Tarkastuksiin voi sisätyä esimerkiksi paikan päällä tehtävät satunnaistarkastukset, turvallisuusauditoinnit, skannaukset sekä tietopyynnöt kyberturvallisuustoimenpiteistä. Toimija vastaa itse auditointien kustannuksista, ellei toimivaltainen viranomainen päätä toisin. (Direktiivi 2022/2555/EU, artiklat 32 ja 33.)

On syytä huomioida, että keskeisten toimijoiden osalta tarkastuksia voidaan tehdä myös ennaltaehkäisevässä tarkoituksessa ja satunnaisesti (Direktiivi 2022/2555/EU, artikla 32). Tärkeiden toimijoiden osalta tarkastuksia voidaan tehdä jälkikäteisvalvontana siinä tapauksessa, että on syytä olettaa, että direktiivin velvoitteta ei ole noudatettu. (Direktiivi 2022/2555/EU, artikla 33)

Organisaatiolle voidaan määrätä sanktioita, kuten määräyksiä tai hallinnollisia sakkoja, mikäli direktiivin määräyksiä ei noudateta. Hallinnollisten sakkojen suuruus määräytyy toimijan luokituksen mukaan (Direktiivi 2022/2555/EU, artikla 34):

- Keskeisille toimijoille: 10 000 000 euroa tai 2 prosenttia maailmanlaajuisesta liikevaihdosta
- Tärkeille toimijoille: 7 000 000 euroa tai 1,4 prosenttia maailmanlaajuisesta liikevaihdosta

Jos kyseessä on samaan aikaan myös yleisen tietosuoja-asetuksen mukainen henkilötietojen tietoturvaloukkaus, josta tietosuojaviranomainen määrää hallinnollisia sakkoja, ei sakkoja määrätä sen lisäksi tämän direktiivin mukaisti (Direktiivi 2022/2555/EU, artikla 35).

Direktiivin edellyttämät säännökset tulee saattaa osaksi kansallista lainsäädäntöä viimeistään 17. lokakuuta 2024 (Direktiivi 2022/2555/EU, artikla 41). Lainsäädäntötyö Suomen osalta on tämän opinnäytetyön kirjoitushetkellä jo käynnissä. Liikenne- ja viestintäministeriö käynnisti alkuvuodesta 2023 kansallisen toimeenpanohankkeen direktiivin vaatimusten saattamiseksi osaksi kansallista lainsäädäntöä. Hankkeen etenemistä voi seurata Valtioneuvoston säädösvalmisteluiden ja kehittämishankkeiden hankeikkunassa. (Valtioneuvosto 2023.)

6 Johtopäätökset ja pohdinta

Tässä luvussa esitetään havaintoja Euroopan Unionin uudesta kyberturvallisuusdirektiivistä peilaten opinnäytetyön tuloksia alussa asetettuihin tavoitteisiin. Opinnäytetyön tavoitteena oli selvittää, millaisia organisaatioita Euroopan Unionin uusi kyberturvallisuusdirektiivi koskee ja millaisia vaatimuksia se asettaa organisaatioille. Lisäksi opinnäytetyön tavoitteena oli tuottaa toimenpide-ehdotuksia näiden vaatimusten täyttämiseksi kytkemällä olemassa olevat kyberturvallisuuden käytännöt ja mallit direktiivin vaatimuksiin. Opinnäytetyön tuotoksena syntyi analyysi direktiivin soveltamisalasta, vaatimuksista sekä lukuisia toimenpide-ehdotuksia keinoista, joilla vaatimuksiin voidaan vastata organisaatioissa.

6.1 Sääntelyllä kohti parempaa kyberturvallisuutta

Kyberturvallisuuden vahvemmalle sääntelylle on ollut selkeä tarve jo pitkään, sillä tietoverkoista ja digitaalisista palveluista on tullut muutaman viimeisen vuosikymmenen aikana keskeinen osa kehittyneitä yhteiskuntia. Sääntelyn puolesta puhuvat erityisesti viime vuosina tapahtuneet vakavat tietomurrot ja kriittisen infrastruktuurin toimintahäiriöt. Sääntelyn keinoin kyberturvallisuuteen voidaan vaikuttaa joko ennaltaehkäisevästi tai reaktiivisesti. Euroopan Unionin uusi kyberturvallisuusdirektiivi pyrkii vaikuttamaan näihin molempiin. Ennaltaehkäiseviä keinoja ovat erityisesti riskienhallintaan ja riskien hallintakeinoihin liittyvät vaatimukset. Toisaalta taas raportointi viranomaisten suuntaan sekä tiedonvaihto toimijoiden kesken edesauttaa laajavaikutteisten häiriöiden tai hyökkäysten rajaamisessa tilanteen ollessa jo käynnissä.

Opinnäytetyön tietoperustana on käytetty muun muassa Yhdysvalloissa laadittua Cybersecurity Framework viitekehystä, joka sai alkunsa samankaltaisista lähtökohdista, mutta toki eri mantereella. Analyysiä toteuttaessa olikin havaittavissa paljon samankaltaisuutta direktiivin ja CSF-viitekehyksen osalta. Helpottava tieto monen etenkin kansainvälisesti toimivan organisaation osalta saattaa myös olla se, että mikäli organisaatiossa on aikaisemmin hyödynnetty CSF-viitekehystä kyberturvallisuuden kehittämisen tukena, ovat vaadittavat toimenpiteet myös uuden kyberturvallisuusdirektiivin näkökulmasta kohtalaisen hyvällä mallilla.

Direktiivin vaatimukset eivät sinällään tuo mitään uutta tai ihmeellistä kyberturvallisuuden saralla. Suuret organisaatiot, jotka ovat toimineet kriittisen infrastruktuurin toimialoilla, ovat todennäköisesti varautuneet kyberturvallisuusuhkiin jo pitkään. Näiden organisaatioiden näkökulmasta direktiivin vaatimusten täyttäminen tuskin tulee vaatimaan erityisen suuria ponnisteluita.

Direktiivi koskettaa kuitenkin myös varsin suurta joukkoa eurooppalaisia organisaatioita, joiden kyberturvallisuuteen liittyviä toimenpiteitä ei ole aikaisemmin säännelty välttämättä lainkaan. Näille pääasiassa keskisuurille ja erityisesti uusille tai kasvuvaiheessa oleville organisaatioille direktiivi saattaa tuoda paljonkin pohdittavaa ja kehitettävää. Kyberturvallisuusriskien hallintatoimenpiteisiin liittyvien toimintamallien ja tarvittavan teknologian käyttöönotto tulee vaatimaan sekä rahaa että työpanosta. Kehittämällä kyberturvallisuutta tässä työssä esiteltyjen käytäntöjen mukaisesti organisaatiot voivat täyttää uuden direktiivin vaatimukset.

Erityisen ilahduttavaa oli huomata, että direktiivi pakottaa kyberturvallisuuden kertaheitolla myös organisaatioiden korkeimpien päättäjien agendalle. Tieto- ja kyberturvallisuus on joskus saatettu nähdä kalliina ja tuottamattomana kustannuseränä tai jopa toimintaa hidastavana jarruna, mutta järkevät panostukset turvallisuuteen maksavat itsensä moninkertaisena

takaisin. Historia tuntee yrityksiä, joiden liiketoiminta on kärsinyt peruuttamattomasti kyberturvallisuuden pettäessä ja onpa viime vuosina nähty jopa tietomurroista johtuvia konkursseja.

6.2 Opinnäytetyöprosessin onnistumisen ja luotettavuuden arviointi

Tutkimusmenetelmien luotettavuutta käsitellään yleensä validiteetin ja reliabiliteetin käsitteiden kautta. Validiteetilla tarkoitetaan sitä, että työssä on tutkittu sitä, mitä on tarkoituskin. Reliabiliteetilla tarkoitetaan työssä saatujen tutkimustulosten toistettavuutta. (Tuomi & Sarajärvi 2018, 160.) Edellä mainituista näkökulmista tarkasteltuna voidaan todeta, että valitut tutkimusmenetelmät ja varsin laaja tietoperusta edesauttavat sekä validiteetin, että reliabiliteetin toteutumista.

Johdantokappaleessa esitettyihin tutkimuskysymyksiin löydettiin vastaukset tutkimuksen aikana ja sisällönanalyysi sopi tutkimusmenetelmänä erinomaisesti kyberturvallisuusdirektiivin ja sen taustamateriaalien muodostaman tekstiaineiston analysointiin ja luokitteluun. Ensimmäisen tutkimuskysymyksen, eli sen millaisia organisaatioita direktiivi koskee, vastaus vaati direktiivin liitteiden ja direktiivissä viitattujen muiden Euroopan Unionin julkaisujen yhdistelemistä ja soveltamisalaan liittyvät reuna-ehdot ja toimialat onkin havainnollistettu kappaleessa 4 esitetyssä taulukossa 1. Toiseen ja kolmanteen tutkimuskysymykseen eli siihen, millaisia vaatimuksia direktiivi sisältää ja millaisin konkreettisin toimenpitein vaatimukset voidaan täyttää, vastaukset saatiin analysoimalla ja luokittelemalla direktiivin artiklat sekä yhdistämällä ne relevanttiin tietoperustaan eli kyberturvallisuuden käytäntöihin. Toiseen ja kolmanteen tutkimuskysymykseen on vastattu luvussa 5 siten, että kullekin vaatimukselle on esitetty yleisen tason toimenpide-ehdotukset.

Reliabiliteettia lisää yksityiskohtaisesti suunniteltu ja kuvattu tutkimusprosessi, jonka toistamalla tutkimustulosten tulisi olla hyvin samankaltaisia kuin tässä työssä. Tietoperusta muodostui laajasta joukosta kansainvälisesti tunnettuja ja laajasti hyödynnettyjä kyberturvallisuuteen liittyviä ohjeistoja ja artikkeleita. Lisäksi tietoperustaan valikoitiin tarkoituksellisesti sekä Yhdysvalloissa, Euroopassa, että kansainvälisestikin tuotettua aineistoa.

Itse opinnäytetyöprosessin tavoitteet saavutettiin hyvin ja erityisen antoisaa oli päästä tutustumaan tähän kyberturvallisuusalan kannalta mahdollisesti vuosikymmenen tärkeimpään lainsäädäntöuudistukseen. Hienoisia haasteita aiheutti alkuvaiheessa sopivan tietoperustan valitseminen, sillä kyberturvallisuudesta on viime vuosien aikana tuotettu paljon monen tasoista materiaalia. Suuri osa julkisista lähteistä löydettävästä kyberturvallisuuteen liittyvästä materiaalista ja ohjeistuksesta liittyy jonkin tietyn teknologian käyttöön ja sisältää markkinoinnillisia elementtejä. CSF-viitekehyksen, standardien sekä viranomaisjulkaisujen hyödyntäminen osana tietoperustaa helpotti valintaa huomattavasti.

Kyberturvallisuusdirektiivi tulee virallisesti voimaan vasta vuoden 2024 aikana, joten sen todellisia vaikutuksia on vaikea arvioida vielä tässä vaiheessa. Erityisen kiehtovana ja tarpeellisena jatkotutkimusaiheena voisi olla direktiivin varsinaisen käyttöönoton vaikutukset tietyn organisaation tai toimialan näkökulmasta. Tutkimuksessa voisi selvittää kuinka paljon uusi sääntely lopulta paransi kyberturvallisuutta kyseisessä organisaatiossa tai toimialalla. Laajempi tutkimuksen aihe voisi olla myös kansallinen tai koko Unionin kattava näkökulma siihen, onko direktiivin voimaantulon myötä kyberturvallisuuden poikkeamien aiheuttamat haitat todellisuudessa vähentyneet.

Lähteet

Painetut

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

Sanastokeskus TSK ry. 2017. Kokonaisturvallisuuden sanasto, 2.laitos. Helsinki: Sanastokeskus TSK.

Sanastokeskus TSK ry. 2018. Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK.

SFS-EN ISO 22301. 2019. Turvallisuus ja kriisinkestävyys. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen standardoimisliitto SFS ry.

SFS ISO 31000. 2018. Riskienhallinta. Ohjeet. Helsinki: Suomen standardoimisliitto SFS ry.

SFS ISO/IEC 27035-1. 2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvahäiriöiden hallinta. Osa 1: Tietoturvahäiriöiden hallinnan periaatteet. Helsinki: Suomen standardoimisliitto SFS ry.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.

Valtiovarainministeriö. 2022. Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri). Helsinki: Valtiovarainministeriö.

Sähköiset

Center for Internet Security 2021. CIS Critical Security Controls. Viitattu 27.2.2023 https://www.cisecurity.org/controls

Check Point 2023. Check Point Software's 2023 Cyber Security Report. Viitattu 28.2.2023. https://pages.checkpoint.com/cyber-security-report-2023.html

Cloud Security Alliance 2021. Cloud Controls Matrix (CCM). Viitattu 27.2.2023. https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Digi- ja väestötietovirasto 2022a. Digitaalisen turvallisuuden arkkitehtuuri. Viitattu 27.1.2023. https://wiki.dvv.fi/display/DTARK/Digitaalisen+turvallisuuden+arkkitehtuuri

Digi- ja väestötietovirasto 2022b. VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön. Viitattu 7.2.2023. https://sanastot.suomi.fi/concepts/b605bc12-1753-4284-8e26-8c68af82964c

Digi- ja väestötietovirasto 2022c. Kriittisten kohteiden luokittelu. Viitattu 1.3.2023. https://dvv.fi/documents/16079645/110183105/Kriittisten+kohteiden+luokittelu.xlsx/8e56cf5d-3102-53da-aa51-b87efb57a535?t=1647262341748

Digi- ja väestötietovirasto 2022d. Nollaluottamusmallin periaatteet. Viitattu 28.2.2023. https://wiki.dvv.fi/display/DTARK/Nollaluottamusmallin+periaatteet

Digi- ja väestötietovirasto 2023a. Tietoa virastosta. Viitattu 26.3.2023. https://dvv.fi/digi-ja-vaestotietovirasto

Digi- ja väestötietovirasto 2023b. Digiturvapalvelut. Viitattu 27.1.2023. https://dvv.fi/digi-turva

Digi- ja väestötietovirasto 2023c. VAHTI-verkosto kehittää digitaalista turvallisuutta. Viitattu 19.3.2023. https://dvv.fi/vahti

Digi- ja väestötietovirasto 2023d. Digiturvallinen elämä -koulutuskokonaisuus. Viitattu 12.3.2023. https://dvv.fi/digiturvallinen-elama

Direktiivi 2016/1148/EU: Ns. NIS-direktiivi. Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Euroopan unionin virallinen lehti 19.7.2016. Viitattu 7.2.2023. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Direktiivi 2022/2555/EU: Ns. kyberturvallisuusdirektiivi. Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi). Euroopan unionin virallinen lehti 27.12.2022. Viitattu 7.2.2023. https://eur-lex.europa.eu/eli/dir/2022/2555

ENISA 2023a. Tietoa Euroopan unionin kyberturvallisuusvirastosta (ENISA). Viitattu 11.3.2023. https://www.enisa.europa.eu/about-enisa/about/fi

ENISA 2023b. Vulnerabilities and Exploits. Viitattu 28.2.2023. https://www.enisa.europa.eu/topics/incident-response/glossary/vulnerabilities-and-exploits

ENISA 2023c. Learn more about EU Cybersecurity Certification. Viitattu 12.3.2023. https://www.enisa.europa.eu/topics/certification/eu-cybersecurity-certification-faq

Euroopan komissio 2023. Mitä tarkoittaa 'sisäänrakennettu' ja 'oletusarvoinen' tietosuoja. Viitattu 12.3.2023. https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_fi

Euroopan Unioni 2016. Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoitu toisinto. Viitattu 7.2.2023. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:12016E288

Huoltovarmuuskeskus 2023. Jatkuvuudenhallinta. Viitattu 1.3.2023. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta

Laki Liikenne- ja viestintävirastosta 935/2018. Viitattu 19.3.2023. https://finlex.fi/fi/laki/alkup/2018/20180935

Liikenne- ja viestintävirasto Traficom 2020a. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 27.2.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Liikenne- ja viestintävirasto Traficom 2020b. Haavoittuvuudet - miten niistä ilmoitetaan oikein. Viitattu 28.2.2023. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein

Liikenne- ja viestintävirasto Traficom 2023a. Kybermittari. Viitattu 27.2.2023 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

Liikenne- ja viestintävirasto Traficom 2023b. Ilmoita meille. Viitattu 28.2.2023. https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Liikenne- ja viestintävirasto Traficom 2023c. ISAC-tiedonvaihtoryhmät. Viitattu 2.3.2023. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/isac-tiedonvaihtoryhmat

MISP project 2023. Open-source threat intelligence and sharing platform. Viitattu 27.2.2023. https://www.misp-project.org

National Institute of Standards and Technology 2018. Framework for Improving Critical Infrastructure Cybersecurity. Viitattu 28.2.2023. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Institute of Standards and Technology 2020. Security and Privacy Controls for Information Systems and Organizations. Viitattu 28.2.2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

National Institute of Standards and Technology 2023a. Cybersecurity Framework. Viitattu 27.1.2023. https://www.nist.gov/cyberframework/framework

National Institute of Standards and Technology 2023b. Getting started. Viitattu 26.3.2023. https://www.nist.gov/cyberframework/getting-started#background

Oasis Open 2021a. STIX Version 2.1. Viitattu 2.3.2023. https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

Oasis Open 2021b. TAXII Version 2.1. Viitattu 2.3.2023. https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html

OWASP 2023. Projects. Viitattu 27.2.2023. https://owasp.org/projects

Tieteen termipankki 2023. Oikeustiede:lain soveltamisala. Viitattu 11.3.2023. https://tieteentermipankki.fi/wiki/Oikeustiede:lain_soveltamisala

U.S. Department of Defence 2021. DoD Enterprise DevSecOps Fundamentals. Viitattu 28.2.2023. https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Fundamentals.pdf

VAHTI 2016. Toiminnan jatkuvuuden hallinta. Viitattu 1.3.2023. https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2016_pdf.pdf

Valtioneuvosto 2023. Kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallinen täytäntöönpano. Viitattu 25.3.2023. https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022

Valtioneuvoston asetus Digi- ja väestötietovirastosta 30.1.2020/53. Viitattu 19.3.2023. https://www.finlex.fi/fi/laki/ajantasa/2020/20200053

Verizon 2021. Data Breach Investigations Report. Viitattu 12.3.2023. https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

Kuviot

Taulukot