



Satakunnan ammattikorkeakoulu  
Satakunta University of Applied Sciences

TEEMU VARTIO

# **Kyberturvallisuuden sääntely Suomessa - NIS2-direktiivi**

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN  
TUTKINTO-OHJELMA  
2024

## TIIVISTELMÄ

Vartio Teemu: Kyberturvallisuuden sääntely Suomessa - NIS2-direktiivi  
Opinnäytetyö, AMK  
Tutkinto-ohjelma: Sähkö- ja automaatiotekniikka  
Lokakuu 2024  
Sivumäärä: 24

Valitsin NIS2-direktiivin opinnäytetyöni aiheeksi aiheen ajankohtaisuuden ja oman kiinnostukseni kyberturvallisuuteen vuoksi.

Tämän opinnäytetyön tarkoituksena oli selvittää mitä sääntelyä NIS2-direktiivi sisältää ja mitä konkreettisia toimenpiteitä se edellyttää yrityksiltä. Aihetta tuetaan esittelemällä jo olemassa olevia Suomea koskevia kyberturvallisuuteen liittyviä sääntelyitä ja säännöksiä.

Opinnäytetyössä keskityin erityisesti NIS2-direktiivin tärkeimpiin ja keskeisiin kohtiin, jotka mielestäni ovat olennaisimpia sekä yrityksille että muille toimijoille. NIS2-direktiivi on laaja, mutta pyrin nostamaan esiin ne seikat, jotka ovat merkityksellisiä yritysten näkökulmasta.

Opinnäytetyön tarkoituksena oli toimia tiivistelmänä ja johdatuksena aiheeseen, joten se on suunnattu kaikille, jotka ovat kiinnostuneita NIS2-direktiivistä ja kyberturvallisuuden sääntelystä. Opinnäytetyön toteutuksen aikana NIS2-direktiivin säännösten soveltaminen kansallisessa lainsäädännössä ei ollut vielä alkanut.

Avainsanat: kyberturvallisuus, sääntely, NIS2-direktiivi

## ABSTRACT

Vartio Teemu: Regulation of cyber security in Finland - NIS2 directive  
Bachelor's thesis  
Electrical and Automation Engineering  
October 2024  
Number of pages: 24

I chose the NIS2 Directive as the topic for my thesis due to the relevance of the subject and my personal interest in cybersecurity.

The purpose of this thesis was to explore the regulations included in the NIS2 Directive and the concrete actions it requires from companies. The topic is supported by presenting existing regulations and laws related to cybersecurity that apply to Finland.

In my thesis, I focused particularly on the most important and central points of the NIS2 Directive, which I believe are the most essential for companies and other actors. While the NIS2 Directive is broad, I aimed to highlight the aspects that are most significant from a business perspective.

The thesis was intended to serve as a summary and introduction to the topic, so it is directed at anyone interested in the NIS2 Directive and cybersecurity regulations. During the preparation of the thesis, the application of the NIS2 Directive's provisions in national legislation had not yet begun.

Keywords: cybersecurity, regulation, NIS2 Directive

# SISÄLLYS

1 JOHDANTO .....	5
2 KYBERTURVALLISUUDEN SÄÄNTELY SUOMESSA.....	6
2.1 ENISA.....	6
2.2 Euroopan unionin kyberturvallisuusasetus .....	7
2.3 Yleinen tietosuojalaki (GDPR).....	7
2.4 Euroopan unionin verkko- ja tietoturva direktiivi .....	8
2.5 Tietosuojalaki .....	8
2.6 Laki sähköisen viestinnän palveluista.....	9
2.7 ISO/IEC 27001 .....	9
2.8 Kyberturvallisuuskeskus .....	9
3 NIS2-DIREKTIIVI .....	10
3.1 Direktiivit yleisesti .....	10
3.2 Taustaa .....	11
3.3 Soveltamisala .....	12
3.4 Riskienhallintavelvoite .....	13
3.5 CSIRT-yksikkö.....	16
3.6 Raportointivelvoite .....	17
3.7 Valvonta ja sakot .....	18
3.8 Kyberturvallisuusstrategia .....	20
4 LOPPUPÄÄTELMÄ.....	21
LÄHTEET .....	23

## 1 JOHDANTO

Suomessa kyberturvallisuus on osa kansallista turvallisuutta. Kyberturvallisuudella tarkoitetaan prosesseja, käytäntöjä ja teknologiaratkaisuja, joilla suojataan järjestelmiä ja verkkoja digitaalisilta hyökkäyksiltä. (Microsoft, n.d; Sisäministeriö, n.d.). Tämän opinnäytetyön tavoitteena on selvittää mitä tuleva NIS2-direktiivi pitää sisällään ja mitä yrityksiltä vaaditaan niiden toteuttamiseen Suomessa. Kyberturvallisuus on käsitteenä laaja ja tämän opinnäytetyön aihe rajataan koskemaan kyberturvallisuuteen liittyvää sääntelyä ja säännöksiä.

Pohjustan aihetta kertomalla aluksi yleisasiaa kyberturvallisuuteen liittyvästä sääntelystä Suomessa. Tämän jälkeen kerron yleisesti jo olemassa olevia kyberturvallisuuteen liittyviä säännöksiä. Suomi kuuluu Euroopan unioniin ja tämän seurauksena moni näistä olemassa olevista sääntelyistä tulee Euroopan unionista kuin myös Suomen omasta lainsäädännöstä. Tämän jälkeen kerron mitä sääntelyä NIS2-direktiivi pitää sisällään, ketä tämä sääntely koskee ja mitä suomessa toimivilta yrityksiltä vaaditaan niiden toteuttamiseen. Kerron myös oman näkemykseni miten tietyt velvoitteet voidaan ratkaista. NIS2-direktiivi on laaja ja käyn direktiivistä läpi vain mielestäni keskeisimmät ja tärkeimmät asiat.

Opinnäytetyön selkeyden vuoksi käytän suomenkielistä sanastoa, vaikka kyberturvallisuudesta kirjoittaessa olisi mielestäni mielekkäämpää käyttää englanninkielistä sanastoa. Motivaatio tämän opinnäytetyön tekemiseen tuli omasta kiinnostuksesta kyberturvallisuuteen.

## 2 KYBERTURVALLISUUDEN SÄÄNTELY SUOMESSA

Kyberturvallisuuden sääntely on yksi kyberturvallisuuden kulmakivistä. Se kattaa erilaisia lainsäädännöllisiä ja normatiivisia toimenpiteitä, joilla pyritään suojaamaan digitaalista infrastruktuuria ja tietojärjestelmiä sekä varmistamaan tietojen luottamuksellisuus ja saatavuus. Kyberturvallisuuden sääntely on jatkuvassa muutoksessa uusien teknologioiden kehittyessä ja vaatii jatkuvaa seuranta ja sopeutumista näiden teknologioiden tuomiin tarpeisiin.

Suomen ja Suomessa toimivien yritysten kyberturvallisuuden sääntelyyn vaikuttavat Suomen lainsäädäntö, Euroopan unionin direktiivit ja päätökset, tietoturvallisuuden standardoinnit ja kansalliset sopimukset.

### 2.1 ENISA

Euroopan unionin kyberturvallisuusvirasto ENISA perustettiin vuonna 2004 ja sen tavoitteena on saavuttaa korkea kyberturvallisuuden taso Euroopan unionissa. ENISA osallistuu kyberturvallisuuspolitiikan kehittämiseen, edistää tuotteiden ja palvelujen turvallisuutta erilaisilla kyberturvallisuuden sertifiointijärjestelmillä. Tiedonjakamisen, osaamisen kehittämisen ja tietoisuuden lisäämisen avulla virasto työskentelee yhdessä sidosryhmien kanssa turvataksaan Euroopan unionin kansalaisten ja yhteiskunnan digitaalisen turvallisuuden. (ENISA, n.d.)

ENISAn merkitys Euroopan unionin kyberturvallisuudelle on voimistunut viime vuosina huomattavasti. Teknologian kehittymisen seurauksena kyberuhat ovat monimutkaistuneet ja vaativat jatkuvaa tarkkailua. ENISAn ollessa Euroopan unionin keskeinen kyberturvallisuudesta vastaava elin on sen pakko pysyä ajan tasalla uusista teknologioista ja kyberuhista. Näin se pystyy varmistamaan, että Euroopan unionilla on ajantasaiset ja tehokkaat työkalut ja toimiva kyberturvallisuuspolitiikka ja näiden avulla Euroopan unioni pysyy turvallisena ja kykenee puolustautumaan kyberuhkia vastaan.

## 2.2 Euroopan unionin kyberturvallisuusasetus

Euroopan unionin kyberturvallisuusasetus tuli käytäntöön kesäkuussa 2019. Asetuksen tarkoituksena oli parantaa kyberturvallisuutta Euroopan unionissa. Asetus koostui kahdesta pääelementistä, ENISAn aseman vahvistaminen ja eurooppalaisen kyberturvallisuussertifiointijärjestelmän luominen. Asetus muutti ENISAn toimeksiannon määräaikaisesta pysyväksi ja antoi sille enemmän resursseja ja vastuuta kyberturvallisuusasioissa. Asetus asettaa sertifiointikehyksen, jossa tieto- ja viestintätekniikan tuotteita, palveluita ja prosesseja voidaan sertifioida. Sertifikaatti osoittaa tuotteen täyttävän tietyt vaatimukset koko elinkaarensa ajan. Sertifikaatti tunnustetaan koko Euroopan unionissa ja tuote ei tarvitse useita kansallisia sertifikaatteja. (Tietoturvamerkki, 2024; Wahl, 2019)

Asetus oli laaja kyberturvallisuuden kehitysohjelma ja se luotiin vastaamaan kasvavaan kyberuhkien määrään. ENISAn aseman parannuksen seuraksensa luotiin yhteiset työkalut ja kyberturvallisuuspolitiikka parantamamaan Euroopan unionin kyberturvallisuutta. Sertifiointijärjestelmän avulla lisättiin digitaalisten palvelujen ja tuotteiden turvallisuutta.

## 2.3 Yleinen tietosuoja-asetus (GPDR)

Yleinen tietosuoja-asetus on Euroopan unionin asettama säädös, joka tuli käytäntöön toukokuussa 2018. Asetus sisältää uusia sääntöjä, joiden tarkoituksena on antaa Euroopan unionin kansalaisille enemmän hallintavaltaa omiin henkilötietoihin. Sen tavoitteena on yksinkertaistaa liiketoimintojen sääntelyä, jotta yritykset ja kansalaiset voivat täysmääräisesti hyötyä digitaalisesta taloudesta. (Palmer, 2019)

Yleisen tietosuoja-asetuksen seurauksena yksilölle turvattiin useita oikeuksia:

- Tiedon saanti oikeus. Henkilölle turvattiin oikeus saada tietää kaikki tiedot mitä hänestä kerätään ja mihin näitä kerättyjä tietoja käytetään.
- Tiedon oikaisu. Henkilölle turvattiin oikeus vaatia virheellisten tietojen korjaamista.

- Oikeus tulla unohdetuksi. Henkilölle turvattiin oikeus pyytää kaikkien tietojensa poistoa rekistereistä.

Näiden lisäksi asetuksessa määriteltiin henkilötietojen rekisterinpitäjän ja käsittelijän vastuita ja henkilötietojen väärinkäytöstä tulevia seuraamuksia.

## 2.4 Euroopan unionin verkko- ja tietoturva direktiivi

Euroopan unionin verkko- ja tietoturva direktiivi on Euroopan unionin asettama säädös, joka tuli käytäntöön elokuussa 2016. Direktiivin tavoitteena on luoda sääntöjä, jotka parantavat kokonaisvaltaisesti tietoturvan tasoa Euroopan unionissa. Tämä direktiivi oli ratkaiseva vaihe tietoturvamääräyksien kehittämisessä Euroopan unionissa. Sen tarkoituksena oli vahvistaa kriittisten infrastruktuurien ja olennaisten digitaalisten palvelujen kestävyyttä kyberuhkia vastaan. Direktiivi edellytti merkittävien tietoturvaloukkauksien ilmoittamista, mikä helpotti uhkatietojen jakamista. (Sadoian, 2023).

Direktiivin seurauksena yhteiskunnan kannalta kriittiset yritykset joutuivat parantamaan kyberturvallisuuttaan ja tietoturvakäytäntöjään. Näiden toimenpiteiden ansiosta varautuminen kyberuhkia vastaan vahvistui, mutta samalla myös yrityksen kustannukset kasvoivat ja yritykset joutuivat käyttämään resursseja kyberturvallisuuden parantamiseksi. Kriittisiä aloja olivat esimerkiksi energiantuottajat, pankkitoiminta ja terveydenhuolto. Tuleva NIS2-direktiivi korvaa tämän direktiivin asettaen laajemman soveltamisalan ja lisäämällä sääntöjä.

## 2.5 Tietosuojalaki

Tietosuojalaki säätelee henkilötietojen käsittelyä ja tietojen vapaata liikkuvuutta Suomessa. Laki perustuu Euroopan unionin yleiseen tietosuoja-asetukseen ja täydentää sitä kansallisella tasolla. Tietosuojalaki koskee kaikkia yrityksiä, jotka käsittelevät henkilötietoja Suomessa. (Finlex, 2018)



## 2.6 Laki sähköisen viestinnän palveluista

Laki sähköisen viestinnän palveluista säätelee sähköisen viestinnän palvelujen tarjontaa ja käyttöä Suomessa. Lain tavoitteena on edistää viestintäverkkojen ja palvelujen kehitystä, käytettävyyttä ja turvallisuutta. Lain tavoitteena on myös turvata sähköisen viestinnän luottamuksellisuus ja yksityisyydensuojan toteutuminen. (Finlex, 2014)

Laki sähköisen viestinnän palveluista on erittäin tärkeä digitalisoituvassa maailmassa, koska se suojaa käyttäjien yksityisyyttä ja henkilötietoja. Laki takaa käyttäjille turvalliset ja luotettavat viestintäpalvelut ja lain puitteissa näitä viestintäpalvelujen tarjoajia valvotaan jatkuvasti.

## 2.7 ISO/IEC 27001

ISO/IEC 27001 on maailman tunnetuin standardi tietoturvan hallintajärjestelmiin. Standardi tarjoaa ohjeita yrityksille koosta ja toimialasta riippumatta tietoturvan hallintajärjestelmän perustamiseen, käyttöönottoon, ylläpitoon ja jatkuvaan parantamiseen. Standardin noudattaminen tarkoittaa, että organisaatio tai yritys on ottanut käyttöön järjestelmän hallitakseen siihen kuuluvien tietojen turvallisuuteen liittyviä riskejä. Lisäksi tämä järjestelmä noudattaa kaikkia parhaita käytäntöjä ja periaatteita, jotka on määritelty tässä standardissa. (ISO, n.d.)

## 2.8 Kyberturvallisuuskeskus

Kyberturvallisuuskeskus on Liikenne- ja viestintäministeriöön kuuluva viranomainen, jonka tarkoituksena on valvoa viestintäverkkojen ja palvelujen turvallisuutta Suomessa. Kyberturvallisuuskeskus luo kyberturvallisuuteen liittyviä määräyksiä ja suosituksia sekä neuvoo yrityksiä kyberturvallisuuteen liittyvissä asioissa. (Kyberturvallisuuskeskus, 2024)

### 3 NIS2-DIREKTIIVI

Direktiivi yhteisistä toimenpiteistä korkeatasoisen kyberturvallisuuden varmistamiseksi unionissa on Euroopan unionin laajuinen kyberturvallisuutta koskeva lainsäädäntö. Direktiivissä säädetään oikeudellisista toimenpiteistä, jolla kyberturvallisuuden tasoa parannetaan Euroopan unionissa. (European Commission, 2023)

Euroopan unionin vuonna 2016 käyttöön otettuja kyberturvallisuussäätöjä päivitettiin NIS2-direktiivillä, jotka tulivat voimaan vuonna 2023. Sillä nykyaikaistettiin nykyistä oikeudellista kehystä pysyäkseen lisääntyvän digitalisoinnin ja kehittyvän kyberturvallisuushkien mukana. Laajentamalla kyberturvallisuus sääntöjen soveltamista uusiin aloihin ja toimijoihin se parantaa julkisten ja yksityisten tahojen, toimivaltaisten viranomaisten ja koko Euroopan unionin kestävyttä ja valmiutta häiriötilanteisiin. (European Comission, 2023)

NIS2-direktiivi on Euroopan unionin lainsäädäntö. Se korvaa aiemman Euroopan unionin verkko- ja tietoturva direktiivin ja asettaa tiukemmat ja laajemmat vaatimukset kyberturvallisuuden osalta. Direktiivin tarkoituksena on parantaa koko Euroopan unionin kyberturvallisuutta, vähentää kyberuhkia ja varmistaa kriittisten palveluiden jatkuvuus kriittisissä tilanteissa. Jäsenvaltiot ovat veloitettuja toteuttamaan direktiivin määrittämät vaatimukset lainsäädäntöönsä, jonka seurauksena yritykset ovat velvollisia noudattamaan kyseisiä vaatimuksia. Jäsenvaltioiden on sovellettava direktiivissä olevia säännöksiä omassa lainsäädännössään 18.10.2024 alkaen. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 41 art.)

#### 3.1 Direktiivit yleisesti

Direktiivi on Euroopan unionin toimielinten hyväksymä Euroopan unionin jäsenvaltioille tarkoitettu säädös. Direktiivi on osa Euroopan unionin johdettua lainsäädäntöä, joka perustuu Euroopan unionin perussopimuksissa asetettuihin periaatteisiin ja tavoitteisiin. Kunkin Euroopan unionin maiden

viranomaiset, joille direktiivi on osoitettu määrittävät missä muodossa ja millä menetelmillä direktiivi sisällytetään osaksi oman maan lainsäädäntöä. (EUR-Lex, n.d.)

### 3.2 Taustaa

Euroopan unionin verkko- ja tietoturva direktiivin voimaantulon jälkeen Euroopan unionin kybervalmius on parantunut merkittävästi. Tarkastelu on osoittanut, että direktiivi on tehostanut institutionaalista ja sääntelyyn perustuvaa lähestymistapaa kyberturvallisuudessa, luoden muutoksen ajattelutavassa. Direktiivillä on parannettu verkko- ja tietojärjestelmien turvallisuutta täydentämällä niitä kansallisilla turvallisuutta parantavilla strategioilla. Direktiivillä on parannettu Euroopan unionin maiden välistä yhteistyötä perustamalla yhteistyöryhmä, ja tietoturvaloukkauksiin reagoivat ja tutkivat kansalliset yksiköt. Saavutuksista huolimatta direktiivin uudelleentarkastelussa on tullut esiin puutteita, jotka estävät sen tehokkaan käytön nykyisiin ja uusiin kyberturvallisuuden haasteisiin. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, Johdanto)

### 3.3 Soveltamisala

#### NIS2 toimialat (uudet punaisella)

##### Liite I

- Energia (vety- ja latauspisteiden palveluntarjoajat)
- Liikenne
- Pankkitoiminta
- Finanssimarkkinoiden infrastruktuuri
- Terveys
- Juomavesi
- Jätevesi
- Digitaalinen infrastruktuuri (tele, luottamuspalvelut, CDN, konesalit)
- TVT-palvelujen hallinta (yritysten välinen)
- Julkishallinto
- Avaruus



11 26.10.2023

##### Liite II

- Posti- ja kuriiripalvelut
- Jätehuolto
- Kemikaalien valmistus, tuotanto ja jakelu
- Elintarvikkeiden tuotanto, jalostus ja jakelu
- Valmistus (mm. lääkinnälliset laitteet, tietokoneet sekä elektroniset ja optiset laitteet, sähkölaitteet, muut koneet ja laitteet sekä kulkuneuvot)
- Digitaalisen palvelun tarjoajat (verkkoyhteisöalustojen tarjoajat)
- Tutkimustoiminta

Kuva 1. NIS2-direktiivin toimialat. Keskeiset toimialat vasemmalla, tärkeät oikealla. (Liikenne- ja viestintäministeriö, 2023)

Direktiivin mukaan direktiiviä sovelletaan yritykseen, joka harjoittaa (kuva 1) tarkoitettua liiketoimintaa ja täyttää Euroopan unionin keskisuuren yrityksen kynnysarvot. Direktiiviä sovelletaan myös yrityksiin, jotka ylittävät keskisuuren yrityksen kynnysarvot. Näin ollen direktiivin soveltamisen piiriin kuuluvat yritykset, jos yrityksessä on vähintään 50 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enemmän kuin 10 miljoonaa euroa. Lisäksi direktiiviä sovelletaan automaattisesti yrityksiin, joissa on yli 250 työntekijää riippumatta yrityksen liikevaihdosta. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 2 art ; Prokyberturva, n.d.).

Poikkeuksena direktiiviä sovelletaan (kuva 1) tarkoitettua toimijatyyppiä oleviin toimijoihin koosta riippumatta, jos toimitsijan palvelu luokitellaan seuraaviin palveluihin:

- Julkiset sähköiset verkot. Julkiset sähköiset verkot palvelun tarjoajalla tarkoitetaan yritystä, jonka toiminta kohdistuu sähköverkkoihin.
- Julkiset sähköiset viestintäpalvelut. Julkiset sähköiset viestintäpalvelut palvelun tarjoajalla tarkoitetaan yritystä, jonka toiminta kohdistuu

sähköiseen viestintään eli esimerkiksi puhelin- ja tekstiviestipalvelut, internetin palvelun tarjoajat ja viestintäsovellukset.

- Luottamuspalvelut. Luottamuspalvelun tarjoajalla tarkoitetaan yritystä, jonka toiminta kohdistuu sähköisten allekirjoitusten ja varmenteiden myöntämiseen.
- Aluetunnusrekisterit. Aluetunnusrekisterin palvelun tarjoajalla tarkoitetaan yritystä, jonka toiminta perustuu fi-verkkotunnuksen hallintaan.
- Nimipalvelujärjestelmät. Nimipalvelujärjestelmän tarjoajalla tarkoitetaan yritystä, jonka toiminta kohdistuu Internetin nimipalvelujärjestelmään eli esimerkiksi muuntavat verkko-osoitteet IP-osoitteeksi.
- Keskustason julkishallinnon toimijat. Keskustason julkishallinnon toimijoilla tarkoitetaan Suomen valtion viranomaisia, jotka ohjaavat toimintaa maassa. Tähän sisältyvät esimerkiksi ministeriöt.
- Verkkotunnusten rekisteröintipalvelut. Verkkotunnusten rekisteröintipalvelun tarjoajalla tarkoitetaan yritystä, jonka toiminta kohdistuu verkkotunnusten rekisteröinti, käyttöönotto ja ylläpito palveluihin.
- Direktiivin (EU) 2022/2557 mukaan kriittiseksi määritetyt yritykset.
- Kaikki yritykset, jotka Suomen viranomaiset ovat määränneet noudattamaan direktiiviä.

(Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 2 art.)

Direktiivin soveltamisalaa on laajennettu huomattavasti aikaisempaan direktiiviin verrattuna. Näin laajan soveltamisalan takia direktiivin piiriin kuuluu suuri määrä uusia yrityksiä, jotka joutuvat huomioimaan direktiivissä olevat asiat toiminnassaan.

### 3.4 Riskienhallintavelvoite

Direktiivi velvoittaa yritykset toteuttamaan riskienhallintasuunnitelman hallitakseen riskejä, joita yrityksen käyttämiin verkko- ja tietojärjestelmien turvallisuuden kohdistuu. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 21 art.). Riskienhallintasuunnitelma koostuu seuraavista asioista ja miten ne käsitellään ja hoidetaan yrityksessä:

- riskianalyysit
- poikkeamien käsittely
- tiedon varmuuskopiointi ja palautumissuunnitelma
- kriisinhallinta
- toimitusketjun turvallisuus
- verkko- ja tietojärjestelmien turvallisuus
- kyberturvallisuuskoulutus
- tiedon salaamiseen liittyvät toimenpiteet
- henkilöstöturvallisuus
- pääsynhallinta
- omaisuudenhallinta
- toimenpiteet, joilla arvioidaan riskienhallinsuunnitelman tehokkuutta.

Riskianalyyseillä tarkoitetaan toimenpiteitä, joiden tarkoituksena on tunnistaa ja arvioida tietoturvallisuuteen ja tietoverkkojen käyttöön liittyviä riskejä. Nämä analyysit auttavat organisaatioita suojautumaan kyberuhkia vastaan ja vähentämään tietoturvapoikkeamien vaikutuksia.

Palautumissuunnitelmalla tarkoitetaan, että yrityksellä on selkeä ja testattu palautumissuunnitelma kyberhyökkäyksen varalta. Palautumissuunnitelman tavoite on saada tietojärjestelmät ja tiedot mahdollisimman nopeasti toimintaan häiriön tapahduttua ja miten toimintaa voidaan jatkaa häiriön aikana. Esimerkkinä liikenteen alalla, miten varmistetaan junalippujen varausjärjestelmän toimiminen häiriön sattuessa tai miten tarkastetaan junalipun aitous, jos lipun tarkastus järjestelmässä on häiriö.

Toimitusketjun turvallisuudella tarkoitetaan tässä yhteydessä, että yrityksen alihankkijoiden ja kumppaneiden kyberturvallisuus on hallinnoitu asianmukaisesti ja toimitusketjun kaikki osat noudattavat turvallisuusvaatimuksia. Hyvänä esimerkkinä, tehdään kriittisessä kohteessa työskentelevälle alihankkijalle turvallisuus selvitys ennen kuin alihankkija aloittaa työt kohteessa. Toisena esimerkkinä yritys on tilannut alihankkijalta uusia tietokoneita, joten alihankkijan on varmistettava, että se myy vain turvallisia tietokoneita. Tähän voidaan lisätä vielä toisen alihankkijan tekemä kuljetus, joten tietokoneita kuljettavan

yrittäjien on huolehdittava, että kukaan ei pääse käpälöimään tietokoneita kuljetuksen aikana.

Kyberturvallisuuskoulutus on ratkaisevassa asemassa NIS2-direktiivin mukaisen kyberturvallisuuden kehittämisessä. Koska iso osa kyberhyökkäyksistä kohdistuu inhimillisiin heikkouksiin, työntekijöiden osaaminen ja tietoisuus riskeistä ovat keskeisiä puolustuskeinoja kyberuhkia vastaan. Kyberturvallisuuskoulutukset voivat esimerkiksi opettaa työntekijöille, miten tunnistetaan tietojenkalasteluyritykset ja miten ne vältetään. Koulutuksessa voidaan kertoa myös yleisistä haittaohjelmista ja miten ne leviävät. Näiden lisäksi työntekijöille voidaan opettaa turvallista salasanojen hallintaa, monivaiheisen tunnistautumisen käyttöä ja miten arkaluotoisia tietoja käsitellään.

Tiedon salaamiseen liittyvät toimenpiteet koskevat erityisesti keskeisten toimialojen yrityksiä. Tietojen salaaminen on yksi kyberturvallisuuden perustarpeista. Se varmistaa tietojen pysyvän suojattuna, vaikka tiedot joutuisivat väärin käsiin. Käytössä tulee olla vahvat salaustekniikat tiedon tallentamisessa ja tiedonsiirtoa käytettäessä.

Henkilöstöturvallisuudella tarkoitetaan työntekijöiden toiminnasta syntyvien riskien hallitsemista. Henkilöturvallisuuteen voi liittyä työntekijän taustatarkastukset sekä prosessit, joiden avulla valvotaan työntekijän tekemistä.

Pääsynhallinnalla tarkoitetaan prosesseja, miten käyttöoikeuksia ja pääsyoikeuksia hallitaan ja valvotaan. Pääsynhallinnassa voidaan käyttää vähimmän oikeuden periaatetta eli annetaan työntekijälle vain välttämättömät oikeudet työtehtävien hoitamiseksi. Pääsynhallinnassa voidaan käyttää myös monivaiheista tunnistautumista. Näiden lisäksi pääsynhallinta voi koostua valvonnasta ja lokitietojen keräämisestä. Käyttöoikeuksia olisi hyvä tarkastella säännöllisesti, jotta oikeudet pysyvät tarpeenmukaisina ja turhat käyttöoikeudet voidaan poistaa.

Omaisuuksienhallinnalla tarkoitetaan prosesseja, joiden avulla yritys suojaa omaisuuttaan. Omaisuuksienhallintaan voi liittyä tässä tapauksessa

järjestelmien tunnistaminen ja luokittelu sekä omaisuudelle tarvittavien turvallisuusvaatimusten laatiminen.

Riskienhallintasuunnitelman laatua ja tehokkuutta olisi hyvä arvioida säännöllisesti. Suunnitelmaa voidaan arvioida monella tavalla. Esimerkiksi erilaisilla mittareilla, jotka voivat sisältää esimerkiksi tietoturvailmoitusten määrän tai korjaavien toimintojen käyttöön saattamisen vasteajan. Arviointia voidaan myös teettää kolmannen osapuolen auditoinneilla ja tarkastuksilla kuin myös teettämällä työntekijöille kyberturvallisuusharjoituksia, miten toimitaan tilanteen sattuessa.

Riskienhallintasuunnitelmaa luodessa on otettava huomioon, että verkko- ja tietojärjestelmien turvallisuuden tulee olla tasapainossa niiden kohtaamien riskien kanssa. Arvioitaessa näiden toimenpiteiden asianmukaisuutta on huomioitava toimijan koko, kuinka paljon toimija altistuu riskeille, mahdollisten poikkeamien esiintymistiheys, sekä poikkeamien yhteiskunnalliset ja taloudelliset vaikutukset. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 21 art.).

Viranomaisten on varmistettava, että yritykset noudattavat riskienhallintavelvoitetta ja toteuttavat riskienhallintasuunnitelman. Jos yritys ei noudata riskienhallintavelvoitetta on varmistettava, että yritys toteuttaa korjaavat toimenpiteet ilman aiheetonta viivästystä. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 21 art.).

### 3.5 CSIRT-yksikkö

CSIRT eli Tietoturvaloukkausten hallintaryhmä on tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö. CSIRT-yksikön tehtävänä on kyberuhkien, haavoittuvuuksien ja poikkeamien seuranta ja analysointi sekä yritysten avustaminen. Näiden lisäksi yksikkö ylläpitää kokonaiskuvaa kyberturvallisuuden tasosta ja jakaa tietoa muiden CSIRT-yksikköjen kanssa. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 11 art.).



Suomen CSIRT-yksikkönä toimii Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. (Liikenne- ja viestintäministeriö, 2023)

### 3.6 Raportointivelvoite

Direktiivissä määritetään raportointivelvoitteesta, joka velvoittaa yritykset raportoimaan kyberturvallisuuden poikkeamista. Yritysten on tiedotettava palvelujensa käyttäjille kyberuhasta sekä mahdollisista jatkotoimenpiteistä mitä käyttäjät voivat tehdä uhan pienentämiseksi. Yritysten on myös ilmoitettava käyttäjille kyberuhasta itsestään, jos se on merkittävä. Poikkeama luokitellaan merkittäväksi, jos se on aiheuttanut tai voisi aiheuttaa palvelun vakavan häiriön tai yritykselle taloudellista menetyksiä sekä tilanteet, joissa luonnollisiin henkilöihin tai oikeushenkilöihin aiheutuu tai voisi aiheutua vahinkoa. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 23 art.).

Merkittävillä poikkeamilla on kolmiportainen raportointivelvoite, ja raportointi tehdään CSIRT-yksilölle tai muulle toimivaltaiselle viranomaiselle. Ensimmäinen raportti on tehtävä vähintään 24 tunnin kuluessa siitä, kun yritys on tullut tietoiseksi poikkeamasta. Toinen raportti on tehtävä 72 tunnin kuluessa siitä, kun yritys on tullut tietoiseksi poikkeamasta ja raportissa on esitettävä arvio poikkeaman vakavuudesta ja vaikutuksista. Loppuraportti tehdään viimeistään kuukauden kuluttua toisen raportin toimittamisesta. Loppuraportti pitää sisällään tiedot poikkeamasta, sen vakavuudesta ja vaikutuksista ja poikkeaman aiheuttaneen uhan tyypin ja toteutetut toimenpiteet vaikutuksien lieventämiseksi sekä tapauksen mukaan poikkeaman rajat ylittävät vaikutukset. CSIRT-yksikkö tai muu toimivaltainen viranomainen voi halutessaan pyytää väliraportteja tilannepäivityksistä. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 23 art.).

Raportointivelvoitteen täytäntöönpano vaatii yritykseltä suunnittelu ja prosessien kehittämistä. Yrityksen tulee nimetä vastuuhenkilö tai tiimi, joka vastaa yrityksen kyberturvallisuuteen liittyvästä valvonnasta, raportoinnista ja viranomaisyhteistyöstä. Vastuuhenkilönä voi toimia esimerkiksi tieturvapäällikkö tai

yrittäjien voidaan perustaa erillinen tiimi hoitamaan kyberturvallisuuteen liittyvät asiat.

Yrityksen tulee myös määrittää selkeä prosessi, miten tietoturvaloukkaukset raportoidaan ja miten tiedonkulku suoritetaan viranomaisten ja vastuuhenkilöiden välillä. Raportointiprosessi voi pitää sisällään järjestelmiä, jotka keräävät tietoa tietoturvaloukkauksista ja ilmoittavat tietoturvaongelmista vastuuhenkilöille. Raportointiprosessista voidaan saada myös selville, miten noudatetaan direktiivin velvoittamaa kolmiportaista raportointivelvoitetta. Myös selkeät ohjeet on hyvä kirjata raportointiprosessiin, mitkä tiedot ovat tarvittavia raportin laatimiseksi.

Raportointi viranomaisille voidaan suorittaa erillisiä raportointikanavia käyttäen esimerkiksi sähköpostin välityksellä. Raportoinnissa voidaan myös käyttää automaattisia raportointityökaluja, jotka helpottavat raporttien laatimista.

### 3.7 Valvonta ja sakot

Direktiivi antaa Suomen toimivaltaisille viranomaisille valtuudet direktiivin valvontaan ja täytäntöönpanoon yrityksissä direktiivissä asetettujen velvoitteiden suorittamiseksi. Valvontatoimenpiteisiin sisältyvät ammattilaisten tekemät tarkastukset ja turvallisuusauditointien suorittaminen. Näiden lisäksi viranomaisilla on oikeus pääsy tietoihin, joita tarvitaan valvontatoimenpiteiden suorittamiseksi. Täytäntöönpano valtuuksilla tarkoitetaan oikeutta antaa korjaavia määräyksiä ja ohjeita liittyen direktiivin rikkomiseen tai puutteisiin ja mahdollisesti pyytää tuomioistuimia määräämään hallinnollisia sakkoja direktiivin rikkomisesta. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 33 art.).

## Valvonta

Valvova viranomainen (25 §)	Toimiala
Liikenne- ja viestintävirasto	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne, avaruus, digitaalinen infrastruktuuri, TVT-palvelujen hallinta, kuriiri- ja postipalvelun tarjoajat, digitaalisen palvelun tarjoajat, valmistus (moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat, muiden kulkuneuvojen valmistusta harjoittavat toimijat, tutkimusorganisaatiot, julkishallinto)
Energiavirasto	Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat)
Turvallisuus- ja kemikaalivirasto	Kaasu (maakaasun toimittajat, varastointilaitteiston haltijat, maakaasun käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat, aineiden valmistusta ja aineiden tai seosten jakelua harjoittavat yritykset sekä yritykset, jotka tuottavat esineitä aineista tai seoksista, tietokoneiden, elektronisten ja optisten laitteiden valmistajat, sähkölaitteiden valmistajat sekä muiden koneiden ja laitteiden valmistajat
Sosiaali- ja terveydenalan lupa- ja valvontavirasto	Terveys
Etelä-Savon ELY-keskus	Juomavesi, jätevesi ja jätehuolto
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta
Lääkealan turvallisuus- ja kehittämiskeskus	Lääkinnällisiä laitteita valmistavat toimijat ja In vitro –diagnostiikkaan tarkoitettuja lääkinällisiä laitteita valmistavat toimijat
Finanssivalvonta	Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri

 23 26.10.2023

Kuva 2. Ehdotus valvovista viranomaisista eri toimialoille. (Liikenne- ja viestintäministeriö, 2023)

Direktiivin valvontaa tapahtuu useilla tavoilla, ja perustuu ennaltaehkäisevään ja reaktiivisiin toimenpiteisiin. Valvonnan tavoite on varmistaa, että yritykset toteuttavat direktiivin vaatimat toimenpiteet ja vastaavat tietoturvaloukkauksiin asianmukaisesti.

Valvontaa voidaan suorittaa pyytämällä tietoja yrityksen tietoturvamenetelmistä ja riskienhallintasuunnitelmaan liittyvistä toimenpiteistä. Viranomaisilla on myös oikeus tehdä satunnaisia tarkastuksia yrityksiin, joiden aikana voidaan tarkastaa yrityksen turvallisuusjärjestelyitä. Tarkastusten yhteydessä voidaan myös suorittaa kyberturvallisuuteen liittyviä harjoituksia ja simulaatioita.

Valvonta voi liittyä myös direktiivin raportointivelvoitteeseen, sillä raporteista viranomaiset saavat tietoa, miten yrityksessä ollaan toimittamassa tietoturvaloukkauksen sattuessa ja millaisilla toimenpiteillä tilanne on ratkaistu.

Direktiivin mukaan riskienhallintavelvoitteen tai raportointivelvoitteen eli direktiivissä 21 tai 23 artiklan rikkomisesta on määrättävä hallinnollisia sakkoja. Sakkojen tulee olla vaikuttavia, oikeasuhteisia ja sakkoja antaessa otetaan

huomioon kunkin tapauksen tilanne. Sakon määrä keskeisille toimijoille on vähintään 10 000 000 euroa tai vähintään 2 % yrityksen liikevaihdosta sen mukaan kumpi on suurempi. Sakon määrä tärkeille toimijoille on vähintään 7 000 000 euroa tai vähintään 1,4 % yrityksen liikevaihdosta sen mukaan kumpi on suurempi. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 34 art.).

Sakkojen tarkoituksena on kannustaa yrityksiä parantamaan kyberturvallisuuttaan ja varmistamaan yritykset tekemään riittävät investoinnit tietojärjestelmien suojaamiseksi.

### 3.8 Kyberturvallisuusstrategia

Direktiivin mukaan Suomen on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritellään strategiset tavoitteet, kyseisten tavoitteiden saavuttamiseksi tarvittavat resurssit ja sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 7 art.).

Tämän kyberturvallisuusstrategian tulee määrittää selkeät tavoitteet ja painopisteet. Lisäksi strategian on sisällettävä hallintokehys, joka ohjaa tavoitteiden saavuttamista, ja tämän hallintokehysten tulisi sisältää toimintaperiaatteet, jotka kattavat kaikki tarvittavat näkökulmat. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 7 art.).

Kyberturvallisuusstrategian on myös selvennettävä kansallisen tason sidosryhmien tehtävät ja vastuut, tukeakseen toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden välistä yhteistyötä ja koordinointia kansallisella tasolla. Lisäksi on tärkeää määrittää menettelytavat riskien arvioimiseksi ja hallitsemiseksi jäsenvaltiossa (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 7 art.).

Direktiivin mukaan Suomi on velvollinen ilmoittamaan kyberturvallisuusstrategiansa Euroopan unionin komissiolle viimeistään kolmen kuukauden kuluttua strategian hyväksymisestä. Jäsenvaltioiden tulee tarkastella kyberturvallisuusstrategiaansa säännöllisesti ja viiden vuoden välein suorituskykyindikaattorien perusteella. (Euroopan parlamentin ja neuvoston direktiivi 2022/2555/Eu, 7 art.).

## 4 LOPPUPÄÄTELMÄ

Opinnäytetyötä tehdessä pääsin laajasti tutustumaan erilaisiin kyberturvallisuuden sääntelyyn liittyviin direktiiveihin ja lakeihin. Tämän työn pohjalta minulle muodostui hyvä näkemys erityisesti NIS2-direktiivin keskeisimmistä asioista ja yleisesti kyberturvallisuuden sääntelyyn liittyvistä asioista.

Mielestäni NIS2-direktiivin tuomat vaatimukset ovat tärkeitä jatkuvan teknologian kehittymisen kannalta ja tulevat parantamaan huomattavasti kyberturvallisuuden tasoa niin yksittäisten yritysten kuin kansallisella tasolla.

NIS2-direktiivin tuomat vaatimukset luovat yrityksille uusia haasteita ja kustannuksia. Direktiivissä olevat sanktiot ovat isoja ja niin tuleekin olla. Tämä myös näyttää sen, että kyberturvallisuuteen liittyvät asiat halutaan ottaa vakavasti. Tämä pakottaa myös yritykset jatkuvasti pysymään ajan tasalla kyberturvallisuuteen liittyvistä velvoitteista ja ohjeista. Näihin asioihin yritykset voivat saada apua Kyberturvallisuuskeskukselta tai kolmannen osapuolen toimijalta.

NIS2-direktiiviä voisi mielestäni parantaa laajentamalla sen soveltamisalaa vieläkin pienempiin yrityksiin. Tällä tavoin saataisiin vieläkin enemmän yrityksiä sääntelyn piiriin ja näin parannettaisiin kokonaisvaltaisesti kyberturvallisuuden tasoa. Tässä tapauksessa tulisi tarkastella vaatimuksia uudelleen ja kehittää pienemmille yrityksille mielestäni hieman pienemmät vaatimukset. Samoin tulisi myös tehdä sanktioiden määrälle.

Opinnäytetyön haastavimmaksi osuudeksi osoittautui lakitekstien lukeminen ja tekstin tuottaminen. Lakitekstit voivat olla hankalia ymmärtää ja vaikeasti luettavia. Tämä oli myös minulle ensimmäinen kerta, kun pääsin lukemaan kyberturvallisuuteen liittyvää lakitekstiä. Opinnäytetyötä kirjoittaessa kehityin lakitekstien lukemisessa ja ymmärtämisessä. Haasteista huolimatta onnistuin tuomaan esille omasta mielestäni olennaiset asiat.

Kyberturvallisuuden sääntely on monimutkainen asia. Sääntelyyn vaikuttavat lait, yleinen suhtautuminen kyberturvallisuuteen ja teknologian jatkuva kehittyminen. Suomessakin useampi laki vaikuttaa kyberturvallisuuteen ja näiden asioiden oppiminen on elinikäinen prosessi, johtuen jatkuvasta muutoksesta digitaalisessa maailmassa. Opin opinnäytetyötä tehdessä paljon ja haluan tulevaisuudessa oppia enemmän.

## LÄHTEET

ENISA. (n.d.). About ENISA - The European Union Agency for Cybersecurity. Haettu 2.3.2024 osoitteesta <https://www.enisa.europa.eu/about-enisa>

EUR-Lex. (n.d.). Directive. Haettu 4.1.2024 osoitteesta <https://eur-lex.europa.eu/EN/legal-content/glossary/directive.html>

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, 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) (ETA:n kannalta merkityksellinen teksti). <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi>

European Commission. (2023). Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Haettu 22.1.2024 osoitteesta <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

Finlex. (2014). Laki sähköisen viestinnän palveluista. Haettu 30.4.2024 osoitteesta <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>

Finlex. (2018). Tietosuojalaki. Haettu 30.4.2024 osoitteesta <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>

ISO (n.d.). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Haettu 26.2.2024 osoitteesta <https://www.iso.org/standard/27001>

Kyberturvallisuuskeskus. (2024). Sääntelyn toimintatavat. Haettu 9.5.2024 osoitteesta <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-toimintatavat>

Liikenne- ja viestintäministeriö. (26.10.2023). NIS2-direktiivin kansallinen toimenpano. Haettu 11.3.2024 osoitteesta [https://api.hankeikkuna.fi/asiakirjat/34beb41e-515a-4fcd-a824-5136fd497329/a50e57e7-9b1d-4f06-87c4-40571ce29470/ESITYS\\_20231026071232.PDF](https://api.hankeikkuna.fi/asiakirjat/34beb41e-515a-4fcd-a824-5136fd497329/a50e57e7-9b1d-4f06-87c4-40571ce29470/ESITYS_20231026071232.PDF)

Microsoft. (n.d.). What is cybersecurity? Haettu 25.2.2024 osoitteesta <https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity>

Palmer D. (17.5.2019). What is GDPR? Everything you need to know about the new general data protection regulations. Haettu 26.2.2024 osoitteesta <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/>

Prokyberturva (n.d.). Useimpien pk-yritysten on parannettava tietoturvan taso vuonna 2024 – NIS2 Kyberturvallisuusdirektiivi. Haettu 25.3.2024 osoitteesta <https://www.kyberturvallisuus.eu/nis2-kyberturvallisuusdirektiivi/>

Sadoian L. (22.9.2023). The NIS Directive: Enhancing Cybersecurity in the Digital Era. Haettu 26.2.2024 osoitteesta <https://www.upguard.com/blog/nis-directive>

Sisäministeriö. (n.d.). Cyber security as part of national security. Haettu 30.4.2024 osoitteesta <https://intermin.fi/en/national-security/cyber-security>

Tietoturvamerkki. (1.2.2024). Kansainvälinen kehitys. Haettu 2.3.2024 osoitteesta <https://www.tietoturvamerkki.fi/fi/kansainvalinen-kehitys>

Wahl T. (10.9.2019). Cybersecurity Act Introduces Cybersecurity Certification and Strengthens EU's Cybersecurity Agency. Haettu 30.9.2024 osoitteesta <https://eucrim.eu/news/cybersecurity-act-introduces-cybersecurity-certification-and-strengthens-eus-cybersecurity-agency/>