Tampereen ammattikorkeakoulu

Tietoturvan minimivaatimukset NIS2-direktiivin mukaisesti

Petja Hartikainen

OPINNÄYTETYÖ
Toukokuu 2025

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

HARTIKAINEN, PETJA:
Tietoturvan minimivaatimukset NIS2-direktiivin mukaisesti

Opinnäytetyö 32 sivua, joista liitteitä 2 sivua
Toukokuu 2025

Päivitetty versio Euroopan unionin verkko- ja tietoturvadirektiivistä, NIS2-direktiivi, tuo aiempaa tiukempia ja laaja-alaisempia vaatimuksia kyberturvallisuudelle erityisesti kriittisillä toimialoilla. Direktiivi edellyttää organisaatioilta muun muassa riskienhallintaa, raportointivelvollisuuksia ja toimitusketjun turvallisuuden varmistamista. NIS2:n vaatimukset koskevat aiempaa useampia toimijoita ja palveluntarjoajia, joita ei aikaisemmin ole säädelty yhtä tarkasti. Opinnäytetyön tavoitteena oli kartoittaa NIS2-direktiivin asettamat tietoturvan minimivaatimukset sekä tunnistaa niihin liittyvät haasteet ja ratkaisut verkkolähteiden ja viranomaissivustojen pohjalta.

Yhtenä yleisenä haasteena havaittiin muutoksen laajuuden aliarviointi. NIS2 ei ole vain tekninen päivitys, vaan koko organisaation toimintaa muuttava sääntely. Tutkimuksen perusteella erityisesti organisaatiot, joilla ei ole aiempaa kokemusta NIS1-direktiivin toimeenpanosta, kohtaavat ongelmia. Suurimmat haasteet liittyvät teknologisiin ongelmiin, riittämättömiin resursseihin ja osaamisen puutteeseen.

Opinnäytetyön tulokset osoittavat, että NIS2:n onnistunut käyttöönotto vaatii systemaattista suunnittelua, kattavaa nykytila-analyysiä ja hallintakehyksen luomista. Keskeisessä roolissa on myös organisaation laaja yhteistyö ja toimintakulttuurin kehittäminen, jossa jokainen työntekijä ymmärtää roolinsa tietoturvassa. Onnistunut toteutus edellyttää jatkuvaa arviointia ja sopeutumista muuttuviin uhkiin. Parhaiksi käytännöiksi vaatimusten täyttämisessä nousevat muun muassa ISO 27001 -standardin hyödyntäminen, Zero Trust -malli sekä säännölliset koulutukset.

Asiasanat: NIS2-direktiivi, tietoturva, kyberturvallisuus

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunication and Networks

HARTIKAINEN, PETJA:
The Minimum Information Security Requirements Under the NIS2 Directive

Bachelor's thesis 32 pages, appendices 2 pages
May 2025

The updated version of the European Union’s network and information security directive, the NIS2 Directive, introduces stricter and broader cybersecurity requirements, particularly for critical sectors. The directive requires organisations to manage risks, report incidents, and ensure the security of their supply chains. The requirements of NIS2 apply to a wider range of operators and service providers, including many that were not previously regulated in such detail. The aim of the thesis was to identify the minimum cybersecurity requirements introduced by the NIS2 Directive and to examine the related challenges and possible solutions based on online sources and official government websites.

One common challenge identified was the underestimation of the scope of change. NIS2 is not just a technical update but a regulation that affects the entire organisation’s operations. According to the research, organisations with no previous experience with the NIS1 Directive are more likely to face difficulties. The biggest challenges are related to technical issues, limited resources, and lack of expertise.

The findings of the thesis show that successful implementation of the NIS2 Directive requires systematic planning, a comprehensive analysis of the current situation, and the establishment of a governance framework. Cooperation across the organisation and the development of a cybersecurity-aware culture, where all employees understand their role in maintaining security, are also essential. Successful implementation must include continuous evaluation and adaptation to changing threats. Best practices identified include the use of the ISO 27001 standard, the Zero Trust model and regular staff training.

Key words: NIS2 directive, information security, cybersecurity

SISÄLLYS

ERITYISSANASTO

CER-direktiivi	Critical Entities Resilience Directive, Euroopan kriittisen infrastruktuurin sietokykyä koskeva direktiivi
ECSO	European Cyber Security Organisation, Euroopan kyberturvallisuusjärjestö
ENISA	European Union Agency for Cybersecurity, Euroopan unionin kyberturvallisuusvirasto
IT	Information Technology, tietotekniikka
Kiristyshaittaohjelma	Ohjelma, joka salaa käyttäjän tiedostoja tai estää laitteen normaalin käytön ja vaatii lunnaita tietojen palauttamiseksi (ransomware)
NIS-direktiivi	The Network and Information Security Directive, Euroopan unionin verkko- ja tietoturvadirektiivi
NIS2-direktiivi	Uusi päivitetty versio Euroopan unionin verkko- ja tietoturvadirektiivistä
Tekoäly	Tietokonejärjestelmien kyky käyttää perinteisesti ihmisen älyyn liitettyjä toimintoja
Tietojenkalastelu	Verkkourkinta, jossa haltuun pyritään saamaan luottamuksellista tietoa (phishing)
Tietomurto	Oikeudeton tunkeutuminen järjestelmään, palveluun tai laitteeseen, jossa yksityisiä tai luottamuksellisia tietoja varastetaan
TVT	Tieto- ja viestintätekniikka
Zero Trust	Tietoturvamalli, luottamattomuuden periaate, pääkohtina käyttäjän varmistaminen, minimi käyttöoikeudet ja oletetaan aina pahinta

1 JOHDANTO

Tietoverkkoihin kohdistuvat uhkat ja hyökkäykset ovat arkipäivää monille organisaatioille. Yhteiskunnan toimintojen digitalisoituminen on tehnyt kyberturvallisuudesta entistä tärkeämmän osa-alueen. Euroopan unionin uusi NIS2-direktiivi pyrkii vastaamaan tähän haasteeseen asettamalla velvoitteita niille organisaatioille, joiden toiminta on kriittistä yhteiskunnan kannalta. Se korvaa aiemman NIS1-direktiivin ja laajentaa soveltamisalaansa kattamaan enemmän toimialoja ja asettaa tiukempia velvoitteita. (European Commission 2025.) Kyseessä ei ole pelkkä tekninen sääntely, vaan kokonaisvaltainen muutos, joka vaikuttaa koko organisaation toimintakulttuuriin (Moczulski 2024).

Opinnäytetyössä tarkastellaan, mitä vaatimuksia NIS2-direktiivi asettaa organisaatioille, millaisia haasteita vaatimusten täyttämisessä kohdataan sekä millaisia ratkaisuja ja parhaita käytäntöjä on esitetty direktiivin tehokkaaseen toteuttamiseen. Tutkimuskysymykset ovat seuraavat:

- Mitä tietoturvan minimivaatimuksia NIS2-direktiivi asettaa organisaatioille?
- Mitkä ovat keskeiset haasteet, joita organisaatiot kohtaavat vaatimusten täyttämisessä?
- Mitä ratkaisuja ja parhaita käytäntöjä on esitetty NIS2 vaatimusten toteuttamiseen?

Opinnäytetyön tavoitteena on kartoittaa NIS2-direktiivin asettamat tietoturvan minimivaatimukset, tunnistaa näihin liittyvät keskeiset haasteet sekä tarkastella parhaimpia ratkaisuja ja toimintamalleja. Tarkoituksena on koota aiheesta tällä hetkellä löytyvä tieto yhteen hyödyntämällä eri verkkolähteitä ja viranomaissivustoja. Opinnäytetyön avulla pyritään muodostamaan kokonaiskuva NIS2-direktiivin merkityksestä ja sen tuomista velvoitteista sekä keinoista, joilla organisaatiot voivat saavuttaa vaatimustenmukaisuuden muuttuvassa kyberturvallisuusympäristössä.

2 NIS2-DIREKTIIVI JA TIETOTURVAN MINIMIVAATIMUKSET

Euroopan unionin uusi NIS2-direktiivi on edeltäjäänsä NIS-direktiiviä (NIS1) tiukempi ja laajempi. Tämä päivitetty versio on astunut voimaan lokakuussa 2024. (European Commission 2025.) Kappaleessa käsitellään direktiivin taustoja ja tavoitteita, sekä perehdytään sen tuomiin vaatimuksiin.

2.1 Direktiivin tausta ja tavoitteet

Euroopan unionin verkko- ja tietoturvadirektiivi, eli NIS-direktiivi, asettaa tietoturvaa ja häiriöraportointia koskevia velvollisuuksia useille eri toimialoille. Sen korvaa uusi NIS2-direktiivi, joka päivittää ja laajentaa aiemman sääntelyn. NIS2-direktiivin keskeisenä tavoitteena on vahvistaa EU:n yhteistä sekä jäsenvaltioiden kansallista kyberturvallisuuden tasoa erityisesti kriittisillä sektoreilla. (NIS2 - Euroopan unionin kyberturvallisuusdirektiivi n.d.)

Direktiivi asettaa näille kriittisille toimialoille kyberturvallisuuteen liittyviä riskienhallintavelvoitteita, sekä edellyttää merkittävien poikkeamien raportointia. Lisäksi se määrittelee vähimmäistoimenpiteet, joita kaikkien toimijoiden on noudatettava suojatakseen toimintansa kyberturvallisuusuhkilta. (NIS2 - Euroopan unionin kyberturvallisuusdirektiivi n.d.) NIS2-direktiivi tuli saattaa osaksi kansallista lainsäädäntöä viimeistään 17.10.2024 ja sen täytäntöönpanoa koskevien säännösten tulisi olla sovellettu 18.10.2024 alkaen (European Commission 2025).

Euroopan komissio on aloittanut rikkomusmenettelyt lähettämällä viralliset huomautuskirjeet 23 jäsenvaltiolle (mukaan lukien Suomi), jotka eivät olleet määräaikaan 17. lokakuuta 2024 mennessä saaneet NIS2-direktiiviä täysimääräisesti osaksi kansallista lainsäädäntöään. Näiden jäsenvaltioiden on vastattava ja saatettava direktiivin täytäntöönpano loppuun. (European Commission 2025.) Suomessa eduskunta on hyväksynyt hallituksen esityksen uudesta kansallisesta kyberturvallisuuslaista, jonka tarkoituksena on ollut saattaa EU:n NIS2-direktiivin vaatimukset osaksi Suomen lainsäädäntöä. Direktiivin mukaiset velvoitteet astuivat Suomessa voimaan 8.4.2025. (Kyberturvallisuuslaki on hyväksytty… 2025.)

Organisaatioiden johdolla on velvollisuus huolehtia kyberturvallisuuteen liittyvien riskien hallinnasta. Heidän tulee suunnitella ja valvoa riskienhallinnan toteutumista sekä hyväksyä siihen liittyvät toimintamallit ja -periaatteet. Johdon on myös ymmärrettävä kyberturvallisuuden riskit riittävällä tasolla, jotta se pystyy ohjaamaan toimintaa asianmukaisesti. Lakiesityksen mukaan johto viittaa esimerkiksi hallitukseen, hallintoneuvostoon, toimitusjohtajaan tai muuhun henkilöön, joka tosiasiallisesti johtaa organisaation toimintaa. (NIS2-direktiivi ja sen… n.d.)

2.1.1 NIS2-direktiivi ja ero NIS1-direktiiviin

NIS1, eli direktiivi 2016/1148, oli ensimmäinen kattava verkko- ja tietojärjestelmien kyberturvallisuutta parantava EU:n lainsäädäntö. Kasvavien kyberuhkien myötä tämä korvattiin direktiivillä 2022/2555, eli toiselta nimeltään NIS2. Tämä uusi direktiivi nostaa EU:n kyberturvallisuustavoitteita laajentamalla sen soveltamisalaa, selkeyttämällä sääntelyä ja vahvistamalla valvontakeinoja. (European Commission 2025.) Vuonna 2016 julkaistu NIS1-direktiivi oli monilta osin liian epämääräinen, mikä johti epäyhtenäiseen toimeenpanoon eri jäsenvaltioissa. Esimerkiksi kriittisen infrastruktuurin määritelmät vaihtelivat maittain, eikä direktiivissä ollut tarkkoja sääntöjä toteutuksen valvonnasta tai kyberuhkien raportoinnista. Lisäksi NIS1-direktiivi ei huomioinut riittävästi kyberturvallisuuden kestävyyttä eikä tarjonnut riittäviä keinoja koordinoituihin kriisivasteisiin. Näiden puutteiden, kasvavien kyberuhkien ja uusien vaatimusten vuoksi Euroopan komissio päätti uudistaa direktiivin. Uusi NIS2-direktiivi hyväksyttiin Euroopan parlamentissa 16. tammikuuta 2023. (Hiess 2023.)

NIS2-direktiivin soveltamisalaan kuuluvat automaattisesti kaikki kriittisillä sektoreilla toimivat suuret yritykset, sekä keskisuuret yritykset, joissa on yli 50 työntekijää ja yli 10 miljoonan euron liikevaihto. Sen lisäksi direktiivi koskee kaikkia toimijoita, jotka ovat kansallisesti tunnistettu kriittisiksi toimijoiksi. Yrityksen koko ei vaikuta tähän määrittelyyn ja kyseiset toimijat saavat siitä erillisen ilmoituksen. (Hyvä tietää NIS2-direktiivistä n.d.) Nämä toimijat ovat määritelty kriittisiksi toimijoiksi CER-direktiivin mukaan (NIS2-direktiivi - Tavoitteena… 2023).

Toimijat luokitellaan kahteen ryhmään: keskeisiin ja tärkeisiin toimialoihin (Tärkeää tietoa Euroopan… 2025). Keskeisiin eli erittäin kriittisiin toimijoihin kuuluu: liikenne, energia, pankki ja finanssi, terveys, vesi, digitaalinen infrastruktuuri, yritysten välinen TVT-palvelujen hallinta, julkishallinto ja avaruus. Tärkeisiin eli muihin kriittisiin toimijoihin luokitellaan: posti, jätehuolto, kemikaalit, elintarvikkeet, valmistava teollisuus, digipalvelut, tutkimustoiminta sekä verkkotunnusten rekisteröintipalveluja tarjoavat toimijat. (Kyberturvallisuuskeskus 2025.) NIS2-direktiiviä sovelletaan myös lueteltuihin toimialoihin koosta riippumatta seuraavissa tapauksissa:

- Toimija on ainoa taho jäsenvaltiossa, joka tuottaa palvelua, jolla on keskeinen rooli yhteiskunnan tai talouden kriittisten toimintojen jatkuvuuden turvaamisessa.
- Toimijan tarjoaman palvelun häiriö voisi vaikuttaa merkittävästi yleiseen järjestykseen, turvallisuuteen tai kansanterveyteen.
- Toimija tarjoaman palvelun häiriö voisi aiheuttaa merkittävän systeemisen riskin etenkin aloilla, joilla häiriöillä olisi potentiaalia aiheuttaa rajat ylittäviä vaikutuksia.
- Toimija katsotaan kriittiseksi, koska sen toiminnalla on erityisen suuri painoarvo kansallisella tai alueellisella tasolla joko oman toimialansa tai palvelutyypin näkökulmasta, tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta. (Tärkeää tietoa Euroopan… 2025.)

NIS2 tulee siis koskemaan paljon laajempaa joukkoa keskeisten palveluiden toimijoita ja digitaalisten palveluiden tarjoajia verrattuna NIS1-direktiiviin. NIS1 koski vain tiettyjen alojen keskeisten palveluiden toimijoita, kuten energia-, liikenne-, terveydenhuolto- ja rahoitusaloja. Nyt yhä useammat organisaatiot EU:ssa kuuluvat direktiivin vaatimusten piiriin, kuten jätehuollon, elintarvikkeiden, postin, avaruuden ja digitaalisen infrastruktuurin toimijat (kuva 1). Soveltamisalan laajennus kuvastaa digitaalisen infrastruktuurin kasvavaa merkitystä ja tarvetta parantaa verkko- ja tietojärjestelmien kestävyyttä laajemmalla toimialakirjolla. (Cipollone 2023.)

KUVA 1. NIS2-direktiiviin lisätyt toimijat verrattuna NIS1-direktiiviin (Cipollone 2023).

2.1.2 ISO 27001 -standardin yhteys NIS2-direktiiviin

ISO/IEC 27001 on kansainvälisesti tunnustettu standardi, joka määrittää vaatimukset tietoturvallisuuden hallintajärjestelmälle. Sen avulla organisaatiot voivat suojata tietojaan ennakoivasti, varmistaa lakisääteisten vaatimusten noudattamisen ja integroida tietoturvan osaksi muita johtamisjärjestelmiä. (ISO/IEC 27001 - tietoturvallisuuden hallintajärjestelmä n.d.) ISO 27001 -standardin parhaat käytännöt tarjoavat organisaatioille selkeän viitekehyksen häiriötilanteiden hallintaan ja raportointiin. NIS2-direktiivi velvoittaa organisaatioita ilmoittamaan merkittävistä kyberturvallisuushäiriöistä, mutta ei määrittele tarkkoja toimintatapoja. ISO 27001 sen sijaan antaa yksityiskohtaiset ohjeet muun muassa häiriöiden tunnistamiseen, hallintaan, niihin reagoimiseen ja toipumiseen. (Tschirpig 2024.)

Ottamalla käyttöön ISO 27001 -standardin organisaatiot voivat varmistaa NIS2 vaatimusten täyttymisen ja samalla vahvistaa tietoturvakäytäntöjään. Lisäksi sertifiointi osoittaa sitoutumista kyberturvallisuuteen ja voi lisätä sidosryhmien luottamusta. Pelkkä standardin noudattaminen ei kuitenkaan riitä, vaan se tulee mu-

kauttaa organisaation erityistarpeisiin. NIS2:n tehokas toteutus edellyttää tasapainoa standardin mukaisten käytäntöjen ja organisaation omien riskienhallintamenetelmien välillä. (Tschirpig 2024.)

Tulevaisuudessa molemmat viitekehykset, ISO 27001 ja NIS2, tulevat todennäköisesti kehittymään rinnakkain täydentäen toisiaan. ISO 27001 tarjoaa laajan ja globaalin lähestymistavan, kun taas NIS2 tuo tarkempia vaatimuksia kriittisiin sektoreihin. Globaalisti toimivat organisaatiot voivat hyödyntää ISO 27001 -standardia perustana ja täydentää sitä NIS2 vaatimuksilla, mikäli toiminta kattaa kriittisiä toimialoja EU:ssa. Puolestaan EU:ssa toimivat organisaatiot voivat ottaa NIS2:n ensisijaiseksi viitekehyksekseen ja yhdistää siihen ISO 27001:n laajemmat kontrollit. (What is the difference… 2024.)

2.2 Keskeiset tietoturvavaatimukset

Toimijoiden on otettava käyttöön ja ylläpidettävä ajantasainen malli kyberturvallisuusriskien hallintaan. Sen tarkoituksena on suojata viestintäverkot, tietojärjestelmät ja niiden fyysiset ympäristöt häiriöiltä ja niiden seurauksilta. Lisäksi toimijoiden on toteutettava mallin mukaisia teknisiä, operatiivisia ja organisatorisia toimenpiteitä, joilla hallitaan kyberturvallisuusriskejä sekä ehkäistään tai minimoidaan mahdolliset haittavaikutukset. (Tärkeää tietoa Euroopan… 2025.)

Toimenpiteiden tulee perustua kokonaisvaltaiseen riskienhallintamalliin, joka ottaa huomioon kaikki mahdolliset uhkatekijät ja tähtää verkko- sekä tietojärjestelmien ja niiden fyysisen toimintaympäristön suojaamiseen häiriöiltä (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 21 §). Lisäksi niiden on sisällettävä vähintään seuraavat NIS2-direktiivin 21 artiklan mukaiset toimet:

- riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat
- poikkeamien käsittely
- toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta
- toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat

- verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen
- toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta
- perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus
- toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä
- henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta
- tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 21 §.)

Kyseinen artikla 21 nousee yhdeksi keskeisimmäksi osaksi direktiiviä, sillä se määrittää ne tietoturvatoimenpiteet, joita organisaatioiden on noudatettava. Tämä artikla löytyy kokonaisuudessaan liitteestä 1.

NIS2-direktiivin alaiset organisaatiot ovat velvoitettuja suorittamaan säännöllisiä ja perusteellisia riskianalyyseja arvioidakseen teknologiaansa ja dataansa kohdistuvia uhkia. Tämä kattava riskianalyysi toimii pohjana tietoturvapolitiikalle, joka määrittelee selkeästi, miten kutakin riskiä hallitaan ja lievennetään. Organisaatiot ovat velvoitettuja luomaan selkeät ja tehokkaat prosessit häiriötilanteiden hallintaan, mukaan lukien uhkien torjunta, liiketoiminnan jatkuvuus ja palautuminen. Tämä tarkoittaa järjestelmällisiä toimintamalleja uhkien havaitsemiseen ja hallintaan, liiketoiminnan jatkuvuussuunnitelmaa palvelukatkosten varalta sekä katastrofista palautumisen strategiaa, joka määrittelee toimenpiteet häiriön jälkeiseen toipumiseen. (NIS2 Directive: What entities… n.d.)

Direktiivi edellyttää, että organisaatiot arvioivat ja hallitsevat toimittajiensa ja yhteistyökumppaneidensa aiheuttamia riskejä. Tietoturvallisuuden varmistamiseksi on tärkeää käyttää turvallisia hankintakäytäntöjä, kehitysmenetelmiä ja ylläpitotoimia. Tämä tarkoittaa selkeitä sopimusvelvoitteita tietoturvavaatimusten noudattamisesta, säännöllisiä auditointeja ja turvallisten kehityskäytäntöjen toteuttamista koko toimintaketjussa. Näiden vaatimusten tehokas noudattaminen edel-

lyttää organisaatioilta ennakoivaa lähestymistapaa kyberturvallisuuden parantamiseen, riskienhallinnan vahvistamiseen ja laadunvarmistukseen. (NIS2 Directive: What entities… n.d.)

Lisäksi kaikkien NIS2-direktiivin soveltamisalaan kuuluvien toimijoiden tulee ilmoittautua oman toimialansa valvovan viranomaisen ylläpitämään toimijaluetteloon. Mikäli toimija kuuluu useaan eri toimialaan, on hänen ilmoittauduttava erikseen jokaiselle toimialakohtaiselle valvontaviranomaiselle. (Kyberturvallisuuslaki on hyväksytty… 2025.)

2.2.1 Raportointivelvoite

NIS2-direktiivin alaisuuteen kuuluvan toimijan on ilmoitettava välittömästi valvovalle viranomaiselle merkittävästä poikkeamasta. Poikkeama viittaa tilanteeseen, jossa viestintäverkkojen ja tietojärjestelmien kautta tarjottujen tai niiden kautta saatavilla olevien tietojen ja palvelujen saatavuus, aitous, eheys, tai luottamuksellisuus vaarantuu. Merkittävällä poikkeamalla tarkoitetaan tilannetta, joka on aiheuttanut tai saattaa aiheuttaa vakavan häiriön palveluiden toiminnassa, taloudellisia menetyksiä kyseiselle toimijalle tai merkittäviä aineellisia tai aineettomia muille yksityishenkilöille tai oikeushenkilöille. (Tärkeää tietoa Euroopan… 2025.)

Ilmoitusprosessi (kuva 2) etenee kolmessa vaiheessa: ensimmäinen ilmoitus on tehtävä 24 tunnin kuluessa poikkeaman havaitsemisesta, jatkoilmoitus 72 tunnin sisällä ja lopullinen raportti on toimitettava kuukauden kuluessa jatkoilmoituksesta. Pitkäkestoisissa poikkeamissa loppuraportti tulee toimittaa kuukauden kuluessa tapauksen käsittelyn päättymisestä. Jos merkittävä poikkeama todennäköisesti vaikuttaa palvelujen toimintaan ja tarjoamiseen, toimijan on myös ilmoitettava siitä palvelun käyttäjille ilman viivytystä. Suomessa on käytössä Traficomin Kyberturvallisuuskeskuksen sähköinen NIS2-poikkeamailmoituspalvelu, jossa ilmoituksen pystyy tekemään. (Tärkeää tietoa Euroopan… 2025.)

KUVA 2. Raportointivaatimusten aikataulu (Robertson 2024).

2.3 Valvonta

Jäsenvaltioiden tulee huolehtia siitä, että toimivaltaiset viranomaiset valvovat direktiivin noudattamista ja toteuttavat tarvittavat toimenpiteet sen täytäntöönpanemiseksi. Valvontatoimenpiteitä voidaan sallia asetettavan etusijalle, tällöin on sovellettava riskiperusteista lähestymistapaa. Viranomaisten tulee tehdä yhteistyötä muiden valvontaviranomaisten kanssa, erityisesti henkilötietojen tietoturvaloukkauksia koskevissa tapauksissa. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 31 §.)

Toimivaltaisilla viranomaisilla on oltava riittävät valtuudet valvoa julkishallinnon toimijoita ja määrätä tarvittaessa täytäntöönpanotoimenpiteitä. Heidän tulee myös olla riippumattomia valvomistaan toimijoista. Valvontatoimenpiteiden on oltava vaikuttavia, oikeasuhteisia ja varoittavia, sekä jokaisen yksittäisen tapauksen olosuhteet on otettava huomioon. Keskeisiin toimijoihin kohdistuvat valvontatoimenpiteet voivat sisältää tarkastuksia, turvallisuusauditointeja ja riskinarviointeihin perustuvia skannauksia. Toimivaltaiset viranomaiset voivat vaatia pääsyä tietoihin ja dokumentaatioon sekä saada näyttöä kyberturvallisuusperiaatteiden noudattamisesta. Tarvittaessa viranomaiset voivat antaa varoituksia, sitovia ohjeita tai määräyksiä, keskeyttää toiminnan tai määrätä sakkoja. Jos aiemmat täytäntöönpanotoimenpiteet eivät ole riittäviä, viranomaiset voivat asettaa määräaikoja puutteiden korjaamiseksi. Mikäli näitä määräaikoja ei noudateta, viranomaisilla on oikeus keskeyttää toimijan lupa tai estää sen johtohenkilöitä jatkamasta tehtävissään. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 32 §.)

Tärkeitä toimijoita koskevat vastaavat toimenpiteet suoritetaan vain siinä tapauksessa, jos on näyttöä tai viitteitä direktiivin noudattamatta jättämisestä. Käytettävissä olevat seuraamukset ovat myös samanlaisia kuin keskeisten toimijoiden kohdalla, mutta ne voivat olla lievempiä. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 33 §.)

Taulukkoon 1 on koottu Suomen valvovat viranomaiset toimialakohtaisesti. Osa toimialoista on jaettu useammalle valvovalle viranomaiselle toimialan osan ja toimijatyypin mukaan. Tämä tarkempi jaottelu löytyy Traficomin kyberturvallisuuskeskuksen sivuilta. (Tärkeää tietoa Euroopan… 2025.)

TAULUKKO 1. Valvovat viranomaiset toimialoittain (Tärkeää tietoa Euroopan… 2025, muokattu).

Toimiala	**Valvova viranomainen**
Energia	Energiavirasto Tukes
Liikenne Digitaalinen infrastruktuuri TVT-palvelujen hallinta Julkishallinto Avaruus Posti- ja kuriiripalvelut Digitaalisen palvelun tarjoajat Tutkimustoiminta	Traficom
Kemikaalien valmistus, tuotanto ja jakelu	Tukes
Terveys	Valvira Fimea
Juomavesi Jätevesi Jätehuolto	Etelä-Savon ELY-keskus
Valmistus	Fimea Tukes Traficom
Elintarvikkeiden tuotanto, jalostus ja jakelu	Ruokavirasto
Pankkitoiminta Finanssimarkkinoiden infrastruktuurit	Finanssivalvonta

2.3.1 Seuraamukset

Jäsenvaltioiden tulee huolehtia, että keskeisille ja tärkeille toimijoille määrättävät hallinnolliset sakot ovat vaikuttavia, oikeasuhteisia ja varoittavia. Valvontaviranomaisten on huomioitava seuraamusten määräämisessä tapauskohtaiset olosuhteet, muun muassa rikkomuksen vakavuus, sen kesto, aiemmat rikkomukset sekä aiheutuneet haittavaikutukset. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 34 §.)

Keskeisille toimijoille sakko voi olla enintään 10 miljoonaa euroa tai 2 % yrityksen edellisen tilikauden maailmanlaajuisesta liikevaihdosta ja tärkeille toimijoille sakko voi vastaavasti olla enintään seitsemän miljoonaa euroa tai 1,4 % liikevaihdosta, riippuen kumman määrä on suurempi. Jäsenvaltiot voivat myös säätää uhkasakoista direktiivin rikkomusten lopettamiseksi. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 34 §.)

Julkishallinnon toimijoiden sakottamisesta voidaan säätää kansallisella tasolla. Mikäli jäsenvaltion oikeusjärjestelmässä ei ole hallinnollisia sakkoja, niiden on varmistettava vaihtoehtoinen tehokas oikeudellinen menettely sakkojen määräämiseksi. (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, 34 §.)

3 HAASTEET MINIMIVAATIMUSTEN TÄYTTÄMISESSÄ

NIS2-direktiivin vaatimukset voivat tuoda mukanaan haasteita joillekin organisaatioille. Kappaleessa käydään läpi yleisimpiä ongelmia ja haasteita, joita minimivaatimusten täyttäminen voi luoda. Lisäksi pohditaan pk-yritysten haasteita verrattuna suuryrityksiin.

3.1 Yleiset ongelmat

NIS2-direktiivin täytäntöönpanoon liittyy useita haasteita, jotka voivat vaikeuttaa sen sujuvaa ja tehokasta käyttöönottoa. Yksi yleisimmistä kompastuskivistä on muutoksen laajuuden aliarviointi. NIS2 ei ole vain pieni päivitys, vaan se merkitsee kokonaisvaltaista uudistusta, jonka toteuttaminen vaatii huolellista suunnittelua sekä riittävästi aikaa ja resursseja. Direktiivin vaatimuksia ei myöskään voi hoitaa kertaluonteisesti, vaan ne edellyttävät jatkuvaa seurantaa ja kehittämistä. Organisaatioiden on rakennettava järjestelmä, joka mahdollistaa jatkuvan kehittämisen. Valmistelut on kannattanut aloittaa mahdollisimman varhain, jotta toteutus voidaan tehdä perusteellisesti ja ilman kiirettä. Viime hetken toimenpiteet harvoin johtavat parhaisiin lopputuloksiin. (Moczulski 2024.)

Toinen tyypillinen virhe on keskittyminen pelkästään teknologiaan. Vaikka kyberturvallisuus usein mielletään tekniseksi asiaksi, NIS2-direktiivin toimeenpano edellyttää koko organisaation osallistumista. Kyseessä on organisatorinen muutos, joka vaatii eri osastojen välistä yhteistyötä. Turvallisuuskulttuurin merkitystä ei sovi unohtaa. Vaikka järjestelmät olisivat teknisesti edistyneitä, ei niistä ole hyötyä, mikäli työntekijät eivät ymmärrä tai osaa käyttää niitä. Tämän vuoksi on tärkeää panostaa koulutukseen ja tietoisuuden lisäämiseen koko organisaatiossa. (Moczulski 2024.)

Erityisiä toimeenpanohaasteita kokevat NIS2-direktiivin piiriin vastikään sisällytetyt uudet toimijat, sillä ne astuvat monimutkaiseen sääntelykehykseen ilman aiempaa kokemusta alkuperäisestä NIS-direktiivistä. Sääntelyn piiriin kuulumi-

nen luo erityistä painetta resurssien kohdentamiseen ja asiantuntemuksen kehittämiseen. Monet näistä organisaatioista ovat perinteisesti investoineet ensisijaisesti operatiiviseen tehokkuuteen ja fyysiseen turvallisuuteen kyberturvallisuuden sijaan. Nyt niiden on nopeasti ohjattava merkittäviä resursseja digitaalisten suojauskyvykkyyksien kehittämiseen, joka tapahtuu usein ilman selkeitä toimialakohtaisia viitekehyksiä tai vakiintuneita parhaita käytäntöjä. (ECSO 2025.)

Joustamattomuus voi myös osoittautua ongelmalliseksi. Kyberuhkat muuttuvat jatkuvasti ja turvallisuusjärjestelmien on kyettävä mukautumaan uusiin tilanteisiin. Direktiivin mukainen järjestelmä edellyttää valmiutta sopeutua ja muuttua uhkien mukana. (Moczulski 2024.) Vuonna 2024 Euroopan unionin alueella havaittiin, että valtaosa rikollisista kyberhyökkäyksistä liittyi kiristyshaittaohjelmiin, tietojenkalasteluun ja tietomurtoihin. Vaikka viranomaisten kyvyt vastata kyberuhkiin ovat parantuneet ja kansainvälinen yhteistyö on tiivistynyt, rikolliset jatkavat toimintansa kehittämistä. Yksi huomattava ilmiö on tekoälyn kasvava käyttö rikollisessa toiminnassa. Tekoälyn avulla tuotetut tietojenkalasteluviestit ovat muuttuneet entistä uskottavammiksi ja vaikeammin tunnistettaviksi, mikä lisää niiden tehokkuutta. Samalla haittaohjelmamuunnelmien määrä kasvaa jatkuvasti, mikä tekee torjunnasta entistä haastavampaa. Kyberrikollisuus myös osoittaa kykenevänsä sopeutumaan nopeasti uusiin teknologioihin ja hyödyntämään esiin tulevia haavoittuvuuksia, jonka myötä ilmiö säilyttää asemansa merkittävänä uhkana myös tulevina vuosina. (Kybersää 2025.)

3.1.1 Teknologiset haasteet

Yksi suurimmista haasteista NIS2-direktiivin käytännön toteuttamisessa etenkin suomalaisissa organisaatioissa on se, että suurella osalla yrityksistä ei ole vielä tietoturvallisuuden hallintajärjestelmää, eikä myöskään ymmärrystä mitä se käytännössä tarkoittaa (Aaltonen 2024). Samoja haasteita kokee myös Suomen ulkopuoliset organisaatiot. Alhaisemman kyberturvallisuuskypsyystason sektorit kohtaavat erityisen suuren haasteen NIS2-direktiivin myötä, sillä niiltä edellytetään käytännössä valtavaa teknologista harppausta lyhyessä ajassa. Näihin sektoreihin kuuluvat esimerkiksi valmistavan teollisuuden toimialat, jotka ovat perin-

teisesti toimineet yksinkertaisilla IT-järjestelmillä ja minimaalisilla kyberturvallisuustoimilla, koska niiden ydinprosessit eivät alun perin ole olleet suunniteltuja pitämään silmällä digitaalisia uhkia. (ECSO 2025.)

NIS2 siis edellyttää, että alhaisemmat kyberturvallisuustason sektorit kehittävät nopeasti kehittyneitä kyberturvallisuusvalmiuksia, joita digitaalisesti kypsemmät alat ovat rakentaneet vähitellen useiden vuosien aikana. Tilannetta vaikeuttaa entisestään se, että näillä aloilla hyödynnetään usein vanhentuneita järjestelmiä ja operatiivista teknologiaa, jotka eivät ole alun perin sisältäneet nykyaikaisia kyberturvallisuusominaisuuksia. (ECSO 2025.)

3.1.2 Taloudelliset ja resurssipulaan liittyvät haasteet

Tietoturvan viitekehykset ja NIS2:n vaatimukset sisältävät paljon käsitteitä ja sanastoa, jotka voivat tuntua vieraalta ilman aiempaa kokemusta alalta. Viranomaiset tarjoavat usein ohjeita ja suosituksia tukemaan yrityksiä vaatimusten täyttämisessä, mikä on lähtökohtaisesti hyvä asia. Ongelmaksi muodostuu se, että nämä ohjeet saattavat paisua alkuperäisiä vaatimuksia paljon laajemmiksi ja ovat usein kirjoitettu alan kielellä. Tämä saattaa tuntua vaikeaselkoiselta ja tilanne muistuttaakin lakitekstien tulkintaa. Kuten lainsäädäntöä tulkittaessa tarvitaan usein juristin apua, myös tietoturvajärjestelmien rakentamisessa tarvitaan asiantuntijaa. Siksi järkevin tapa aloittaa NIS2-vaatimusten mukaisen tietoturvajärjestelmän kehittäminen on hyödyntää esimerkiksi koulutettua ja kokenutta konsulttia, joka osaa selittää vaatimukset ymmärrettävästi ja auttaa toteuttamaan ne tehokkaasti organisaation tarpeisiin soveltaen. (Aaltonen 2024.) Tämä kuitenkin tuo mukanaan yrityksille lisäkustannuksia.

EU:n kyberturvallisuusviraston (ENISA) raportissa käy ilmi, että neljättä vuotta peräkkäin IT-tunnit, jotka on omistettu tietoturvalle, ovat laskeneet. Tämä lasku voi heijastaa rekrytointiongelmia, sillä organisaatiot kamppailevat kyberturvallisuusroolien täyttämisessä, erityisesti teknistä asiantuntemusta vaativissa tehtävissä. Suuntaus on erittäin merkittävä, sillä 89 % datan keräämisessä mukana olleista organisaatioista odottaa tarvitsevansa lisää kyberturvallisuushenkilöstöä NIS2-direktiivin noudattamiseksi. (Navigating cybersecurity investments… 2024.)

ECSO:n NIS2 Implementation: Challenges and Priorities -julkaisussa (2025), joka tarkastelee NIS2-direktiivin toimeenpanon tilaa jäsenvaltioissa ja siihen kuuluvissa organisaatioissa, todetaan kyselytietojen osoittavan, että noin 75 % organisaatioista ei ole varannut erillistä taloudellista resurssia direktiivin toimeenpanoon. Joillakin organisaatioilla nykyiset kyberturvallisuuskäytännöt saattavat jo olennaisesti vastata NIS2-vaatimuksia, mikä vähentää lisärahoituksen tarvetta. Toiset voivat olla vasta NIS2-suunnitteluprosessin alkuvaiheessa tekemässä vaikutusarviointeja ja aukkoanalyyseja ennen tarkkojen budjettivarausten tekemistä. On kuitenkin olemassa riski, että jotkut organisaatiot aliarvioivat täyden toimeenpanon vaatimat resurssit, tai kamppailevat kyberturvallisuussijoitusten priorisoinnissa toimintabudjettiensa puitteissa.

3.2 Pk-yritysten haasteet verrattuna suuryrityksiin

Erityisesti pk-yrityksille, eli pienille ja keskikokoisille, NIS2-direktiivin täytäntöönpano saattaa tuoda haasteita. NIS2-direktiivi tuo laajempia vaatimuksia ja samalla lisää raportointivelvoitteita ja valvontaa, jotka voivat olla erityisen raskaita pk-yrityksille. Laajentunut soveltamisala voi aiheuttaa merkittävää hallinnollista taakkaa toimijoille, joilla ei ole ennestään kyberturvallisuusjärjestelmiä eikä riittäviä resursseja kyberturvallisuuden takaamiseksi ja raportoinnin hoitamiseksi. Tämä voi luoda riskin, jossa pienet yritykset voivat kokea sääntöjen noudattamisen liian vaativaksi ja rajoittavaksi, mikä puolestaan voi johtaa siihen, että ne jättävät kyberturvallisuustoimet tekemättä tai tekevät ne vain osittain. (Vandezande 2023.)

Hallinnollinen taakka kasvaa, sillä pienillä yrityksillä ei ole yleensä riittävästi henkilöstä tai asiantuntemusta kyberturvallisuuden vaatimusten täyttämiseen. Tämä voi johtaa tilanteeseen, jossa pienet yritykset eivät kykene täyttämään direktiivin vaatimuksia tehokkaasti. Pk-yritykset voivat joutua kohtaamaan suuria vaikeuksia hallinnollisen työn ja valvonnan lisääntymisen myötä. (Vandezande 2023.)

Pienten yritysten rooli direktiivin täytäntöönpanossa on erityisen kriittinen, sillä niiden aliresursoitu tila tekee kyberturvallisuustoimien toteuttamisesta haastavaa.

Vaikka pk-yritysten osuus digitaalisessa ekosysteemissä on merkittävä, ne voivat jäädä usein huomiotta kyberturvallisuuspolitiikassa ja niiden kyky vastata kyberuhkiin on usein rajallinen. Tämä asettaa paineita lainsäätäjille ja viranomaisille luoda tasapainoinen ja oikeudenmukainen lähestymistapa, jossa pk-yrityksille annetaan realistisia ja käytännöllisiä mahdollisuuksia täyttää NIS2-direktiivin vaatimukset ilman kohtuuttomia hallinnollisia rasitteita. (Vandezande 2023.)

4 RATKAISUT JA PARHAAT KÄYTÄNNÖT

Kappaleessa tuodaan esiin ratkaisuja ja parhaimpia käytäntöjä, joiden avulla NIS2-direktiivin minimivaatimusten täyttäminen voi helpottua ja mitä asioita siinä kannattaa ottaa huomioon. Loppuun on vielä koottu hyödyllisiä neuvoja ja keinoja, jotka auttavat organisaatioita vastaamaan direktiivin velvoitteisiin.

4.1 Yleinen valmistautuminen

Valmistautuminen NIS2-direktiiviin on strateginen askel kohti entistä kestävämpää ja häiriönsietokykyisempää toimintaa. Ensin on hyvä ymmärtää direktiivin vaatimukset ja perehdyttävä sen yksityiskohtiin. Syvällinen ymmärrys vaatimuksista auttaa suunnittelemaan tehokkaan strategian vaatimuksenmukaisuuden saavuttamiseksi. Vaatimuksenmukaisuus ei ole erillinen prosessi, vaan monialaista yhteistyötä vaativa kokonaisuus. Tätä varten voi koota tiimin, johon kuuluu edustajia organisaation keskeisiltä alueilta. (NIS2 Directive: What entities… n.d.)

Nykytilasta kannattaa kartoittaa analyysi. Tämä tarkoittaa selvitystä, missä tilanteessa organisaatio on tällä hetkellä ja mitä sen on vielä tehtävä täyttääkseen NIS2 -vaatimukset. Tavoitteena on tunnistaa haavoittuvuudet ja vaatimuksenmukaisuuden puutteet. (NIS2 Directive: What entities… n.d.) Näiden pohjalta voi laatia konkreettisen listan tarvittavista toimenpiteistä. Toimenpiteet kannattaa priorisoida ja asettaa tärkeysjärjestykseen aloittamalla kriittisimmistä ja kiireellisimmistä asioista. (Moczulski 2024.)

Kattavan kyberturvallisuusstrategian ja hallintakehyksen laatiminen on tärkeää. Strategian tulisi linjata kyberturvallisuustoimenpiteet liiketoiminnan tavoitteiden kanssa. Hallintakehys puolestaan määrittää selkeät roolit ja eskalointipolut. Myös toimitusketjun turvallisuutta voi vahvistaa ottamalla käyttöön tiukat turvallisuusstandardit kumppaneille ja toimittajille. (NIS2 Directive: What entities… n.d.)

4.1.1 Teknologiset ratkaisut

Vahvat tietoturvan hallintakäytännöt tulisi ottaa käyttöön. Tämän voi toteuttaa parantamalla tiedonsiirron turvallisuutta, käyttämällä salauksia sekä soveltamalla tiukkaa käyttöoikeuksien hallintaa. Lisäksi ottamalla käyttöön selkeät häiriötilanteiden raportointikäytännöt ja kehittämällä tehokkaita reagointistrategioita voidaan tietoturvaa parantaa. (Moczulski 2024.)

Kaikki organisaatiot voivat hyötyä Zero Trust -suojausmallista, joka perustuu periaatteeseen ”älä koskaan luota, varmista aina”. Käyttäjiin, laitteisiin tai verkkoihin ei tule luottaa oletuksena ja jokainen pääsypyyntö on todennettava, valtuutettava ja salattava ennen pääsyn myöntämistä. Käyttäjille annetaan vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Verkkoa ei myöskään käsitellä yhtenä suurena kokonaisuutena, vaan se jaetaan pieniin eristettyihin vyöhykkeisiin. Tämä vaikeuttaa hyökkääjän etenemistä verkossa. Zero Trust vaatii jatkuvaa valvontaa ja reaaliaikaista turvallisuustilan arviointia, joka mahdollistaa uhkien nopean havaitsemisen ja niihin reagoinnin. (Christi 2024.)

Säännölliset auditoinnit sekä turvalliset IT-hankinta- ja kehitysprosessit ovat myös keskeisiä (Moczulski 2024). Auditoinnilla organisaatio voi osoittaa täyttävänsä esimerkiksi lainsäädännön tai sopimusten edellyttämiä velvoitteita. Auditointi on aina dokumentoitu prosessi, jossa kerätään puolueetonta näyttöä siitä, että sovitut kriteerit täyttyvät. Se toimii myös organisaatioiden oman toiminnan kehittämisen tukena. (Lindroos 2019.)

Lisäksi järjestelmiä tulisi testata säännöllisesti sekä arvioida suojaustoimenpiteiden tehokkuutta ja tehdä ennakoivia parannuksia (NIS2 Directive: What entities… n.d.). NIS2 on jatkuva prosessi ja on varauduttava säännöllisiin päivityksiin ja tietoturvajärjestelmän parantamiseen (Moczulski 2024). Vaikka kyberrikollisuus säilyttää asemansa merkittävänä uhkana digitaalisen yhteiskunnan turvallisuudelle, positiivista on se, että kyberturvallisuuteen liittyvä sääntely kehittyy jatkuvasti. Tämä auttaa vahvistamaan puolustuskykyä ja rajoittamaan rikollisten vaikutusmahdollisuuksia. EU:ssa kehitetty lainsäädäntö tukee jäsenvaltioiden pyrkimyksiä hillitä kyberrikollisuuden vaikutuksia ja edistää turvallisempaa digitaalista toimintaympäristöä. Kyberrikollisuuden painopisteet vaihtelevat eri EU-

maissa, mutta Suomessa tilannetta seurataan aktiivisesti kyberturvallisuuskeskuksen toimesta. Se tarjoaa ajankohtaista tietoa ja tukee toimijoita kyberturvallisuuden ylläpitämisessä alati muuttuvassa uhkaympäristössä. (Kybersää 2025.)

4.1.2 Hallinnolliset ratkaisut

Lopullinen vastuu IT-asioiden linjauksista ja niiden toteutuksista on yrityksen johdolla. NIS2-direktiivin vaatimusten täyttäminen kuuluu erityisesti ylimmän johdon vastuulle, joten johtavassa asemassa olevien on syytä perehtyä sen sisältöön huolella. Johdon on tunnettava organisaation kyberturvallisuuden nykytila ja varmistettava, että käytännön tietoturvatoimet ovat hyvin organisoituja ja hyväksyttyjä ylimmällä tasolla. Jotta kyberturvallisuustyö olisi tehokasta, vastuuhenkilöillä on oltava kokonaisvaltainen ymmärrys tilanteesta ja organisaation sisäiset tiedonkulun esteet, kuten eri yksiköiden erillään toimimisesta johtuvat siiloutuneet käytännöt, on purettava suunnitelmallisesti. (Pennanen 2024.)

NIS2:n toteuttaminen voi edellyttää taloudellisia investointeja. Olisi hyvä suunnitella budjetti, joka kattaa tarvittavat laite- ja ohjelmistohankinnat sekä koulutukset henkilökunnalle. Koulutus on hyvinkin keskeinen asia ja koko henkilöstön säännöllisistä kyberturvallisuuskoulutuksista laadittu suunnitelma on toimiva ratkaisu. (Moczulski 2024.)

Tietoturvallinen toimintaympäristö rakentuu jokaisen työntekijän panoksesta. Kun jokainen tietää oman roolinsa, ei työntekijää tarvitse nähdä riskinä, vaan osana ratkaisua. Yhteinen toimintakulttuuri luo ilmapiirin, jossa myös puutteet voidaan nostaa esiin avoimesti ja turvallisesti. Vaikka työntekijän ei tarvitse olla tietoturvan asiantuntija, hänen on tärkeää tunnistaa riskitilanteet ja tietää keneltä saa apua ja mihin poikkeamat tulee ilmoittaa. (Pennanen 2024.)

Jos organisaatio haluaa ottaa käyttöön Zero Trust -mallin, se ei ole pelkästään tekninen haaste, vaan kulttuurinen muutos. Se edellyttää muutoksia IT:n hallintaan, käytäntöihin ja jopa työntekijöiden ajattelutapaan tietoturvasta. Muutos todennäköisesti vaikuttaa myös työntekijöiden rooleihin ja vastuisiin. Heitä tulee

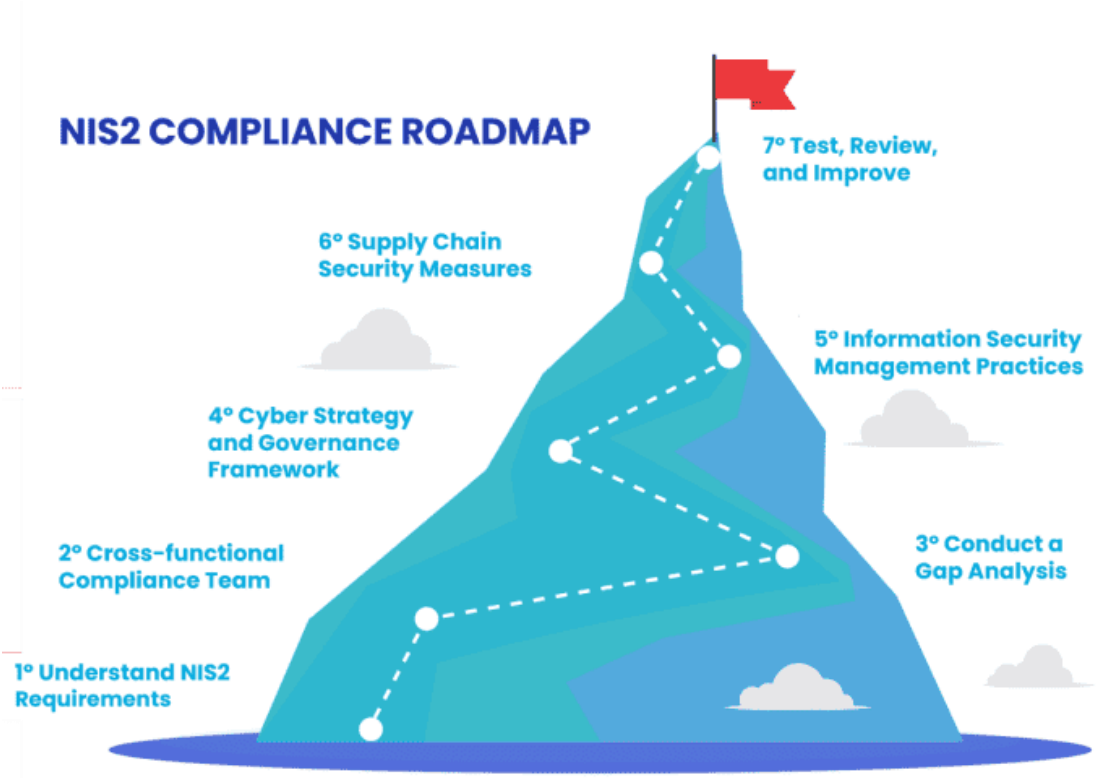
kouluttaa ymmärtämään tietoturvan merkitys ja oma roolinsa sen ylläpidossa. Tähän lukeutuu esimerkiksi lisätodennuksien hyväksyminen tai erilliset pääsypyynnöt resursseihin, joihin heillä oli aiemmin automaattinen oikeus. Zero Trust -malliin siirtyminen edellyttää organisaatiolta nykytilan arviointia, kriittisten resurssien tunnistamista, tietovirtojen mallintamista sekä vähimmän oikeuden periaatteeseen perustuvien käytäntöjen kehittämistä. Tärkeää on myös jatkuva valvonta ja suojaustoimenpiteiden ylläpito. (Christi 2024.)

4.2 Organisaatioiden tueksi

Monet etenkin teknologia- ja tietoturvayritykset tarjoavat palveluja organisaatioiden tueksi, joiden avulla he voivat avustaa NIS2-direktiivin vaatimuksiin vastaamisessa. Esimerkiksi Huld Oy tarjoaa NIS2 vaatimuksenmukaisuuden arviointia, joka sisältää haastatteluja ja organisaation turvallisuusjohtamisen dokumentaation tarkastelua erityisesti riskienhallinnan näkökulmasta. Käytännöt, prosessit ja ohjeistukset verrataan NIS2-vaatimuksiin ja arvioinnin tuloksena syntyy luettelo havaituista kehitystarpeista sekä konkreettisista suosituksista. Täytäntöönpanon tukena tarjotaan myös apua riskienhallintaratkaisujen suunnitteluun ja toteutukseen. Lisäksi NIS2-koulutus on mahdollista sisällyttää osaksi projektia. (What we do, NIS2-directive n.d.) Suomalainen ICT-alan yritys Loihde Oyj tarjoaa muun muassa kyberturvan asiantuntijapalveluita, jotka tukevat vaatimusten eri osa-alueissa. Lisäksi he tuottavat segmentoituja verkkoratkaisuja sekä jatkuvaa tietoturvavalvontaa, jota NIS2 vaatii. (Hyvä tietää NIS2-direktiivistä n.d.) Myös ICT-ratkaisuja tuottava Mintly Oy tarjoaa esimerkiksi hallinnollisia ja teknisiä tietoturvapalveluita, joista on apua direktiivin uusien säädöksien noudattamisessa (Mikä on NIS2-direktiivi… 2025).

Tietoturvayritys SealPath on koonnut vaiheet vaatimuksenmukaisuuden saavuttamiseksi (kuva 3). Ensimmäinen vaihe on perehtyä direktiivin vaatimuksiin perusteellisesti ja koota poikkitoiminnallinen tiimi, joka vastaa vaatimuksenmukaisuuden suunnittelusta ja toteutuksesta. Nykytila-analyysin avulla selvitetään organisaation vahvuudet ja puutteet suhteessa NIS2:n velvoitteisiin, minkä jälkeen laaditaan kyberturvallisuusstrategia ja selkeä hallintomalli, jotka tukevat koko or-

ganisaation toimintaa. Käytännön toimenpiteisiin kuuluu tietoturvan hallintakäytäntöjen vahvistaminen, kuten salaus, käyttöoikeuksien hallinta, häiriöiden raportointi ja reagointivalmiudet. Toimitusketjun turvallisuus on myös varmistettava kumppaneille asetettavilla vaatimuksilla ja säännöllisillä tarkastuksilla. Lopuksi järjestelmien ja käytäntöjen tehokkuutta on arvioitava jatkuvasti testaamalla, seuraamalla ja kehittämällä niitä aktiivisesti. (NIS2 Directive: What entities… n.d.)



KUVA 3. Etenemissuunnitelma NIS2 vaatimusten saavuttamiseksi (NIS2 Directive: What entities… n.d.).

5 JOHTOPÄÄTÖKSET JA POHDINTA

Tämä opinnäytetyö tarjosi kokonaiskuvan NIS2-direktiivin asettamista tietoturvan minimivaatimuksista, niiden täyttämiseen liittyvistä keskeisistä haasteista sekä esitteli ratkaisuja ja käytäntöjä, joilla organisaatiot voivat vastata uusiin velvoitteisiin. Opinnäytetyön perusteella voidaan todeta, että NIS2-direktiivi edustaa merkittävää muutosta EU:n kyberturvallisuussääntelyssä. Se laajentaa vaatimusten kohteena olevien organisaatioiden määrää ja tiukentaa tietoturvaan liittyviä velvoitteita. Direktiivin toimeenpano edellyttää organisaatioilta strategista lähestymistä, teknisiä ratkaisuja, säännöllistä koulutusta ja johdon vahvaa sitoutumista.

Opinnäytetyön tulokset osoittavat, että direktiivin täytäntöönpano voi olla monille organisaatioille kuormittavaa erityisesti silloin, kun tietoturvallisuuteen ei ole aiemmin kiinnitetty riittävästi huomiota. Keskeisiksi haasteiksi nousivat teknologiset ja taloudelliset haasteet, kuten vanhentuneet järjestelmät, resurssipula ja osaamisen puute. Nämä korostuvat etenkin pk-yrityksissä. Myös sääntelyn monimutkaisuus ja tulkinnan vaikeus voi muodostua esteeksi tehokkaalle toimeenpanolle ja aiheuttaa epävarmuutta sekä hallinnollista kuormitusta. Näihin haasteisiin vastaaminen edellyttää kokonaisvaltaisia toimia, esimerkiksi organisaation sisäistä yhteistyötä, ulkopuolista asiantuntemusta sekä selkeiden ja skaalautuvien toimintamallien kehittämistä. Työssä esitellyt ratkaisut, eli ISO 27001 -standardin hyödyntäminen, Zero Trust -mallin käyttöönotto ja jatkuva riskienhallinta tarjoavat konkreettisia apuvälineitä vaatimusten täyttämiseen.

Opinnäytetyön tavoitteet täyttyivät hyvin ja tutkimuskysymyksiin löydettiin selkeitä vastauksia. Vastaukset perustuvat ajankohtaisiin verkkolähteisiin, eivätkä yritysten omiin kokemuksiin. Jatkotutkimuksina voitaisiinkin kysyä yritysten näkemyksiä siitä, mitkä direktiivin toimeenpanossa oikeasti osoittautuivat haasteiksi ja mitkä toimintatavat olivat tehokkaimpia. Lisäksi voitaisiin myös selvittää, miten direktiivin käytännön soveltaminen toimii eri toimialoilla ja miten yritykset arvioivat omia tietoturvavalmiuksia direktiivin voimaantulon jälkeen. Kehittämisehdotuksena voidaan esittää, että erityisesti pienemmille toimijoille suunnataan selkokielistä ohjeistusta ja tukea, jotta sääntelyn tavoitteet voidaan saavuttaa yhdenvertaisesti.

LÄHTEET

Aaltonen, J. 2024. NIS2-direktiivi. ICT Elmo Oy. Verkkosivu. Viitattu 9.4.2025. https://www.elmo.fi/ajankohtaista/nis2-direktiivi/

Christi. 2024. Zero Trust Security: Principles of the Zero Trust Security Model. Zero Security. Verkkosivu. Viitattu 2.5.2025. https://zerosecurity.org/zero-trust-security-principles/14814/

Cipollone, F. 2023. NIS2 vs NIS1 Key Regulation and Differences for vulnerability management. Phoenix security. Verkkosivu. Viitattu 13.3.2025. https://phoenix.security/nis2-regulation-differences/

ECSO. 2025. White Paper: NIS2 Implementation: Challenges and Priorities. PDF. Viitattu 6.5.2025. https://ecs-org.eu/ecso-uploads/2025/01/ECSO-NIS2-White-Paper.pdf

European Commission. 2025. NIS2 Directive: new rules on cybersecurity of network and information systems. Verkkosivu. Viitattu 2.4.2025. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555. Annettu 14 päivänä joulukuuta 2022. Euroopan Unioni. Verkkosivu. Viitattu 17.3.2025. https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi

Hiess, M. 2023. NIS2 directive brings major challenges. Anexia. Verkkosivu. Viitattu 28.3.2025. https://anexia.com/blog/en/nis2-directive-brings-major-challenges/

Hyvä tietää NIS2-direktiivistä. n.d. Loihde. Verkkosivu. viitattu 13.3.2025. https://www.loihde.com/nis2-direktiivi

ISO/IEC 27001 - tietoturvallisuuden hallintajärjestelmä. n.d. DNV. Verkkosivu. Viitattu 31.3.2025. https://www.dnv.fi/services/iso-iec-27001-tietoturvallisuuden-hallintajarjestelma-3327/

Kybersää. 2025. TRAFICOM Kyberturvallisuuskeskus. PDF. Viitattu 2.5.2025. https://kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4n%20maaliskuu%202025.pdf

Kyberturvallisuuskeskus. 2025. TRAFICOM NIS2 taulukko. PDF. Viitattu 13.3.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_07012025.pdf

Kyberturvallisuuslaki on hyväksytty eduskunnassa – NIS2-direktiivin mukaiset velvoitteet astuvat voimaan 8.4.2025. 2025. TRAFICOM. Verkkosivu. Viitattu 9.4.2025. https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksytty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet

Lindroos, E. 2019. Mitä on auditointi? Arter. Verkkosivu. Viitattu 2.5.2025. https://www.arter.fi/mita-on-auditointi/

Mikä on NIS2-direktiivi ja ketä se koskee? 2025. Mintly Oy. Verkkosivu. Viitattu 15.5.2025. https://mintly.fi/uutiset/mika-on-nis2-direktiivi-ja-keta-se-koskee/

Moczulski, R. 2024. Understanding the NIS2 Directive: New Challenges and Opportunities in Cybersecurity. TTMS. Verkkosivu. Viitattu 8.4.2025. https://ttms.com/uk/understanding-the-nis2-directive-new-challenges-and-opportunities-in-cybersecurity/

Navigating cybersecurity investments in the time of NIS 2. 2024. ENISA. Verkkosivu. Viitattu 6.5.2025. https://www.enisa.europa.eu/news/navigating-cybersecurity-investments-in-the-time-of-nis-2

NIS2-direktiivi ja sen vaikutukset yrityksille. n.d. PwC. Verkkosivu. Viitattu 10.4.2025. https://www.pwc.fi/fi/palvelut/teknologia-ja-digitaalisuus/kyberturvallisuus-ja-tietosuoja/nis2-direktiivi-ja-sen-vaikutukset-yrityksille.html

NIS2-direktiivi - Tavoitteena kyberturvallisempi tulevaisuus. 2023. Deloitte. Verkkosivu. Viitattu 14.3.2025. https://www.deloitte.com/fi/fi/services/risk-advisory/perspectives/nis2-direktiivi-tavoitteena-kyberturvallisempi-tulevaisuus.html

NIS2 Directive: What Entities Need to Know about Compliance? - Complete Guide & Real Case Studies. n.d. SealPath. Verkkosivu. Viitattu 31.3.2025. https://www.sealpath.com/blog/nis2-directive-guide-requirements/

NIS2 – Euroopan unionin kyberturvallisuusdirektiivi. n.d. Kyberturvallisuuskeskus. Verkkosivu. Viitattu 12.3.2025. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Pennanen, J. 2024. NIS2:n parhaat käytännöt: varmista nämä seitsemän asiaa. Loihde. Verkkosivu. Viitattu 7.5.2025. https://www.loihde.com/ajankohtaista/blogi/nis2n-parhaat-kaytannot-varmista-nama-seitseman-asiaa

Robertson, B. 2024. Taking Time to Understand NIS2 Reporting Requirements. Imperva. Verkkosivu. Viitattu 2.4.2025. https://www.imperva.com/blog/taking-time-to-understand-nis2-reporting-requirements/

Tschirpig, C. 2024. NIS2 - direktiivin häiriöiden raportointivaatimukset ja liittyvät ISO 27001:n parhaat käytännöt. Digiturvamalli. Verkkosivu. Viitattu 31.3.2025. https://www.digiturvamalli.fi/blogi/nis2-hairioiden-raportointivaatimukset-ja-niihin-liittyvat-iso-27001--standardin-parhaat-kaytannot

Tärkeää tietoa Euroopan unionin kyberturvallisuusdirektiivistä (NIS2). 2025. Kyberturvallisuuskeskus. Verkkosivu. Viitattu 17.3.2025. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa#67853-0

Vandezande, N. 2023. Cybersecurity in the EU: How the NIS2-Directive Stacks Up Against its Predecessor. SSRN. PDF. Viitattu 7.4.2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4383118

What is the difference between ISO 27001 and NIS2? 2024. PrivacyEngine. Verkkosivu. Viitattu 9.4.2025. https://www.privacyengine.io/blog/iso-27001-nis2-differences/

What we do, NIS2-directive. n.d. Huld Oy. Verkkosivu. Viitattu 15.5.2025. https://huld.io/what-we-do/nis2-directive/

LIITTEET

Liite 1. NIS2-direktiivin artikla 21 kokonaisuudessaan (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555).

21 artikla 1 (2)

Kyberturvallisuusriskien hallintatoimenpiteet

1. Jäsenvaltioiden on varmistettava, että keskeiset ja tärkeät toimijat toteuttavat asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet hallitakseen riskejä, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu, ja estääkseen tai minimoidakseen poikkeamien vaikutuksen palvelujensa vastaanottajiin ja muihin palveluihin.

Kun otetaan huomioon viimeisin kehitys ja tapauksen mukaan asiaa koskevat eurooppalaiset ja kansainväliset standardit sekä täytäntöönpanokustannukset, ensimmäisessä alakohdassa tarkoitetuilla toimenpiteillä on varmistettava, että verkko- ja tietojärjestelmien turvallisuuden taso on oikeassa suhteessa riskeihin. Näiden toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon se, missä määrin toimija altistuu riskeille, toimijan koko ja poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset.

2. Edellä 1 kohdassa tarkoitettujen toimenpiteiden on perustuttava kaikki vaaratekijät huomioivaan toimintamalliin, jolla pyritään suojaamaan verkko- ja tietojärjestelmät ja näiden järjestelmien fyysinen ympäristö poikkeamilta, ja niihin on sisällyttävä vähintään seuraavat:

a) riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;
b) poikkeamien käsittely;
c) toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;
d) toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;
e) verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;
f) toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;
g) perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;
h) toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;
i) henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta;
j) tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

3. Jäsenvaltioiden on varmistettava, että toimijoiden harkitessa, mitkä tämän artiklan 2 kohdan d alakohdassa tarkoitetuista toimenpiteistä ovat asianmukaisia, toimijat ottavat

(jatkuu)

huomioon kullekin välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, niiden tuotteiden yleisen laadun sekä toimittajiensa ja palveluntarjoajiensa kyberturvallisuuskäytännöt, mukaan lukien tuotekehityksen suojausmenettelyt. Jäsenvaltioiden on myös varmistettava, että toimijoiden harkitessa, mitkä kyseisessä alakohdassa tarkoitetuista toimenpiteistä ovat asianmukaisia, toimijoita vaaditaan ottamaan huomioon 22 artiklan 1 kohdan mukaisesti tehtyjen kriittisiä toimitusketjuja koskevien koordinoitujen riskinarviointien tulokset.

4. Jäsenvaltioiden on varmistettava, että toimija, joka toteaa, ettei se noudata 2 kohdassa säädettyjä toimenpiteitä, toteuttaa ilman aiheetonta viivytystä kaikki tarvittavat, asianmukaiset ja oikeasuhteiset korjaavat toimenpiteet.

5. Komissio hyväksyy viimeistään 17 päivänä lokakuuta 2024 täytäntöönpanosäädöksiä, joilla vahvistetaan 2 kohdassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset, jotka koskevat DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia.

Komissio voi hyväksyä täytäntöönpanosäädöksiä, joilla vahvistetaan 2 kohdassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä tarvittaessa alakohtaiset vaatimukset, jotka koskevat muita keskeisiä ja tärkeitä toimijoita kuin tämän kohdan ensimmäisessä alakohdassa tarkoitettuja toimijoita.

Valmistellessaan tämän kohdan ensimmäisessä ja toisessa alakohdassa tarkoitettuja täytäntöönpanosäädöksiä komissio noudattaa mahdollisimman pitkälle eurooppalaisia ja kansainvälisiä standardeja sekä asiaankuuluvia teknisiä eritelmiä. Komissio vaihtaa neuvoja ja tekee yhteistyötä yhteistyöryhmän ja ENISAn kanssa 14 artiklan 4 kohdan e alakohdan mukaisesti, kun kyse on ehdotuksista täytäntöönpanosäädöksiksi.

Nämä täytäntöönpanosäädökset hyväksytään 39 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen.